

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

Кваліфікаційна наукова
праця на правах рукопису

СИТНІК ЄВГЕН ІГОРОВИЧ

УДК 005:[658:338.246:004(043.3)

ДИСЕРТАЦІЯ

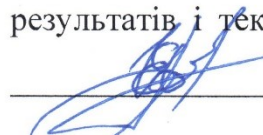
УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА
НА ОСНОВІ ІННОВАЦІЙНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ

073 Менеджмент

07 Управління та адміністрування

Подається на здобуття ступеня доктора філософії

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

 Є.І. Ситнік

Науковий керівник: Правдивець Олександр Миколайович, к. військ. наук

Київ – 2026

АНОТАЦІЯ

Ситнік Є.І. Управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 073 «Менеджмент» (07. Управління та адміністрування). – ВНЗ «Університет економіки та права «КРОК», Київ, 2026.

Дисертація присвячена вирішенню наукового завдання, яке полягало у обґрунтуванні теоретико-методичних засад та розробці науково-практичних рекомендацій щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Досліджено теоретико-методичні засади, наукові підходи, стратегію, механізми, методи, моделі, технології управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

У дисертації розроблено модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, що передбачає оцінювання на трьох рівнях: рівні загальних процесів функціонування, рівні окремих бізнес-процесів діяльності та в забезпеченні економічної безпеки підприємства. Крім того модель передбачає комплексне оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки, що забезпечує нові можливості для проведення аналізу, оцінювання та отримання об'єктивних комплексних даних щодо стану та рівня впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та дозволяє впровадити моніторинг та виявити слабкі місця, недоліки, спланувати своєчасні заходи з метою зростання рівня цифрової безпеки та ефективності підприємства у протидії ризикам та загрозам в умовах сучасної цифрової трансформації, зростання рівня кіберзагроз зовнішнього середовища.

Розроблено стратегію управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій, яка включає реалізацію стратегічних та оперативних цілей за ключовими напрямками та передбачає цифровізацію процесів здійснення управлінської, операційної, безпекової діяльності підприємства завдяки впровадженню і використанню інноваційних цифрових технологій і дає можливість удосконалити процеси управління, розбудову і функціонування системи та механізму управління економічною безпекою підприємства на сучасному техніко-технологічному рівні, відповідно до вимог та викликів цифрового, техніко-технологічного, ринкового середовищ і забезпечує можливості протидіяти ризикам, загрозам, забезпечувати безпеку, конкурентоспроможність, стійкість і ефективний розвиток підприємства.

Обґрунтовано структуру і елементи системи економічної безпеки підприємства розбудованої із впровадженням цифрових технологій та визначено правову, фінансову, кадрову, інтелектуальну, виробничо-операційну, матеріально-майнову, техніко-технологічну, інноваційно-інвестиційну, інформаційно-цифрову, інтерфейсну, ринкову, фізичну складові системи економічної безпеки, цифровізація якої, на відміну від існуючих, дає можливість автоматизувати, оптимізувати процеси управління, зменшити витрати, забезпечити зростання ефективності та результативності у всіх функціональних сферах діяльності підприємства, як єдиної цілісної системи і таким чином досягнути зростання рівня стабільності, надійності економічної безпеки підприємства.

Сформовано механізм управління системою економічної безпеки підприємства на основі впровадження інноваційних цифрових технологій, який виступає сукупністю елементів, і на відміну від існуючих, забезпечує комплекс дій з розробки та реалізації планів і заходів відповідно до прийнятої стратегії забезпечення економічної безпеки та організації контролю за їх виконанням відповідно до прийнятих стандартів, норм виконання робіт з застосуванням адміністративно-організаційних, оперативно-розпорядчих,

економічних, соціально-психологічних, техніко-технологічних методів та їх інструментів, що дає можливість забезпечувати стійкість та формує умови для подальшого ефективного розвитку підприємства завдяки впровадженню інновацій, передових інноваційних цифрових технологій у всіх сферах діяльності та в системі економічної безпеки; забезпечує захист підприємства від внутрішніх та зовнішніх небезпек, загроз; забезпечує утримання ринкових позицій, зростання конкурентоспроможності та подальший розвиток підприємства.

Досліджено концептуально-методичні засади управління системою економічної безпеки підприємства та виявлено дію наукових підходів трьох рівнів: (1) підходів до розуміння поняття економічної безпеки; (2) підходів до розуміння системи економічної безпеки; (3) підходів до управління системою економічної безпеки підприємства, та на відміну від існуючих, обґрунтовано новий технологічний підхід до розуміння управління системою економічної безпеки підприємства як сукупності підсистем, складових та елементів, взаємодія яких реалізується із застосуванням сучасних цифрових технологічних засобів, що забезпечує ефективне функціонування механізму системи безпеки та застосування методів, інструментів, технологій управління; найбільш оптимальне раціональне використання її кадрових, фінансових, матеріальних ресурсів; зростання рівня безпеки підприємства завдяки широкому використанню технологічних можливостей і зростанню ролі та значення інформаційно-аналітичного забезпечення в прийнятті управлінських рішень.

Ідентифіковано та систематизовано три групи показників: цифровізації загальних процесів функціонування підприємства; показників впровадження цифрових технологій для управління бізнес-процесами діяльності; показників впровадження цифрових технологій в забезпеченні економічної безпеки до складу яких віднесено п'ятдесят два показника системний аналіз яких забезпечує можливості для комплексного дослідження процесів впровадження інноваційних цифрових технологій та на основі отриманих даних дає

можливість здійснювати моніторинг та подальше всебічне системне оцінювання процесів управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Систематизовано наукові концепти, узагальнено функції застосування цифрових технологій в управлінні з виявленням дії облікової, логістичної, безпекової, інформаційно-аналітичної, комунікаційної, операційної, маркетингової функцій, використання яких забезпечує можливість впровадження цифровізації, цифрової трансформації бізнес-процесів у всіх функціональних сферах діяльності підприємства та формування якісно нових комунікацій співпраці і взаємодії з партнерами, стейкхолдерами зовнішнього, глобального середовища, що дасть можливість оптимізувати та зменшити витрати, забезпечити зростання економічної та ринкової ефективності діяльності підприємства.

Досліджено теоретичні основи застосування інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та визначено сутність інформаційно-цифрової складової системи економічної безпеки підприємства, яка поєднує в собі ознаки та функції інформаційної та цифрової складових, що разом надають технології, інструменти та засоби, мають значно ширші можливості для впровадження ефективного інформаційно-аналітичного забезпечення та формують комплексний дієвий захист підприємства адаптований до протидії реалізації небезпек і загроз зовнішнього ринкового і внутрішнього середовищ в умовах впровадження технологій Четвертої промислової революції, Індустрії 4.0. та нових технологічних викликів і змін.

Проведено аналіз та сформовано проекцію впливу впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, яка дає можливість виявити та ідентифікувати вплив використання цифрових технологій загального спрямування, інноваційних цифрових технологій управління забезпеченням функціональної діяльності та безпосередньо цифрових технологій, які використовуються в забезпеченні

економічної безпеки підприємства, загальне та комплексне використання яких дає можливість здійснювати управління системою економічної безпеки на сучасному цифровому рівні та забезпечувати належний рівень економічної безпеки підприємства в умовах нових цифрових викликів та загроз.

Практичне значення результатів дисертаційного дослідження полягає у використанні його наукових положень, висновків і здобутків у науковій та науково-дослідній діяльності, а також в процесі управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Ключові слова: управління, економічна безпека, безпека, система економічної безпеки підприємства, управління системою економічної безпеки, інноваційні цифрові технології, інновації, стратегія, механізм управління, технології штучного інтелекту, технології блокчейн, ризики, загрози, кризові умови, інноваційна діяльність, інноваційний розвиток

ANNOTATION

Sytnik Y. Management of the system of economic security of the enterprise based on innovative digital technologies. – Qualification scientific work on the rights of manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 073 «Management» (07. Management and administration). – “KROK” University, Kyiv, 2026.

The dissertation is devoted to solving the scientific problem, which was to substantiate the theoretical and methodological foundations and develop scientific and practical recommendations for managing the system of economic security of the enterprise on the basis of innovative digital technologies.

The theoretical and methodological foundations, scientific approaches, strategy, mechanisms, methods, models, technologies of management of the system of economic security of enterprise on the basis of innovative digital technologies have been studied.

The dissertation develops a model for a comprehensive assessment of the implementation of innovative digital technologies in the management of the system of economic security of an enterprise, which provides for assessment at three levels: the level of general processes of functioning, the level of individual business processes of activity and in ensuring the economic security of the enterprise. In addition, the model provides for a comprehensive assessment of the introduction of innovative digital technologies in the management of the system of economic security, which provides new opportunities for analysis, assessment and obtaining objective comprehensive data on the state and level of implementation of innovative digital technologies in the management of the economic security system of the enterprise and allows monitoring and identification of weaknesses, shortcomings, planning timely measures to increase the level of digital security and efficiency of the enterprise in countering risks and threats in the context of modern digital transformation, an increase in the level of cyber threats to the external environment.

A strategy for managing the system of economic security of an enterprise based on innovative digital technologies has been developed, which includes the implementation of strategic and operational goals in key areas and provides for the digitalization of the processes of managerial, operational, security activities of the enterprise through the introduction and use of innovative digital technologies and makes it possible to improve the processes of management, development and functioning of the system and mechanism of management of economic security of the enterprise at the modern technical and technological level, in accordance with the requirements and challenges of digital, technical, technological, market environments and provides opportunities to counteract risks, threats, ensure security, competitiveness, sustainability and effective development of the enterprise.

The structure and elements of the system of economic security of the enterprise built with the introduction of digital technologies are substantiated and the legal, financial, personnel, intellectual, production and operational, material and property, technical and technological, innovation-investment, information-digital, interface, market, physical components of the economic security system are determined, the digitalization of which, in contrast to the existing ones, makes it possible to automate, optimize management processes, reduce costs, to ensure the growth of efficiency and effectiveness in all functional areas of the enterprise, as a single integral system and thus to achieve an increase in the level of stability, reliability of the economic security of the enterprise.

A mechanism for managing the system of economic security of an enterprise based on the introduction of innovative digital technologies has been formed, which is a set of elements, and in contrast to the existing ones, provides a set of actions for the development and implementation of plans and measures in accordance with the adopted strategy for ensuring economic security and the organization of control over their implementation in accordance with the adopted standards, norms for the performance of work with the use of administrative and organizational, operational-administrative, economic, socio-psychological, technical and technological methods and their tools, which makes it possible to ensure sustainability and forms conditions

for further effective development of the enterprise through the introduction of innovations, advanced innovative digital technologies in all areas of activity and in the system of economic security; provides protection of the enterprise from internal and external dangers, threats; ensures the maintenance of market positions, growth of competitiveness and further development of the enterprise.

The conceptual and methodological foundations of management of the system of economic security of an enterprise have been investigated and the effect of scientific approaches of three levels has been revealed: (1) approaches to understanding the concept of economic security; (2) approaches to understanding the system of economic security; (3) approaches to the management of the system of economic security of the enterprise, and in contrast to the existing ones, a new technological approach to understanding the management of the system of economic security of the enterprise as a set of subsystems, components and elements, the interaction of which is implemented with the use of modern digital technological means, which ensures the effective functioning of the mechanism of the security system and the use of methods, tools, management technologies; the most optimal rational use of its human, financial, material resources; growth of the level of enterprise security due to the wide use of technological capabilities and the growth of the role and importance of information and analytical support in managerial decision-making.

Three groups of indicators have been identified and systematized: digitalization of the general processes of enterprise functioning; indicators of the introduction of digital technologies for the management of business processes of activity; indicators of the introduction of digital technologies in ensuring economic security, which include fifty-two indicators, the system analysis of which provides opportunities for a comprehensive study of the processes of introduction of innovative digital technologies and on the basis of the obtained data makes it possible to monitor and further comprehensive systematic assessment of the processes of managing the system of economic security of the enterprise based on innovative digital technologies.

Scientific concepts are systematized, the functions of using digital technologies in management are generalized with the identification of the effects of accounting, logistics, security, information and analytical, communication, operational, marketing functions, the use of which provides the possibility of introducing digitalization, digital transformation of business processes in all functional areas of the enterprise and the formation of qualitatively new communications of cooperation and interaction with partners, stakeholders external, global environment, which will make it possible to optimize and reduce costs, ensure the growth of economic and market efficiency of the enterprise.

The theoretical foundations of the application of innovative digital technologies in the management of the system of economic security of the enterprise have been investigated and the essence of the information-digital component of the system of economic security of the enterprise has been determined, which combines the features and functions of the information and digital components, which together provide technologies, tools and means, have much wider opportunities for the introduction of effective information and analytical support and form a comprehensive effective protection enterprises adapted to counteract the implementation of dangers and threats of the external market and internal environments in the context of the introduction of technologies of the Fourth Industrial Revolution, Industry 4.0. and new technological challenges and changes.

The analysis is carried out and a projection of the impact of the introduction of innovative digital technologies in the management of the system of economic security of the enterprise is formed, which makes it possible to identify and identify the impact of the use of digital technologies of general purpose, innovative digital technologies for managing the provision of functional activities and directly digital technologies used in ensuring the economic security of the enterprise, general and integrated use which makes it possible to manage the economic security system at the modern digital level and ensure the appropriate level of economic security of the enterprise in the face of new digital challenges and threats.

The practical significance of the results of the dissertation research lies in the use of its scientific provisions, conclusions and achievements in scientific and research activities, as well as in the process of managing the system of economic security of the enterprise on the basis of innovative digital technologies.

Keywords: *management, economic security, security, enterprise economic security system, economic security system management, innovative digital technologies, innovations, strategy, management mechanism, artificial intelligence technologies, blockchain technologies, risks, threats, crisis conditions, innovation activity, innovative development*

**Список публікацій здобувача,
в яких опубліковані основні наукові результати дисертації:**

1. Ситнік Є. Концептуальні засади та наукові підходи до розуміння поняття сутності економічної безпеки підприємства. *Вчені записки Університету «КРОК»*. 2024. № 4 (76). С. 249-255. <https://doi.org/10.31732/2663-2209-2024-76-249-255> (0,8 д. а).
2. Ситнік Є. Теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства. *Вчені записки Університету «КРОК»*. 2025. № 1(77). С. 371-378. <https://doi.org/10.31732/2663-2209-2025-77-371-378> (1 д. а).
3. Ситнік Є. Науково-практичні аспекти розбудови та управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій. *Вчені записки Університету «КРОК»*. 2025. № 2(78). С. 390-397. <https://doi.org/10.31732/2663-2209-2025-78-390-397> (1 д. а).
4. Ситнік Є. Аналіз та ідентифікація показників впровадження цифрових технологій в забезпеченні економічної безпеки підприємств. *Вчені записки Університету «КРОК»*. 2025. №3(79). С. 351-359. <https://doi.org/10.31732/2663-2209-2025-79-351-359> (1 д. а).
5. Ситнік Є. Обґрунтування стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій. *Сталий розвиток економіки*. 2025. № 56. С. 302-306. <https://doi.org/10.32782/2308-1988/2025-56-41> (0,7 д. а).

які засвідчують апробацію матеріалів дисертації:

6. Ситнік Є.І. Сутність та наукові підходи до визначення поняття економічної безпеки підприємства. Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2024: тези доповідей науково-практичної конференції (квітень, 2024 р.). Київ: Університет "КРОК", 2024. <https://conf.krok.edu.ua/MMO/MMO-2024/paper/view/2127> (0,25 д. а).

7. Ситнік Є.І. Наукові підходи до розбудови системи економічної безпеки підприємства. Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку- 2024: тези доповідей науково-практичної конференції (грудень, 2024 р.). Київ: Університет "КРОК", 2024. <https://conf.krok.edu.ua/SRE/SRE-2024/paper/view/2362> (0,25 д. а).

8. Ситнік Є. І. Поняття цифрової безпеки як складової економічної безпеки підприємства. Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2025: тези доповідей міжнародної науково-практичної конференції (квітень, 2025 р.). Київ: Університет "КРОК", 2025. <https://conf.krok.edu.ua/MMO/MMO-2025/paper/view/2851> (0,25 д. а).

9. Ситнік Є.І. Впровадження інноваційних цифрових технологій в забезпеченні економічної безпеки підприємства. Economics, accounting, finance and management: strategic priorities for development in the context of globalization: тези доповідей Міжнародної науково-практичної конференції (березень, 2025 р.). Tampere, Finlan, 2025. С. 21-23. <https://www.economics.in.ua/2025/03/21-2025.html> (0,25 д. а).

10. Ситнік Є.І. Показники використання цифрових технологій в забезпеченні економічної безпеки підприємств. Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку- 2025: тези доповідей науково-практичної конференції (грудень, 2025 р.). Київ: Університет "КРОК", 2025. <https://conf.krok.edu.ua/SRE/SRE-2025/paper/view/3169> (0,25 д.а.).

11. Ситнік Є.І. Впровадження управління системою економічної безпеки підприємства та основі інноваційних цифрових технологій. Національна економіка в умовах війни: безпека та розвиток: тези Всеукраїнської науково-практичної конференції (листопад, 2025 р.). Львів: Львівський державний університет внутрішніх справ, 2025. С. 407-410. (0,25 д.а.).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	16
ВСТУП.....	17
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА.....	29
1.1. Концептуально-методичні засади управління системою економічної безпеки підприємства.....	29
1.2. Сучасні наукові концепти в дослідженні сутності цифрових технологій та їх впровадження в управлінні.....	50
1.3. Теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства....	74
Висновки до розділу 1	94
РОЗДІЛ 2. ХАРАКТЕРИСТИКА СТАНУ ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА.....	97
2.1. Аналіз стану впровадження інноваційних цифрових технологій в діяльності підприємств.....	97
2.2. Показники впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.....	126
2.3. Оцінка процесів впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства....	153
Висновки до розділу 2	169
РОЗДІЛ 3. УДОСКОНАЛЕННЯ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ ІННОВАЦІЙНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ.....	174
3.1. Розбудова системи економічної безпеки підприємства на основі інноваційних цифрових технологій.....	174

3.2. Розробка стратегії управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.....	198
3.3. Формування механізму управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.....	216
Висновки до розділу 3.....	236
ВИСНОВКИ.....	241
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	245
ДОДАТКИ.....	271

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ERP – системи управління ресурсами
CRM – системи управління взаємовідносинами з клієнтами
MES – системи управління виробництвом
WMS – системи інтелектуального управління складами
4ПР – Четверта промислова революція
АС – автоматизовані системи
ВВП – валовий внутрішній продукт
ВДВ – валова додана вартість
ВЕФ – Всесвітній економічний форум
ВНП – валовий національний продукт
ГІІ – Глобальний індекс інновацій (Global Innovation Index)
ДКР – дослідно-конструкторські роботи
ДТР – дослідно-технічні роботи
ДЦНТП – державні цільові наукові та науково-технічні програми
ЕБ – економічна безпека
ЕБП – економічна безпека підприємства
ЄС – Європейський Союз
ІКТ – інформаційно-комунікаційні технології
ІНТ – інтерактивні технології
ІТ – інформаційні технології
НВО – науково-виробниче об'єднання
НДДКР – науково-дослідні та дослідно-конструкторські роботи
НДІ – науково-дослідні інститути
НІС – Національна інноваційна система
НТП – науково-технічний прогрес
ІІ – штучний інтелект

ВСТУП

Актуальність теми. В сучасних економічних умовах невизначеності, значного впливу зовнішніх негативних факторів, забезпечення високої ефективності діяльності та стійкості економічної системи підприємства є одним із першочергових завдань управління. Вирішення цього складного завдання та організація активної протидії зовнішнім дестабілізуючим впливам вирішується завдяки формуванню та зміцненню системи економічної безпеки підприємства. Недосконалість існуючих структур, наявність значних недоліків в плануванні та реалізації управлінських дій значно послаблюють захист підприємств та їх можливість протидіяти внутрішнім та зовнішнім загрозам. Саме тому розбудова системи економічної безпеки підприємства є одним із важливих сучасних напрямів управління, здатних забезпечити не лише ефективне функціонування самих суб'єктів господарювання, а й виступає чинником сталого розвитку загалом. За цих умов, дослідження теоретично-методичних засад управління системою економічної безпеки підприємства набуває важливого пріоритетного значення.

Водночас, стрімкий динамічний розвиток технологій сучасної інформаційної економіки та впровадження нових цифрових інновацій призводить до значних трансформацій, змін економічного та суспільного життя і здійснює значний вплив на всі сфери функціонування. Нові цифрові технології є каталізатором та рушійною силою цих змін, внаслідок яких змінюються операції, процеси, системи, змінюється як сама сутність, зміст, так і вектори суспільно-економічного розвитку. Проте, впровадження нових цифрових технологій не лише забезпечує та оптимізує діяльність, воно може супроводжуватись новими викликами, загрозами та ризиками, реалізація яких негативно впливатиме на все подальше функціонування підприємства. Саме тому в умовах цифровізації проблеми належного рівня забезпечення економічної безпеки є принципово важливими та актуальними.

Питання сутності та значення застосування цифрових технологій широко досліджується в працях багатьох провідних науковців сучасності. Передусім, це пов'язано з високою актуальністю та розумінням зростаючої ваги та значення цих технологій в процесах функціонування як кожного підприємства зокрема, так і мезо та макроекономічних систем загалом. Цифровізація, впровадження цифрових технологій сьогодні стосується всіх сфер функціонування, в тому числі і сфери економічної безпеки. Це пов'язано із широким використанням цифрових технологій в техніко-технологічному, інформаційному забезпеченні економічної безпеки підприємства як нових інноваційних, так і в використанні традиційних технічних засобів. При цьому, фахівці зазначають переваги та високу ефективність використання інноваційних технологій в забезпеченні економічної безпеки і це передусім пов'язано із можливістю зменшення економічних витрат і водночас зростання надійності та ефективності забезпечення безпеки.

Загальна проблематика та окремі теоретично-методичні засади, механізми та моделі управління системою економічної безпеки підприємств на основі інноваційних цифрових технологій широко досліджували у своїх наукових доробках провідні науковці: В. Айзексон, В. Алькема, О. Ареф'єв, Б. Андрушків, І. Белоусова, Т. Васильців, З. Варналій, Н. Ващенко, З. Гбур, Л. Гнилицька, Н. Гуржій, В. Дикань, Л. Донець, Г. Долматова, З. Живко, Т. Іванюта, О. Ілляшенко, А. Заїчковський, О. Захаров, Н. Зачосова, К. Єфремова, М. Єрмошенко, М. Камлик, В. Кириленко, О. Кириченко, І. Керницький, Г. Козаченко, М. Копитко, І. Комарницький, Н. Краус, О. Лященко, І. Мігус, І. Назаренко, Н. Негропonte, В. Ортинський, Л. Омелянович, О. Пищуліна, В. Пономарьов, В. Прохорова, Л. Птащенко, Н. Реверчук, Т. Тарпсot, В. Франчук, М. Фоміна, І. Хома, О. Черевко, Л. Шемаєва, О. Шнипко та інші науковці.

З огляду на актуальність цього напряму досліджень було сформульовано **наукове завдання**, суть якого полягає у обґрунтуванні теоретико-методичних засад та розробці науково-практичних рекомендацій управління системою

економічної безпеки підприємства на основі інноваційних цифрових технологій.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційну роботу виконано у відповідності з планом науково-дослідних робіт ВНЗ «Університет економіки та права «КРОК», а саме: НДР «Науково-методичні засади реалізації сучасних концепцій та технологій управління підприємствами, установами та організаціями в умовах економічного відновлення і глобалізованого розвитку» (номер державної реєстрації 0122U201378) де автором систематизовано сучасні наукові концепти в дослідженні сутності та впровадження цифрових технологій в управлінні; досліджено теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та визначено сутність інформаційно-цифрової складової системи економічної безпеки підприємства; обґрунтовано структуру, елементи та визначено складові системи економічної безпеки підприємства розбудованої на основі інноваційних цифрових технологій.

Мета і завдання дослідження. Метою дисертаційної роботи є обґрунтування теоретико-методичних засад та розробка науково-практичних рекомендацій з управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Досягнення поставленої мети зумовило необхідність вирішення таких завдань:

- дослідити концептуально-методичні засади управління системою економічної безпеки підприємства;
- систематизувати сучасні наукові концепти в дослідженні сутності цифрових технологій та особливостей їх впровадження в управління;
- дослідити теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки та визначити сутність інформаційно-цифрової складової системи економічної безпеки підприємства;

- провести аналіз та сформулювати проєкцію впливу впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства;
- ідентифікувати та систематизувати показники впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства;
- розробити модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства;
- обґрунтувати структуру, елементи та визначити складові системи економічної безпеки підприємства на основі інноваційних цифрових технологій;
- розробити стратегію управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій;
- сформулювати механізм управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Об’єктом дослідження є процес управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Предметом дослідження є теоретико-методичні та науково-практичні засади, стратегії, методи, механізми, моделі управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Методи дослідження. Для досягнення визначеної мети та виконання поставлених завдань щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій у дисертації було використано низку наукових підходів, загальнонаукових та і спеціальних методів наукового пізнання. Зокрема, захисний, стійкісний, гармонізаційний, адаптивний, конкурентний, підхід з позицій реалізації власних стратегічних економічних інтересів, комплементарний та комплексний наукові підходи до розуміння поняття економічної безпеки підприємства; системний, цільовий, процесний, структурний, комплексний, функціональний та ситуаційний

наукові підходи до розуміння системи економічної безпеки підприємства; *ресурсно-функціональний, програмно-цільовий, ситуаційний, стратегічний, системний та інституційний підходи* до управління системою економічної безпеки підприємства (п. 1.1); обґрунтовано новий *технологічний підхід* до управління системою економічної безпеки підприємства (п. 1.1.); *процесний та функціональний, проектний підходи* до впровадження цифрових технологій в управлінні підприємством (п. 1.2.); *системний, структурний, комплексний підходи* до дослідження теоретичних основ впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства (п. 1.3); *методи спостереження, порівняння, узагальнення, аналізу, синтезу, статистичний аналіз* для дослідження стану впровадження інноваційних цифрових технологій в діяльності підприємств, *ідентифікації та структурування* показників впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства (п. 2.1., 2.2.); *системний, динамічний наукові підходи та формування проєкції* впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства (п. 2.1); *методи спостереження, опитування, експертний аналіз, моделювання, індексний аналіз* для розробки моделі комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства (п. 2.3); *системний, структурний, комплексний, функціональний, процесний підходи* до обґрунтування структури, елементів, складових системи економічної безпеки підприємства розбудованої на основі інноваційних цифрових технологій (п. 3.1); *стратегічний, системний підходи* до розроблення стратегії управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій (п. 3.2); *адміністративно-розпорядчі, економічні, соціально-психологічні методи, техніко-технологічні методи та технології* для формування механізму управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій (п. 3.3).

Інформаційною основою дисертаційної роботи є державні

нормативно-правові акти України, інформація Державної служби статистики України, праці провідних учених за напрямком наукового дослідження, інформація та матеріали мережі Інтернет.

Наукова новизна одержаних результатів полягає у розробці й обґрунтуванні теоретико-методичних засад та напрацюванні науково-практичних рекомендацій щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Основні положення, які характеризують наукову новизну дисертаційного дослідження, полягають у такому:

вперше:

- розроблено модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, що передбачає оцінювання на трьох рівнях: рівні загальних процесів функціонування, рівні окремих бізнес-процесів діяльності та в забезпеченні економічної безпеки підприємства. Крім того модель передбачає комплексне оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки, що забезпечує нові можливості для проведення аналізу, оцінювання та отримання об'єктивних комплексних даних щодо стану та рівня впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та дозволяє впровадити моніторинг та виявити слабкі місця, недоліки, спланувати своєчасні заходи з метою зростання рівня цифрової безпеки та ефективності підприємства у протидії ризикам та загрозам в умовах сучасної цифрової трансформації, зростання рівня кіберзагроз зовнішнього середовища;

- розроблено стратегію управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій, яка включає реалізацію стратегічних та оперативних цілей за ключовими напрямками та передбачає цифровізацію процесів здійснення управлінської, операційної, безпекової діяльності підприємства завдяки впровадженню і використанню

інноваційних цифрових технологій і дає можливість удосконалити процеси управління, здійснювати розбудову і функціонування системи та механізму управління економічною безпекою підприємства на сучасному техніко-технологічному рівні, відповідно до вимог та викликів цифрового, техніко-технологічного, ринкового середовищ і забезпечує можливості протидіяти ризикам, загрозам, забезпечувати безпеку, конкурентоспроможність, стійкість і ефективний розвиток підприємства;

удосконалено:

– структуру, елементи та визначено правову, фінансову, кадрову, інтелектуальну, виробничо-операційну, матеріально-майнову, техніко-технологічну, інноваційно-інвестиційну, інформаційно-цифрову, інтерфейсну, ринкову, фізичну складові системи економічної безпеки, цифровізація якої, на відміну від існуючих, дає можливість автоматизувати, оптимізувати процеси управління, зменшити витрати, забезпечити зростання ефективності та результативності у всіх функціональних сферах діяльності підприємства, як єдиної цілісної системи і таким чином досягнути зростання рівня стабільності, надійності економічної безпеки підприємства;

– механізм управління системою економічної безпеки підприємства на основі впровадження інноваційних цифрових технологій, який виступає сукупністю елементів, і на відміну від існуючих, забезпечує комплекс дій з розробки та реалізації планів і заходів відповідно до прийнятої стратегії забезпечення економічної безпеки та організації контролю за їх виконанням відповідно до прийнятих стандартів, норм виконання робіт з застосуванням адміністративно-організаційних, оперативно-розпорядчих, економічних, соціально-психологічних, техніко-технологічних методів та їх інструментів, що дає можливість забезпечувати стійкість та формує умови для подальшого ефективного розвитку підприємства завдяки впровадженню інновацій, передових інноваційних цифрових технологій у всіх сферах діяльності та в системі економічної безпеки; забезпечує захист підприємства від внутрішніх

та зовнішніх небезпек, загроз; забезпечує утримання ринкових позицій, зростання конкурентоспроможності та подальший розвиток підприємства;

– концептуально-методичні засади управління системою економічної безпеки підприємства та виявлено дію наукових підходів трьох рівнів: (1) наукових підходів до розуміння поняття економічної безпеки; (2) наукових підходів до розуміння системи економічної безпеки; (3) підходів до управління системою економічної безпеки підприємства, та на відміну від існуючих, обгрунтовано новий технологічний підхід до розуміння управління системою економічної безпеки підприємства як сукупності підсистем, складових та елементів, взаємодія яких реалізується із застосуванням сучасних цифрових технологічних засобів, що забезпечує ефективне функціонування механізму системи безпеки та застосування методів, інструментів, технологій управління; найбільш оптимальне раціональне використання її кадрових, фінансових, матеріальних ресурсів та зростання рівня безпеки підприємства завдяки широкому використанню технологічних можливостей і зростанню ролі та значення інформаційно-аналітичного забезпечення в прийнятті управлінських рішень;

– ідентифікацію та систематизацію трьох груп показників: цифровізації загальних процесів функціонування підприємства; показників впровадження цифрових технологій для управління бізнес-процесами діяльності; показників впровадження цифрових технологій в забезпеченні економічної безпеки до складу яких віднесено п'ятдесят два показника системний аналіз яких забезпечує можливості для комплексного дослідження процесів впровадження інноваційних цифрових технологій та на основі отриманих даних здійснення моніторингу та подальшого всебічного системного оцінювання процесів управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій;

набули подальшого розвитку:

– систематизація наукових концептів, узагальнення функцій застосування цифрових технологій в управлінні та виявлення дії облікової,

логістичної, безпекової, інформаційно-аналітичної, комунікаційної, операційної, маркетингової функцій, використання яких забезпечує можливість впровадження цифровізації, цифрової трансформації бізнес-процесів у всіх функціональних сферах діяльності підприємства та формування якісно нових комунікацій співпраці і взаємодії з партнерами, стейкхолдерами зовнішнього, глобального середовища, що дасть можливість оптимізувати, зменшити витрати, забезпечити зростання економічної та ринкової ефективності діяльності підприємства;

– теоретичні основи застосування інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та визначено сутність інформаційно-цифрової складової, яка поєднує в собі ознаки та функції інформаційної та цифрової складових, що разом надають технології, інструменти та засоби, мають значно ширші можливості для впровадження ефективного інформаційно-аналітичного забезпечення та формують комплексний дієвий захист підприємства адаптований до протидії реалізації небезпек і загроз зовнішнього ринкового та внутрішнього середовищ в умовах впровадження технологій Четвертої промислової революції, Індустрії 4.0. та нових технологічних викликів і змін;

– аналіз та формування проєкції впливу впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, яка дає можливість виявити та ідентифікувати вплив використання цифрових технологій загального спрямування, інноваційних цифрових технологій функціональної діяльності та безпосередньо цифрових технологій, які використовуються в забезпеченні економічної безпеки підприємства, загальне та комплексне використання яких дає можливість здійснювати управління системою економічної безпеки на сучасному цифровому рівні та забезпечувати належний рівень економічної безпеки підприємства в умовах нових цифрових викликів та загроз.

Практичне значення результатів дисертаційного дослідження полягає у використанні його наукових положень, висновків і здобутків у

науковій та науково-дослідній діяльності, а також в процесі управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Зокрема, висновки та пропозиції, щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій використані у роботі ТОВ "ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНІХРОМ", а саме систематизовані наукові концепти сутності та узагальнені функції застосування цифрових технологій в управлінні; запропоновані підходи до дослідження управління системою економічної безпеки підприємства та аналізу управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій; сформовану проєкцію впливу застосування інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства; розроблену стратегію управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій (довідка № 08/09-04 від 08.09.2025 р.).

Прийнято до уваги такі науково-практичні положення дисертаційної роботи як: обґрунтовану структуру, елементи та визначені складові системи економічної безпеки підприємства розбудованої на основі цифрових технологій, розроблену модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та використано у роботі ТОВ «ЄВРОУКРСІТІГРІН» (довідка № 003/18 від 18.09.2025 р.).

Науково-практичні положення дисертаційної роботи: розроблена модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства; практичні рекомендації щодо формування механізму управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій, розроблені здобувачем підходи до управління системою економічної безпеки та сформовані механізм і інструменти управління

системою економічної безпеки підприємства на основі інноваційних цифрових технологій впроваджені у практичну діяльність з управління системою економічної безпеки ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ ІМ. Є.О. ПАТОНА" НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ (довідка № 07/003/9 від 22.09.2025 р.). Висновки та пропозиції щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій використані під час підготовки аналітичних матеріалів ТОВ «Леві-9 Україна» (довідка № 29/9 від 29.09.2025 р.).

Особистий внесок здобувача. Дисертаційне дослідження є одноосібною науковою працею, у якій здійснено обґрунтування теоретико-методичних засад та розробка науково-практичних рекомендацій щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій. Основні наукові положення, висновки і результати, що є науковим здобутком автора та виносяться на захист, одержані автором особисто.

Апробація результатів дослідження. Основні напрацювання і положення проведених досліджень були апробовані на науково-практичних конференціях, в тому числі міжнародних: «Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2024» (квітень, 2024 р., Київ), «Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку 2024» (грудень, 2024 р., Київ), «Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2025» (квітень, 2025 р., Київ), «Economics, accounting, finance and management: strategic priorities for development in the context of globalization» (березень, 2025 р., Tampere, Finlan), «Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку 2025» (грудень, 2025р., Київ), «Національна економіка в умовах війни: безпека та розвиток» (листопад, 2025 р., Львів).

Публікації. Основні положення та результати дисертаційного

дослідження опубліковані у 11 наукових працях загальним обсягом 6 друк. арк., з яких особисто автору належить 6 друк. арк., у тому числі 5 статей у наукових фахових виданнях України (4,5 друк. арк.), а також 6 публікацій матеріалів участі у науково-практичних конференціях різного рівня (1,5 друк. арк.)

Структура та обсяг роботи. Дисертація складається зі вступу, анотації, трьох розділів, висновків, списку використаних джерел, додатків. Наукову роботу викладено на 288 сторінках, із них 229 сторінок основного тексту. Дисертація містить 15 таблиць, 30 рисунків та 17 сторінок додатків. Список використаних джерел налічує 248 найменувань на 24 сторінках.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Концептуально-методичні засади управління системою економічної безпеки підприємства

В сучасних економічних умовах невизначеності, значного впливу зовнішніх негативних факторів, забезпечення високої ефективності діяльності та стійкості економічної системи підприємства є одним із першочергових завдань управління. Вирішення цих складних завдань та організація активної протидії зовнішнім дестабілізуючим впливам вирішується завдяки формуванню та зміцненню системи економічної безпеки підприємства. Недосконалість існуючих структур, наявність значних недоліків в плануванні та реалізації управлінських дій значно послаблюють захист підприємств та їх можливість протидіяти внутрішнім та зовнішнім загрозам. Саме тому розбудова системи економічної безпеки підприємства є одним із важливих сучасних напрямів управління, здатних забезпечити не лише ефективне функціонування самих суб'єктів господарювання, а й виступає чинником сталого розвитку загалом. За цих умов дослідження теоретично-методичних засад управління системою економічної безпеки підприємства набуває важливого пріоритетного значення.

Розпочинати дослідження в цьому напрямі доцільно безпосередньо із розгляду самого поняття безпеки та наукових підходів до розуміння, визначення його сутності і значення.

Грунтовний аналіз праць провідних вітчизняних науковців щодо бачення та розуміння змісту та сутності поняття економічної безпеки свідчить про значні відмінності, широту та різноманітність наукових підходів.

Одним із перших наукових підходів до дослідження та розуміння економічної безпеки був захисний підхід, представлений в працях Л. Омелянович та Г. Долматової. За цим підходом економічна безпека

підприємства трактується як стан його захищеності від впливу небезпек та загроз, негативної дії внутрішніх і зовнішніх негативних чинників та факторів. Водночас, на думку авторів, забезпечення економічної безпеки гарантує підприємствам стабільність функціонування, ефективний розвиток та відтворення, впровадження та використання здобутків науково-технічного прогресу, інновацій [1, с. 46]. В цілому, погоджуючись з авторами щодо першочергового пріоритетного значення безпеки в питаннях захисту від негативного впливу зовнішніх загроз та небезпек, зазначимо, що ефективний розвиток, відтворення та впровадження інновацій є результатами планування та впровадження комплексу управлінських дій, в якому захисний підхід є лише складником в сукупності інших необхідних підходів до прийняття і реалізації ефективних обґрунтованих управлінських рішень.

У працях І. Хома економічна безпека суб'єкта господарювання є економічним явищем чи властивістю, що виникає завдяки відсутності реалізації небезпек, загроз та упередженні впливу зовнішніх та внутрішніх негативних факторів на стан підприємства, здійснення його фінансово-економічної діяльності та його економічний потенціал [2, с. 21]. Таким чином, автором наголошується на необхідності досягнення рівня захищеності, яка є результатом ефективності економічної безпеки підприємства.

Іншим провідним науковцем Н. Реверчук зазначалося, що економічна безпека підприємства є системою, яка забезпечує активний захист суб'єкта господарювання від фінансових, матеріальних та людських втрат завдяки впровадженню превентивних попереджуючих дій, що можуть запобігти реалізації негативних подій та нанесенню підприємству збитків [3, с. 21]. Відповідно, мова йде про активний захист заснований на розробці та впровадженні превентивних дій та заходів, і таким чином стає актуальним питання системності аналізу та оцінювання, моніторингу ризиків, загроз, що є необхідним для розробки та цільового впровадження таких превентивних дій та заходів.

У дослідженнях науковців економічна безпека є категорією захищеності суб'єктів на всіх рівнях, а основою такого захисту виступають механізми забезпечення та безперервного розвитку завдяки ефективному застосуванню всіх наявних ресурсів та можливостей у здійсненні підприємницької діяльності [4]. Таким чином, захисний підхід в дослідженнях цього науковця поєднано із ресурсним підходом, а самі можливості та забезпечення захисту ґрунтуються на ресурсному потенціалі підприємства, що може бути спрямованим на забезпечення безпеки.

На думку В. Дикань та І. Назаренко економічна безпека є станом захищеності функціонування підприємства від загроз внутрішніх та зовнішніх, за якого функціонування підприємства є стабільним, а ефективне використання наявних ресурсів та адаптованість до дестабілізуючих впливів економічного середовища забезпечує стабільний майбутній розвиток [5, с. 72]. Представлене науковцями бачення значно розширює межі розуміння економічної безпеки з позицій захисного підходу, акцентує увагу на важливості наявності та використання ресурсів, як основи безпеки та значенні своєчасної та відповідної адаптації до змін економічної кон'юнктури, що свідчить про ознаки застосування авторами ресурсного та адаптаційного підходів.

У дослідженнях М. Копитко економічна безпека підприємства є поняттям комплексним. Вона визначає стан та здатність суб'єкта господарювання до ефективної організації роботи з протидії негативному впливу дестабілізуючих внутрішніх і зовнішніх факторів, можливості швидкого та ефективного адаптування до змін з найменш можливими втратами [6, с. 59]. Повністю погоджуючись із думкою цієї авторки зазначимо, що в її працях представлено як захисний так і комплексний підходи до розуміння сутності та значення економічної безпеки та обґрунтування і впровадження комплексності дій, спрямованих на розбудову систем безпеки, створення безпечного функціонування підприємства загалом.

Науковець Л. Шемаєва визначає економічну безпеку як здатність підприємства реалізувати визначені стратегічні інтереси в економічній сфері в існуючих ринкових зовнішніх умовах, завдяки використанню цих зовнішніх умов на користь підприємства та забезпечуючи його належний захист [7, с. 12]. Автором наголошується на якостях і характеристиках самого підприємства у його здатності протидіяти зовнішнім факторам, водночас в дослідженнях проявляється розуміння безпеки через реалізацію стратегічних економічних інтересів, що свідчить про ознаки розуміння безпеки з позицій реалізації власних економічних інтересів та просування власної стратегії підприємства.

Узагальнюючи зазначимо, що підхід з позицій захисту інтересів від зовнішніх і внутрішніх негативних впливів, факторів з використанням його ресурсного потенціалу і можливостей є одним із найбільш поширених внаслідок того, що за своєю суттю головною функцією забезпечення безпеки і є безпосередньо захист. Проте, в сучасних умовах економічна безпека має значно ширше розуміння, передумови та складові забезпечення, саме тому захисний підхід в значній частині наукових праць представлено в поєднанні з іншими науковими підходами, на засадах яких науковці будують своє бачення забезпечення безпеки підприємства.

Одним із поширених наукових підходів до дослідження економічної безпеки підприємства є стійкісний підхід, який визначає економічну безпеку як можливість до забезпечення рівноваги і стійкості економічної системи підприємства, що може бути отримано завдяки ефективному використанню ресурсів підприємства, його гнучкості і адаптивності, ринкових можливостей, та більш ефективного використання інструментів управління [8]. Таким чином, за стійкісним підходом економічна безпека визначається як здатність до забезпечення стійкого сталого функціонування в умовах негативної дії внутрішніх, зовнішніх факторів та змін. Втім, на практиці забезпечення стійкості є більш комплексним та складним завданням, ніж безпосереднє забезпечення захисту від загроз чи ефективного використання ресурсів, оскільки за цим підходом економічної безпеки виступає не якістю чи

процесом, а наслідком ефективних комплексних дій, що забезпечують не лише дієвий захист, а й ефективність функціонування фінансово-економічної, виробничої та операційної систем підприємства. Проте, на нашу думку саме стійкісний підхід найбільш повно відображає сутність та значення економічної безпеки сучасного підприємства та є основою формування та функціонування його системи економічної безпеки.

У дослідженнях І. Білоусової економічна безпека підприємства визначається як збалансований безперервний сталий розвиток, що є результатом найбільш ефективного використання ресурсів та сприятливих факторів підприємницької діяльності [9, с. 17]. На думку автора найбільш ефективне використання ресурсів та підприємницьких можливостей забезпечує змогу досягнути тривалого стійкого функціонування та динамічного науково-технічного і соціального розвитку та ефективної протидії зовнішнім загрозам і ризикам в існуючих умовах та в майбутньому. Таким чином, безпека невід'ємно пов'язана з розвитком, є його основою і водночас результатами цього розвитку. Це розкриває багатогранність, багатоаспектність, комплексність такого поняття як економічна безпека її взаємозв'язок з іншими базовими поняттями, таким як інновації, науково-технічний прогрес та інші.

На думку Б. Андрушківа економічна безпека виступає економічним станом підприємства, що визначається сталістю до впливу внутрішніх та зовнішніх змін, які відбуваються в операційній, фінансовій, господарській діяльності підприємства завдяки формуванню умов, що забезпечують ефективний захист підприємств від реалізації небезпек та ризиків [10, с. 23]. По суті, мова йде про захист економічних інтересів підприємства та формування на підприємстві умов, за яких цей захист буде ефективно забезпечений.

Науковцями М. Єрмошенко, К. Горячовою економічна безпека суб'єкта господарювання визначається як збалансований стан його економічної системи, що є стійким до негативного впливу небезпек, загроз та здатний

забезпечити ефективний сталий розвиток завдяки реалізації підприємством його економічних інтересів [11, с. 23]. На нашу думку, в працях цих науковців економічна безпека має значно вагомішу роль та значення, адже вона виступає невід'ємною складовою та умовою сталого розвитку, а сам сталий розвиток є результатом збалансованого стійкого стану його економічної системи. Таким чином, простежується взаємозалежність та взаємозв'язок між безпекою, розвитком, збалансуванням, стійкістю економічних систем, що є важливим для розуміння розбудови та функціонування систем економічної безпеки підприємства, її ролі та значенні в загальній економічній системі підприємства.

Загалом стійкісний підхід до розуміння сутності економічної безпеки засновано на можливості суб'єктів господарювання забезпечувати безперервний розвиток, незважаючи на зміни умов функціонування та вплив дестабілізуючих факторів. Проте, економічна безпека характеризується не лише стійкістю, а досягнення підприємством стану економічної стійкості залежить не лише від забезпечення економічної безпеки, а в першу чергу від результатів його фінансово-господарської діяльності та якості управління капіталом, фінансовими ресурсами та активами підприємства, успішністю його інвестиційно-інноваційної діяльності.

Одним із найбільш поширених в наукових працях підходів до розуміння сутності економічної безпеки є ресурсний та ресурсно-функціональний підходи. Ресурсний підхід загалом заснований на баченні визначення ресурсів підприємства як основи забезпечення його економічної безпеки. Передусім, таке бачення пов'язано із тим, що фінансові, кадрові, матеріальні, технологічні, інформаційні ресурси загалом визначають можливості здійснення підприємством своєї фінансово-господарської діяльності та її масштабів без залучення зовнішніх учасників та джерел фінансування. Це, в свою чергу, зменшує ризики і забезпечує більшу автономність підприємств, мобільність, активність у можливостях реагування на зовнішні та внутрішні зміни, в тому числі на вплив дестабілізуючих факторів та ризиків. Водночас,

достатність власних в першу чергу фінансових та інших ресурсів зменшує ризики та дає можливість керівникам приймати рішення в сфері власної фінансово-господарської діяльності в межах допустимих ризиків, без переходу в зону критичних ризиків, оскільки керівники, приймаючи інвестиційні чи управлінські рішення ризикують виключно власним капіталом підприємств, а не зовнішніми запозиченими чи залученими ресурсами.

Так, у працях В. Кириленко економічна безпека підприємства визначається як стан його корпоративних ресурсів, що дає підприємству можливості реалізувати його поставлені цілі та захищає від загроз і ризиків конкурентного ринкового середовища [12, с. 18-19]. Таким чином, автор акцентує увагу на важливості достатності корпоративних ресурсів та їх ефективного використання, що забезпечує можливості до реалізації ризиків і тим самим забезпечує необхідний для функціонування підприємства в існуючих ринкових умовах рівень економічної безпеки.

На думку М. Фоміної найбільш ефективне використання ресурсів підприємства здатне суттєво знизити ризики та загрози в його діяльності, як в безпосередньому функціонуванні, так і в перспективах майбутнього розвитку і таким чином забезпечити його безпеку та стабільність [13, с. 11]. Зазначимо, що здатність забезпечення підприємства кадровими, матеріальними, фінансовими та іншими видами ресурсів, необхідних для його роботи та їх ефективне використання загалом формує основу для стабільної роботи будь-якої організації, проте це дає можливість охопити лише внутрішнє середовище організації, тоді як на підприємство впливає значна кількість різних за джерелами виникнення та інтенсивності дії зовнішніх чинників.

У дослідженнях Ю. Бровкіної представлено ресурсно-функціональний підхід, що являє собою трансформацію ресурсного підходу та його поєднання з функціональним [14]. Таким чином, ресурсно-функціональний підхід цієї дослідниці є комплексним баченням, а його об'єктами є функціональні складові - такі як фінансова, виробнича, інформаційна, кадрова, збутова, техніко-технологічна та інші функціональні складові економічної безпеки

підприємства та їх забезпечення відповідними і необхідними для ефективного функціонування ресурсами. Проте, як вже зазначалося, ресурсний підхід зосереджений на внутрішньому середовищі, наявності та ефективності використання цих ресурсів, але це не применшує вагу та значення зовнішнього середовища підприємства як джерела отримання ним всіх вище зазначених ресурсів задля функціонування відповідних функціональних сфер складових його діяльності.

У дослідженнях А. Єпіфанова, О. Пластуна, В. Домбровського акцентується увага на важливості та знаннях найбільш оптимізованого та ефективного використання ресурсів, впровадження сукупності дій та заходів дієвого фінансового контролю здатного виявити та діагностувати негативні чинники внутрішнього та зовнішнього характеру, які здатні погіршити стан використання цих ресурсів та ефективність роботи підприємства загалом [15, с. 25]. Відповідно, на думку цих авторів економічна безпека та її забезпечення невід'ємно пов'язані з необхідністю впровадження та використання фінансового контролю, адже саме цей контроль здатен оптимізувати, забезпечити більш раціональне використання ресурсів, а системність впровадження таких контрольних заходів здатна запобігти реалізації ризиків в управлінні ресурсами.

Одним із найбільш поширених методологічних підходів до розуміння сутності економічної безпеки в сучасних економічних ринкових умовах є конкурентний підхід. Формування цього підходу пов'язане із активним розвитком підприємництва, малого та середнього бізнесу, значною динамікою ринкових змін, зростанням конкуренції на внутрішньому та зовнішніх ринках і відповідно активуванням та збільшенням загроз зовнішнього ринкового середовища із цим пов'язаних.

Так, у дослідженнях Т. Васильціва зазначається, що в умовах сучасності стабільність діяльності підприємства може бути досягнута завдяки зростанню рівня його конкурентоспроможності. Таким чином, економічна безпека визначається як стан функціонування суб'єкта господарювання, за якого

випущена і реалізована ним продукція та послуги є конкурентними на ринку та за умов найбільш раціонального та ефективного використання всіх його ресурсів забезпечення стійкого прогресивного розвитку [16, с. 18]. На нашу думку, визначення цього автора є одним із найбільш повних, ґрунтовних та комплексних бачень сутності економічної безпеки як з позицій конкурентного підходу, так і одночасно з позицій ресурсного, стійкісного підходів, що дає можливість виявити та узагальнити основні складові забезпечення безпеки підприємства в протидії внутрішнім та зовнішнім загрозам, ризикам, що здійснюють безпосередній вплив на діяльність підприємств в сучасних умовах.

Зазначимо, що конкурентний підхід до дослідження економічної безпеки є дуже важливим, оскільки отримання підприємством ринкових переваг в умовах значної конкуренції та динамічних змін які відбуваються на сучасних ринках, є важливою умовою стабільного функціонування та відкривають можливості для подальшого розширення діяльності, розвитку підприємства, що відповідно свідчитиме про надійний рівень та зростання забезпечення їх економічної безпеки.

Наступним важливим методичним підходом до розуміння сутності та значення економічної безпеки представлених у працях провідних науковців є гармонізаційний підхід.

Гармонізаційний підхід представлено та обґрунтовано у працях Г. Козаченко, В. Пономарьова, О. Ляшенко. За гармонізаційним підходом економічна безпека підприємства визначається як міра гармонізації економічних інтересів підприємства та інтересами суб'єктів-партнерів зовнішнього середовища [17, с. 87]. Таким чином, економічні інтереси суб'єктів мають бути узгоджені в часі та просторі. Отже, за гармонізаційним підходом вплив партнерів зовнішнього середовища, що мають власні економічні інтереси має бути гармонізований, тобто взаємоузгоджений з економічними інтересами самого підприємства. Зазначимо, що з практичної точки зору відсутність необхідної гармонізації може призвести до появи та

загострення протистояння, конфліктів з контрагентами зовнішнього середовища, а їх дії можуть становити значні загрози та небезпеки для діяльності підприємства, його економічної безпеки. Проте, незважаючи на очевидний факт важливості та значення такого підходу з позицій теоретично-методичних, досягнути такої гармонізації та рівноваги на практиці є завданням складним та багатоаспектним.

Водночас, важливість гармонізаційного підходу полягає у його представленні зовнішнього середовища не лише як осередку появи та дії ризиків і загроз для діяльності суб'єктів господарювання, а як середовища потенційних ринкових можливостей, що здатні зміцнити фінансово-економічні ринкові позиції підприємства та забезпечити зростання його стабільності і рівня економічної безпеки за умов знаходження спільних інтересів, ефективного партнерства та взаємодії з контрагентами зовнішнього середовища.

У дослідженнях Л. Корчевської, А. Деменської економічна безпека є мірою гармонізації економічних інтересів підприємства з інтересами інших ринкових контрагентів, партнерів, яка може бути досягнутою з метою захисту від економічних небезпек та загроз завдяки застосуванню відповідних організаційних, фінансових, соціально-психологічних заходів [18]. Слід зазначити, що таким чином авторами надаються цілком конкретні напрями заходів та дій з забезпечення економічної безпеки підприємства, здатні забезпечити таку гармонізацію.

У працях І. Зайцева наголошується на тому, що така гармонізація передбачає узгодженість в часі та просторі інтересів менеджерів та керівників з інтересами партнерів в умовах швидкого оперативного прийняття управлінських рішень із застосуванням ситуаційного підходу [19, с. 16–17]. Зазначимо, що у праці цього автора звертається увага на важливості застосування ситуаційного підходу в мовах здійснення управління за ситуаціями, тоді коли керівникам необхідно приймати швидкі управлінські

рішення, які водночас зможуть враховувати економічні інтереси всіх сторін та учасників, як підприємства так і його партнерів.

В продовженні дослідження гармонізаційного підходу О. Ляшенко було розроблено комплементарний підхід до розуміння сутності економічної безпеки, за яким економічна безпека виступає певною мірою економічної свободи, яку має суб'єкт господарювання завдяки управлінню процесами взаємоузгодження економічних інтересів учасників внутрішнього, зовнішнього середовища задля організації протидії небезпекам та загрозам з використанням потрібних для цього ресурсів [20, с. 23]. Варто зазначити новизну цього наукового підходу та його комплексне охоплення і розуміння тих процесів, що відбуваються в діяльності організації в процесі забезпечення економічної безпеки та необхідністю залучення, взаємодії для забезпечення безпеки підприємства, всіх учасників цих процесів, як самого колективу підприємства так і його партнерів, стейкхолдерів, представників державних організацій і т.д. Проте, загалом досягнення збалансування гармонізації різних, а іноді абсолютно протилежних інтересів учасників є дуже складним завданням, що потребує високого рівня управлінської майстерності та врахування загальної кон'юнктури ринку.

У праці О. Сосновської представлено комплексний підхід до розуміння економічної безпеки підприємства як діяльності, яка спрямована на ефективне використання ресурсів підприємства в різних сферах його функціонування з метою забезпечення його стійкості в умовах динамічних змін зовнішнього та внутрішнього середовища підприємства [21].

Узагальнюючи зазначимо, що застосування захисного, конкурентного, ресурсного, ресурсно-функціонального, комплексного, стійкісного, гармонізаційного та комплементарного наукових підходів до сутності та дослідження дефініції економічної безпеки підприємства дає можливість узагальнити та систематизувати всі умови, аспекти, функціональні складові, напрями спрямування дій, методи та засоби, що мають ключове значення в забезпеченні економічної безпеки підприємства.

Саме визначення розуміння цих наукових підходів формує підґрунтя та до подальшого розуміння та вивчення теоретично-методичних засад формування розбудови системи економічної безпеки підприємства, як сукупності всіх складових та елементів, спрямованих на забезпечення економічної безпеки підприємства з формуванням взаємозв'язків та взаємодії як в межах самого підприємства між його функціональними підсистемами, так і у взаємодії з партнерами зовнішнього середовища.

Забезпечення економічної безпеки підприємства не має здійснюватися вибірково, фрагментарно, як реакція на певні загрози та ризики, що виникають в діяльності підприємства. Її ефективність можлива за умови впровадження системних безперервних дій, професійного управління в сфері економічної безпеки і внаслідок цього залучення та використання ресурсів, формування механізму, впровадження методів, засобів та інструментів забезпечення економічної безпеки підприємства. Таким чином, забезпечення економічної безпеки підприємства потребує формування та розбудови системи економічної безпеки.

Дослідження теоретично-методичних засад формування системи безпеки потребує розгляду дефініції сутності поняття системи економічної безпеки підприємства, наукових підходів та принципів її розбудови і функціонування.

В науковій літературі представлена значна кількість визначення дефініції системи економічної безпеки підприємства, що свідчить про відсутність єдиної точки зору та бачення науковцями цього поняття.

У працях Л. Донець система економічної безпеки визначається як обмежена безліч елементів, що взаємопов'язані між собою, здатних забезпечити досягнення мети та безпеку підприємства [22, с. 51]. При цьому, на думку цього автора, складовими такої системи виступають об'єкт та суб'єкт безпеки, механізми її забезпечення та безпосередньо дії та заходи, спрямовані на забезпечення безпеки. Таким чином, визначено основоположні складові

системи економічної безпеки, такі як суб'єкт, об'єкт, механізми, що формують її структуру і водночас забезпечується її функціонування та управління.

На думку О. Шнипко система економічної безпеки підприємства є сукупністю характеристик, якостей здатних забезпечити її самовиживання в умовах дії небезпек, загроз та розвитку [23, с. 22]. Варто зазначити, що в цьому визначенні акцентується увага на основних властивостях, таких як самовиживання та розвиток, притаманних будь-яким системам загалом і відповідно автором визначається застосування системного підходу до управління безпекою в діяльності підприємства, відзначаються ключові філософсько-методичні аспекти та закономірності функціонування такої системи.

У дослідженнях Т. Слободяник система економічної безпеки підприємства виступає комплексом організаційно-правових заходів та дій, що мають реалізовуватися відповідними службами, підрозділами, органами з метою захисту життєво важливих інтересів людей, суб'єктів господарювання, держави від незаконних дій, які можуть завдати цим підприємствам чи фізичним особам значних втрат, реалізації небезпек та ризиків в майбутньому [24, с. 23]. Повністю погоджуючись з автором зазначимо, що це визначення є одним із найбільш повних та представляє комплексний підхід до розуміння сутності системи економічної безпеки та розкриття необхідності взаємодії з широким колом в першу чергу правових організацій в забезпеченні економічної безпеки підприємства, оскільки така безпека не може бути забезпеченою лише силами та засобами самого підприємства. Крім цього в дослідженнях автора акцентується увага на правових аспектах безпеки, що буде важливо, оскільки ми розглядаємо безпеку не лише з організаційної та управлінської площини, як одну із внутрішніх фінансово-господарської функцій безпеки, але й спираємось на правові аспекти їх забезпечення.

У дослідженнях М. Камлика економічна безпека визначається як стан розвитку суб'єкта господарської діяльності, що має можливості до ефективної протидії реалізації загроз, ризиків, упередження їх негативного впливу та

визначається стабільністю фінансового та економічного функціонування [25, с. 9]. Таким чином, економічна безпека трактується автором як стан розвитку, за якого підприємство має можливості, спроможність ефективно протидіяти негативним чинникам, маючи необхідний та достатній для цього рівень економічної фінансової стабільності.

За визначенням І. Шульги (І. Мігус) система економічної безпеки підприємства є сукупністю економічних відносин суб'єкта господарювання, спрямованих на зменшення впливу зовнішніх та внутрішніх небезпек, загроз та реалізацію визначених стратегічних цілей його діяльності [26, с. 155]. Таким чином, у визначенні цього автора саме функціонування системи економічної безпеки має цільову спрямованість та стратегічні цільові орієнтири.

Досліджуючи складові елементи системи економічної безпеки підприємства Л. Шемаєва зазначає їх як організаційну сукупність суб'єктів зовнішньої та внутрішньої безпеки, а саме органів, служб, наукових підходів, об'єктів, нормативно-правових засад, концепції, стратегії, політики, функцій, принципів, методів та засобів, спрямованих на забезпечення захисту підприємства, реалізацію його стратегічних та тактичних інтересів [27]. З таким повним та всеохоплюючим визначенням можна лише погодитись, оскільки воно найбільш повно розкриває як складові, так і сутність призначення та цільові аспекти розбудови і функціонування системи економічної безпеки підприємства.

Науковиця Н. Зачосова визначає систему економічної безпеки суб'єктів господарювання як сукупність відносин, спрямованих на найбільш оптимальне управління фінансовою, операційною чи інвестиційною діяльністю суб'єкта завдяки упередженню небезпек, загроз та того негативного впливу, який вони здатні здійснювати на їх діяльність задля найбільш ефективного досягнення визначеної мети та цілей, зміцнення потенціалу та забезпечення майбутнього розвитку [28, с. 243]. Варто зазначити, що в цьому розумінні системи економічної безпеки, саме її функціонування невід'ємно пов'язано з процесом управління, оскільки саме

внаслідок управління успішно реалізуються як і захисні функції цієї системи та можливість протидіяти загрозам та ризикам, так і можливість управляти відносинами з партнерами та зміцненням власного економічного ресурсного потенціалу суб'єкта господарювання.

За іншим визначенням Т. Іванюти, А. Заїчковського система економічної безпеки є обмеженою множиною елементів, які маючи взаємозв'язки між собою дають можливість забезпечити безпеку та досягнення визначених підприємством цілей [29, с. 24–25]. Складовими системи, здатними забезпечити реалізацію цих цілей виступають суб'єкт, об'єкт, механізми забезпечення безпеки та прийнята підприємством політика в сфері безпеки. Таким чином, авторами акцентується увага не лише на складових, необхідних для функціонування системи безпеки, а й на необхідності формування та впровадження політики в сфері безпеки.

Науковець В. Прохорова акцентує увагу на єдності економічної безпеки підприємства як цілісної системи, що виступає сукупністю пов'язаних зв'язками елементів, до яких, на думку автора, відносять суб'єкт, об'єкт та механізми управління [30, с. 24–25]. Загалом погоджуючись з автором зазначимо, що не менш важливими для системи економічної безпеки є її організаційна структура та працівники, інформаційне, технічне, фінансове забезпечення, правові засади та інші складові та елементи.

У дослідженнях О. Захарова система економічної безпеки передусім поєднує внутрішніх та зовнішніх суб'єктів, що маючи спільну мету та цілі спрямовують свої зусилля на її забезпечення та мають для цього необхідну матеріально-технічну базу, фахівців, співробітників, механізм управління, з широким колом методів, технологій та засобів забезпечення безпеки [31]. Водночас, важливим є надання цим суб'єктам управління необхідних прав та повноважень, функцій, які давали б їх можливість до ефективного управління і таким чином забезпечували здатність до ефективної протидії небезпекам та загрозам. На нашу думку визначення О. Захарова є одним із найбільш повних комплексних бачень системи економічної безпеки підприємства та її

складових, що спрямовані на практичні можливості, дій та забезпечують ефективність функціонування такої системи.

Праці О. Коробчинського описують систему економічної безпеки як сукупність організаційних, управлінських, технічних, маркетингових та профілактичних дій, засобів, здатних забезпечити захист інтересів підприємства від загроз та небезпек як на самому підприємстві, так і від впливу зовнішніх негативних факторів [32]. Варто зазначити, що автор представляє систему економічної безпеки сформовану з її функціональних складових, що визначають напрями практичних заходів забезпечення безпеки, що на думку автора забезпечуватимуть якісний та кількісний захист інтересів суб'єкта господарювання.

Досліджуючи теоретично-методичні засади управління системою економічної безпеки підприємства слід зазначити, що науковці розуміють його як систему принципів та методів розробки та впровадження управлінських рішень, спрямованих на забезпечення захисту підприємства від зовнішніх та внутрішніх загроз [33; 34; 35]. При цьому основна увага науковців сфокусована на складових управління.

Метою управління системою економічної безпеки підприємства є планування та реалізація дій, здатних забезпечити захист підприємства від небезпеки та ризиків і забезпечити його стабільну та ефективну діяльність. Відповідно до мети завданнями управління системою економічної безпеки науковці зазначають оцінку стану зовнішнього та внутрішнього середовища підприємства, небезпек та загроз його діяльності; виявлення деструктивних тенденцій, потенціальних загроз та ризиків його діяльності; розробку концепції та стратегії забезпечення економічної безпеки підприємства; розбудову та впровадження механізму забезпечення економічної безпеки; розробку заходів спрямованих на протидію захисту підприємства від фактичних та потенційних ризиків, небезпек його діяльності.

На думку С. Ілляшенко та інших науковців управління системою економічної безпеки підприємства повинно відповідати таким загальним

принципам як системність, комплексність, взаємоузгодженість, об'єктивність, універсальність, результативність, адекватність [36]. Зазначимо, що представлені принципи є загальними та відповідно є основами для розбудови та управління системами економічної безпеки для підприємств, що функціонують в різних сферах, галузях економічної діяльності, в різних умовах дії загроз та небезпек зовнішнього ринкового середовища.

На думку Б. Корецького методичними підходами, на засадах яких має здійснюватися управління системою економічної безпеки підприємства [37] є ресурсно-функціональний підхід, відповідно до якого планування та впровадження заходів з управління економічною безпекою підприємства має розроблятися та впроваджуватися з плануванням відповідних обсягів, необхідних для цього ресурсів, а саме управління безпекою, що здійснюватиметься за відповідними функціональними напрямками складовими економічної безпеки підприємства.

Іншим важливим науковим підходом до управління системами економічної безпеки підприємства у працях О. Молодід представлено програмно-цільовий підхід, основою якого є розрахунок низки показників, за якими визначають економічну безпеку [38]. У працях М. Чорної обґрунтовано ситуаційний підхід, який на думку автора дає можливість управляти конкретними ситуаціями, приймаючи найбільш ефективні, відповідно до ситуації, оперативні управлінські рішення [39].

У дослідженнях групи науковців З. Живко, О. Черевко, Н. Зачосової, М. Живко, О. Баворовської, В. Занори представлено системний, програмно-цільовий та інституційний підходи до управління системою економічної безпеки підприємства [40]. Так, застосування програмно-цільового підходу, на думку науковців спрямоване на досягнення масштабних стратегічних цілей, здатних значною мірою змінити, трансформувати підприємство та його економічну систему в майбутньому і пов'язано із реалізацією стратегії економічної безпеки, розробкою та реалізацією підприємством інвестиційно-інноваційних проектів.



Рис. 1.1. Наукові підходи до розуміння економічної безпеки, розбудови та функціонування, управління системою економічної безпеки

Джерело: сформовано автором на основі [41-80]

На рисунку 1.1. представлено наукові підходи до розуміння економічної безпеки, розбудови та функціонування, управління системою економічної безпеки підприємства.

При цьому, як зазначають науковці, зміни які забезпечує впровадження програмно-цільового підходу забезпечуються завдяки одночасному прояву двох типів інтеграції – просторової, яка передбачає об'єднання зусиль всіх учасників процесів забезпечення безпеки та часової, яка передбачає стійку послідовність етапів управління в реалізації запланованих програмних цілей.

За визначенням науковців програмно-цільовий підхід до управління розуміють як реалізацію комплексу запланованих дій та заходів організаційного, економічного та інформаційного характеру, що дає можливість спрямувати діяльність суб'єкта на досягнення визначених цілей [81-83]. При цьому, на процеси управління, на думку науковців, можуть впливати інституціональні фактори, що формують нормативні організаційні засади, що дають можливість сформувати порядок виконання, впровадження запланованих дій, заходів та зменшити невизначеність в процесі дій та взаємодії з контрагентами зовнішнього середовища.

Слід зазначити, що в сучасних умовах цифровізації всіх сфер діяльності людства, і в тому числі розбудови та функціонування самого підприємства, всі процеси та роботи всіх функціональних підсистем підприємства, в тому числі організаційно-управлінських, логістичних, операційно-виробничих маркетингових та безпекових здійснюється та супроводжується використанням сучасних цифрових технологій. Технології виступають засобом виконання задач, заходів, дій з застосуванням програмного забезпечення, техніки, обладнання, приладів та технологій, як техніко-технологічної основи завдяки якій здійснюється діяльність, в тому числі із забезпечення економічної безпеки підприємства. Саме тому інноваційні цифрові технології, комп'ютерна техніка, спеціалізоване програмне забезпечення стали невід'ємною складовою в сучасному розумінні економічної безпеки підприємства.

Це дає підстави до обґрунтування нового технологічного підходу до управління системою економічної безпеки підприємства як сукупності підсистем, складових та елементів, взаємодія яких реалізується із застосуванням сучасних цифрових технологічних засобів та технологій, використання яких забезпечує ефективне функціонування механізму системи безпеки, застосування методів та інструментів управління, найбільш оптимальне раціональне використання її кадрових, фінансових, матеріальних ресурсів, зростання рівня безпеки підприємства завдяки широкому використанню технологічних можливостей та зростанню ролі та значення інформаційно-аналітичного забезпечення системи економічної безпеки підприємства.

Зазначимо, що головною метою розбудови системи економічної безпеки та управління такою системою є попередження проявів небезпек та загроз, розгортання можливих кризових явищ на підприємстві, забезпечення його стабільного, успішного функціонування та ефективного розвитку в майбутньому.

Узагальнюючи наукові концепти та бачення перелічимо перелік завдань, які мають вирішувати системи економічної безпеки підприємства з метою досягнення поставленої мети. Серед таких завдань: інформаційно-аналітична робота пов'язана зі збором та опрацюванням значного обсягу інформації щодо аналізу ситуації, даних та прогнозування майбутніх подій; впровадження моніторингу дій партнерів, конкурентів, інших контрагентів; захист прав та інтересів підприємства, інтелектуальних ресурсів, комерційної таємниці, інформації, захист майна, фінансових ресурсів підприємства, його товарно-матеріальних цінностей; примноження капіталу підприємства; забезпечення конкурентоспроможності підприємства його продукції; забезпечення фінансової стійкості та високої продуктивності, ефективності, діяльності підприємства на ринку; формування організаційної структури, яка повною мірою відповідала б масштабам, потребам підприємства, його цілям в забезпеченні безпеки, а в її складі необхідного за розміром та чисельністю

підрозділу, служби економічної безпеки; забезпечення високого рівня професіоналізму роботи працівників служби безпеки у виконанні покладених на них обов'язків, зростання їхніх знань та компетенцій; цифровізація, удосконалення технологічного забезпечення служб та підрозділів, працівників системи економічної безпеки підприємства та вирішення інших важливих для стабільного функціонування і майбутнього розвитку підприємства завдань та цілей.

Теоретико-методичною основою розбудови та функціонування систем економічної безпеки, крім наукових підходів, виступають принципи, на засадах яких здійснюється їх розбудова та управління.

У працях науковців В. Алькеми [81], О. Данченко [82], Л. Гнилицької [83], В. Ортинського, І. Керницького [84] та ін. представлено наступні принципи розбудови та управління системою економічної безпеки підприємства: системність; цілеспрямованість; компетентність; адаптивність; автономність; конкретність; гнучкість; досяжність; безперервність; емерджентність; відкритість; координованість; єдиноначальність. Ці принципи визначають основні засади формування та функціонування безпекових систем суб'єктів господарювання, проте цей перелік не є вичерпним, оскільки в залежно від виду економічної діяльності, специфіки функціонування та управління цей перелік може доповнюватися специфічними принципами, які відображатимуть особливості діяльності та завдання, які стоять перед системами економічної безпеки конкретних суб'єктів господарської діяльності.

У дослідженнях О. Подра, Г. Левків, М. Копитко визначено низку принципів, на засадах яких базуються та функціонують системи безпеки [85]. Серед таких принципів, в першу чергу, науковці зазначають принципи розвитку, що забезпечують відповідність реакцій на зовнішні та внутрішні зміни та впровадження відповідних змін у власній структурі; принцип законності, який визначає необхідність діяти згідно із нормами прийнятого законодавства; принцип адаптивності, як здатність швидкої адаптації до

зовнішніх та внутрішніх змін; принцип єдності всіх структур та підрозділів підприємства у їх взаємодії та узгодженості дій, спрямований на забезпечення економічної безпеки підприємства; принцип удосконалення, який передбачає необхідність впровадження техніко-технологічних удосконалень, нових технологій та підходів; принцип безперервності, оскільки забезпечення економічної безпеки повинно здійснюватися безперервно з метою повного та постійного захисту підприємства; принцип оперативності, оскільки реакція на впливи негативних зовнішніх та внутрішніх чинників, ризики та загрози має бути швидкою, оперативною; принцип економічної доцільності та обґрунтованості, оскільки всі витрати ресурсів спрямовані на забезпечення економічної безпеки повинні мати економічну доцільність та бути меншими, ніж втрати від реалізації небезпек та загроз; принцип координації, заснований на необхідності взаємодії між структурними підрозділами та працівниками підприємства, зовнішніми партнерами, стейкхолдерами в спільному впровадженні заходів та дій із забезпечення економічної безпеки підприємства.

1.2. Сучасні наукові концепти в дослідженні сутності цифрових технологій та їх впровадження в управлінні

Питання сутності та значення, застосування цифрових технологій широко досліджується в працях багатьох провідних науковців сучасності. Передусім це пов'язано з високою актуальністю та розумінням зростаючої ваги та значення цих технологій в процесах функціонування як кожного підприємства зокрема, так і мезо та макроекономічних систем загалом. Цифровізація, впровадження цифрових технологій сьогодні стосується всіх сфер функціонування, в тому числі і сфери економічної безпеки. Це пов'язано із широким використанням цифрових технологій в техніко-технологічному,

інформаційному забезпеченні економічної безпеки підприємства як нових інноваційних, так і в використанні традиційних технічних засобів. При цьому, фахівці зазначають переваги та високу ефективність використання інноваційних технологій в забезпеченні економічної безпеки, і це передусім пов'язано із можливістю значного зменшення економічних витрат і водночас значним зростанням надійності та ефективності в забезпеченні безпеки.

Концептуальні засади використання цифрових технологій в функціонуванні підприємства загалом представлено у працях В. Ткаченко, М. Климчук [86]. Так, науковцями визначаються зміни розширення інструментарію методів управління підприємством, пов'язаних із застосуванням цифрових технологій. Досліджуючи вплив цифровізації на економічні процеси загалом, науковцями наголошується на особливостях, пов'язаних із застосуванням цифрових технологій, таких як індивідуалізація, глобалізація, значні темпи та динамічність з якими, завдяки впровадженню цифрових технологій, здійснюються зміни як загалом в економічному середовищі, так і в управлінні та функціонуванні підприємства.

У працях І. Струтинської досліджуються процеси реалізації концепції розвитку цифрової економіки в діяльності підприємств малого та середнього бізнесу [87]. Автором наголошується, що активність впровадження нових цифрових технологій в діяльності малого та середнього бізнесу є значною, оскільки це дає підприємствам можливість до реалізації їх конкурентних функцій та для зростання ефективності діяльності за умови зайнятості невеликої чисельності працівників завдяки значній оптимізації, цифровізації у виконанні завдань та робіт.

У дослідженнях Я. Тертичного виявлено основні детермінанти впливу, який здійснює цифровий бізнес загалом на глобальний економічний розвиток [88]. Зазначимо, що автором ґрунтовно досліджено глобальні трансформації, які відбуваються в системах різних рівнів внаслідок впливу інформаційних цифрових технологій та те, як ці зміни загалом впливають на подальше функціонування та розвиток цих соціально-економічних систем.

Окрема увага науковців спрямована на можливості та переваги впровадження сучасних цифрових технологій в розбудові та функціонуванні глобальних ланцюгів постачання. Концептуальні засади такого впровадження досліджено С. Коляденко при розгляді питань діджиталізації та її значення у функціонуванні ланцюгів постачання [89].

У праці І. Чикова досліджувалася сутність процесів цифрової трансформації, особливості її впровадження та технології, що є змістом цифрової трансформації [90]. У працях цього автора досліджено і представлено технологію «блокчейн», як одну із найбільш провідних вагомих технологій, що має значні перспективи подальшого впровадження в діяльності організації та глобалізації процесів економічної і ринкової взаємодії суб'єктів господарювання, проте має як значні переваги, так і недоліки.

Автори Н. Юрчук та С. Кіпоренко досліджуючи наукові засади використання цифрових технологій в діяльності підприємств аграрної сфери обґрунтували перспективні напрямки розвитку інформаційних цифрових технологій в цій сфері [91]. Таким чином, виявлено та обґрунтовано стратегічні вектори, за якими доцільно впроваджувати і в подальшому розвивати використання цифрових технологій та вплив нових технологій на оптимізацію удосконалення діяльності підприємств цієї сфери.

У працях О. Солоня, М. Бурдяк, І. Томашук досліджено сутність та концептуальні засади впровадження цифрових технологій [92, 93]. Зазначається висока динаміка їх розробки, впровадження та швидкого поширення, дифузії в інші напрями та сфери діяльності, що забезпечує високі темпи застосування сучасних цифрових технологій в різних сферах економічної діяльності організації.

Цифрові трансформації, що відбуваються внаслідок широкого впровадження цифрових технологій дають можливість вивести бізнес-процеси які реалізуються в операційній управлінській маркетинговій діяльності на новий рівень впровадження, при цьому значно оптимізуючи їх. На нашу думку, така оптимізація отримана внаслідок широкого використання

цифрових технологій в різних сферах діяльності організацій здатна значно зменшити витрати підприємств від здійснення їх фінансово-господарської, операційної діяльності.

У праці О. Лебідь дослідження сутність інформаційних цифрових технологій в діяльності підприємств, визначено важливість їх значення для забезпечення розвитку підприємства [94]. Сучасне застосування інтернет-технологій дає можливість значно зменшити час, необхідний для отримання інформації, зменшує трансакційні витрати, забезпечує зростання продуктивності праці та ефективної діяльності. Автором зазначається пріоритетність важливість таких цифрових технологій як Інтернет речей, доповнена реальність, Великі дані, робототехніка, машинне навчання та багато інших. Зазначимо, що відповідні нові інноваційні технології на даний час знаходяться на етапі становлення і їх подальше широке впровадження є найближчою очікуваною перспективою, а отже застосування таких технологій стає не вибором, а скоріше об'єктивною необхідністю, здатною забезпечити належний рівень конкурентоспроможності, підтримання ефективності та діяльності підприємства.

Невід'ємними складовими впровадження сучасних цифрових технологій є розбудова необхідної цифрової інфраструктури, комунікацій які забезпечуватимуть технічні можливості, передачі цієї інформації, її збереження і подальшого поширення та використання.

Відповідно до прийнятої в країнах Європейського Союзу Програми «Цифрова Європа 2021-2027» визначено дії та напрями, подальшого впровадження та розвитку цифрових технологій, формування єдиного цифрового простору, що забезпечуватиме подальше створення та розвиток цифрових інновацій [95]. Зазначимо, що метою цієї програми є розвиток, зміцнення цифрового потенціалу країн ЄС, сприйняття формування єдиного цифрового ринку, створення та впровадження інновацій, що загалом здатне забезпечити зростання якості економічного та соціального функціонування. Таким чином, цифрові технології та цифровізація, як цифрові інноваційні

зміни, здатні трансформувати процеси суспільно-економічного середовища, пришвидшити, оптимізувати їх.

Провідними напрямками, за якими відповідно до Стратегії «Цифрова Європа 2021-2027» [96] буде здійснюватися цифрова трансформація, є: цифрові навички та цифрова освіта; цифрові технології; цифрова безпека; цифрова інфраструктура; цифрова трансформація суб'єктів господарювання та загалом цифровізація суспільства. На нашу думку, ці напрями найбільш повно комплексно представляють ті ключові вектори змін та організації діяльності на макрорівні, які спрямовані на забезпечення цифровізації суспільно-економічного життя, формування та розбудови цифрової економіки, цифрового суспільства. Зазначимо, що цифрова трансформація суб'єктів господарювання, цифрова безпека та її забезпечення виступають тими напрямками, що безпосередньо стосуються та мають реалізовуватися на мікро-рівні кожного окремого підприємства як суб'єкта господарювання. Проте, підприємство, як відкрита система безпосередньої взаємодії з макро-середовищем є його невід'ємною складовою, а тому й інші напрями цифровізації, такі як розвиток цифрових навичок та освіти, розвиток цифрової інфраструктури та інші будуть безпосередньо впливати на можливості та перспективи кожного підприємства до впровадження цифрових змін в усіх сферах своєї діяльності.

На думку науковця О. Лебідь цифрова трансформація це не лише удосконалення, зміна, вихід на нові рівні технічного забезпечення, широкого використання комп'ютерної техніки, програмного забезпечення та мережі Інтернет [97]. Це тривалий процес трансформації всієї діяльності підприємства, його бізнес-процесів, внутрішнього середовища та процесів взаємодії з партнерами зовнішнього середовища, що забезпечує автоматизацію, оптимізацію цих процесів та загалом зміну якості функціонування операційної, управлінської, маркетингової систем підприємства та загалом системи управління.

Таким чином, впровадження цифрової трансформації діяльності надає можливості до більш ефективного оптимізованого управління ресурсами, управління в ланцюгах поставок і відстеження вантажів, обліку, прогнозування та ін.

На думку С. Коляденко застосування цифровізації дає можливість [89]: швидкого та ефективного здійснення моніторингу бізнес-процесів, відстеження та аналізу їх ефективності, що загалом забезпечує можливість для прийняття управлінських рішень; автоматизувати виконання рутинних операцій; розбудувати та оптимізувати комунікації з партнерами; покращити процеси роботи з інформацією: підняти на кращий рівень можливості щодо забезпечення безпеки; удосконалити та оптимізувати системи контролю підприємства.

Досліджуючи вплив цифровізації на функціонування традиційних галузей економіки науковці [98] зазначають, що застосування нових цифрових технологій призводить до зміни, цифровізації існуючих моделей бізнес-процесів, оптимізацію процесів які відбуваються в діяльності підприємств за рахунок автоматизації та роботизації процесів, що дає можливість зменшення виробничих операційних витрат, забезпечує індивідуалізацію пропозицій на ринку, зменшує необхідність у кадрових ресурсах замінюючи людську працю та рутинні операції автоматизованими цифровими системами, забезпечуючи зростання попиту в інтелектуалізації праці.

Водночас, поширення цифрових технологій призвело до зростання нових галузей та секторів які впроваджують бізнес-моделі в основі яких цифрові технології. Це докорінно змінює бізнес-процеси та операції забезпечуючи їх оптимізацію, автоматизацію, подальше зростанням інтелектуалізації праці та появу запиту на нових фахівцях інформаційного забезпечення за напрямками впровадження цих технологій.

Досліджуючи функції, які дає можливість реалізувати впровадження нових цифрових технологій слід зазначити операційну. Науковцями наголошується на тому, що впровадження нових цифрових технологій здатне

суттєво вплинути на виконання та результати операційної діяльності підприємства, використання робіт та операцій, змінюючи їх якість, термін виконання та вартість [99]. Цілком погоджуючись з думками авторів зазначимо, що автоматизація операційної діяльності підприємства не лише впливає на значення показника вартості та якості, а й має безпосередній вплив на рівень технологічності самої виробленої продукції, послуг, змінюючи та підвищуючи її цінність для споживачів.

Іншою важливою функцією цифрових технологій є забезпечення безпеки та контролю в захисті даних, які становлять комерційну таємницю підприємства.

Впровадження нових цифрових технологій забезпечує можливість до зростання ефективності та продуктивності діяльності підприємства внаслідок удосконалення виконання процесів та зменшення, оптимізацію витрат ресурсів.

Одними із найбільш важливих цифрових технологій, які забезпечують можливості до удосконалення систем управління науковцями зазначається впровадження систем управління взаємовідносинами з клієнтами CRM-систем та ERP-систем обліку ресурсів. У дослідженнях колективу науковців Н. Матвєєва, І. Килимник, О. Коюда висвітлюється бачення розвитку цифрової економіки загалом як певної екосистеми, яка визначається як поєднання суб'єктів, процесів та компонентів, що формують цифрову економіку [100]. По суті, така екосистема включає розробку та використання цифрових технологій, інновацій в сфері змісту та розбудови інформаційних комунікацій, обміну інформацією, розробки та впровадження цифрових інновацій.

У дослідженнях О. Лебідь [97] екосистема цифрової економіки поділяється на дві головні підсистеми: підсистему яка об'єднує функціональних суб'єктів, між якими формуються взаємозв'язки, взаємодія та підсистему об'єктів управління, що складається з цифрових технологій, мереж, інструментів впровадження цифровізації. Взаємодія цих двох підсистем здатна забезпечити впровадження цифрової трансформації

спрямоване на продуктивний розвиток самої економічної системи, зростання ефективності її функціонування. Водночас, науковцями наголошується на формуванні певного синергетичного ефекту від функціонування цих двох підсистем, який впливає на розвиток економіки загалом.

Серед найбільш важливих рішень в сфері цифровізації, що необхідні для її впровадження, виділяють формування стратегії цифрової трансформації; впровадження нових цифрових технологій; здійснення аналітичного оцінювання зростаючого обсягу даних; забезпечення кібербезпеки; необхідності зміни культури організації; адаптації до нових реалій цифровізації бізнес-процесів і необхідності залучення талантів та нових споживачів [97]. На нашу думку, аналіз цих досліджень дає можливість виділити такі важливі функції впровадження цифрової трансформації як аналітична функція, яка забезпечує можливість до швидкого та ефективного опрацювання зростаючого обсягу інформації; безпекова функція, яка забезпечує безпеку інформації в умовах зростаючої кількості загроз інформаційного середовища; операційна функція, оскільки мова йде про впровадження нових технологій та адаптацію існуючих бізнес-процесів до нових технологій та рішень щодо оптимізації удосконалення операційної діяльності підприємств.

У праці О. Лебідь зазначено основні етапи планування та впровадження цифрової трансформації, такі як [97]: аналіз потреб та можливостей підприємства щодо її впровадження; визнання стратегії цифровізації, її стратегічних цілей; застосування цифрового інструментарію та технологій; впровадження змін організаційної культури підприємства; здійснення моніторингу та оцінювання результатів цифровізації діяльності підприємства та забезпечення подальшої взаємодії інтеграції з партнерами з формуванням нових цифрових каналів інформаційного обміну; забезпечення захисту інформації; забезпечення навчання та підвищення навичок працівників у роботі з новими інформаційними технологіями. Таким чином, впровадження цифрових технологій має проходити низку послідовних етапів, що загалом

забезпечує можливості до функціонування підприємств в нових інформаційних цифрових умовах та зумовлює зростання конкурентоспроможності підприємств.

В сучасних економічних умовах впровадження цифрової трансформації є основою зростання конкурентоспроможності та ефективності вітчизняних підприємств в різних галузях та видах економічної діяльності. Впровадження цифровізації потребує системних планових дій, які забезпечать послідовність впровадження цифрових змін та охоплення всіх функціональних та економічних напрямів діяльності підприємства. Комплексність та системність таких змін за короткий період часу дасть можливість повною мірою перебудувати, цифровізувати процеси та функції на нових цифрових основах. Це забезпечить підприємствам необхідний в умовах сучасності рівень цифрової відповідності та конкурентоспроможності підприємства та забезпечить можливості для ефективного динамічного розвитку. Водночас, цифровізація діяльності розширює можливості підприємств до активної роботи на ринку, просування та поширення, реалізації продукції, послуг, зростання вартості бізнесу та можливостей до його майбутнього розвитку.

Сучасний розвиток нових цифрових технологій здійснює безпосередній вплив на функціонування бізнесу загалом внаслідок зміни, трансформації бізнес-процесів у всіх сферах функціонування: виробництві, операційній діяльності, просуванні та реалізації продукції, логістиці, обліку та управлінні кадрами, безпеці, і насамперед в управлінні. Цифровізація бізнес-процесів підприємства, перехід на використання сучасних цифрових технологій в плануванні та виконанні процесів діяльності підприємств, супроводжується широким впровадженням інноваційних рішень та підходів, нових інноваційних цифрових технологій, програмного забезпечення, розбудови нових цифрових комунікацій.

У дослідженнях Н. Гуржій, В. Гавран, Н. Сапотницька представлено застосування нових технологій та цифровізацію процесів логістичної діяльності підприємств [101]. Зазначається, що впровадження цифрових

технологій в управлінні та оптимізації логістичних процесів підприємства, включаючи пакування, складування, розміщення, транспортування товарів дає можливість значно зменшити витрати, оптимізувати виконання цих процесів в часі і просторі, зменшити витрати людських та часових ресурсів, що загалом забезпечить зниження витрат та зростання прибутковості діяльності підприємства. Враховуючи те, що логістичні процеси займають значну частину в загальній чисельності бізнес-процесів діяльності підприємства і разом з операційними чи виробничими процесами по суті складають зміст виробничої діяльності та матеріально-технічного забезпечення, безумовно така оптимізація здатна значною мірою змінити, зменшити обсяги витрат, зменшити собівартість виробничої операційної діяльності та забезпечити зростання прибутку.

У праці В. Маргасової, О. Самойлович досліджуються можливості та перспективи впровадження цифрових технологій в управління процесами логістичної та маркетингової сфери діяльності підприємства. Сама складність, особливість маркетингових та логістичних процесів полягає у необхідності формування взаємовідносин з постачальниками, покупцями, посередниками, забезпечення контролю якості продукції та процесів її постачання [102, с. 9]. На думку науковців, сучасна інтеграція, зміна геополітичних умов та зростання конкуренції на економічних ринках призводять до необхідності широкого використання нових цифрових технологій в логістичній та маркетинговій діяльності, здатних змінити та трансформувати ці процеси, оптимізуючи їх до рівня сучасних вимог партнерів та споживачів. Впровадження цих технологій здатне вивести взаємодію з партнерами та новий рівень цифрових комунікацій, долаючи кордони у розбудові і впровадженні ланцюгів постачання, будуючи новий цифровий простір економічної співпраці на площині нових глобальних цифрових ринків. Функції впровадження цифрових технологій в управлінні підприємством представлено на рис. 2.1.



Рис. 1.2. Функції впровадження цифрових технологій в управлінні підприємством

Джерело: сформовано автором на основі [103-125]

Значна частина науковців наголошує на тому, що впровадження нових цифрових технологій здатне оптимізувати більшість сфер функціонування підприємства, таких як: фінансова діяльність, логістика, маркетинг та інші [103]. Цілком погоджуючись із думкою авторів зазначимо, що враховуючи сучасний рівень техніко-технологічного розвитку, загально світовий процес переходу до технологій Четвертої промислової революції та в промисловості до Індустрії 4.0. перехід на цифрові технології та сама технологізація всіх сфер суспільно-економічного життя, гостро ставить питання необхідності переходу

на використання цифрових технологій не лише процесів фінансової, логістичної, маркетингової сфери, а й цифровізації процесів виробничої, операційної діяльності, забезпечення безпеки, забезпечення обліку і звітності та реалізацію інших принципово важливих функцій як для функціонування самого підприємства, так і для його взаємодії із зовнішніми партнерами.

Дослідження синтезування думок, науковців та практиків дає можливість узагальнити систематизувати основні функції застосування цифрових технологій в управлінні підприємством, а саме: облікову, логістичну, безпекову, інформаційно-аналітичну, комунікаційну, операційну, маркетингову функції, застосування яких забезпечує та дає можливість впровадження цифровізації, цифрової трансформації бізнес-процесів у всіх функціональних сферах діяльності підприємства та формування якісно нових комунікацій співпраці та взаємодії із партнерами, стейкхолдерами зовнішнього, глобального середовища, що дасть можливість оптимізувати та зменшити витрати, забезпечити зростання економічної та ринкової ефективності діяльності підприємства.

Науковцями зазначається, що питання впровадження цифрових технологій має безпосереднє значення в аспектах підвищення якості та оптимізації економічної, фінансової та логістичної діяльності підприємства. Управління логістичними процесами передбачає різні заходи, спрямовані на створення, аналіз ефективних методів управління, забезпечення роботи транспортних, складських та операційних відділів. Щоб поліпшити якість власного бізнесу, компанії використовують цифрову інфраструктуру, яка дає їм змогу розширювати можливості та прискорювати свою логістичну діяльність. Протягом останніх років швидкого темпу розвитку набувають такі процеси як Smart-логістика, яка базується на основі використання автоматизованих технологій, концепції роботи з великими даними, хмарними обчисленнями, тощо. На думку науковців Р. Воронко, І. Редченко, О. Бурдик з початком впровадження технологій Індустрії 4.0. цифровізація зробила значний крок вперед та стала головним інструментом впровадження

комерційної діяльності, просування та реалізації продукції [126]. Впровадження Індустрії 4.0. пов'язано із застосуванням значної кількості цифрових технологій, здатних успішно виконувати як традиційні, так і нові функції з кращою якістю, швидкістю та зі значною економією витрат, що є однією із найбільш важливих переваг цифрових технологій.

Цифрові технології передусім впроваджуються з метою обліку трудових процесів, формування та використання внутрішніх інформаційних баз. Такими новими інноваційними технологіями виступають CRM та ERP-системи [126]. Так, ERP-системи дають можливість управління виконанням конкретних задач, таких як: управління фінансами, виробництвом та операційною діяльністю: створенням та управлінням запасами матеріалів, товарів на складах, тобто забезпечуються можливості для ефективного управління підприємством. Загалом, системи планування ресурсів (enterprise resource planning) або (ERP) є певним типом програм, впровадження яких забезпечує підприємству можливість для щоденного поточного планування та управління його ресурсами у їх використанні в процесах виробничо-господарської діяльності та процесах, які здійснюються в ланцюгах постачання. Таким чином, забезпечуються нові можливості для управління логістикою, ризиками, впровадженням нових проектів. Загалом впровадження (ERP) для планування ресурсів забезпечує нові можливості для контролю внутрішніх процесів, які відбуваються у важливих функціональних підсистемах підприємства і є важливим інструментарієм для управління у режимі реального часу.

Системи управління відносинами з клієнтами (customer relationship management) або CRM-системи, мають в першу чергу маркетингове спрямування та є потужними платформами, які дають можливість оптимізувати роботу підрозділів, діяльність яких спрямована на просування та реалізацію продукції, надання послуг чи сервісів [126]. Це сучасні цифрові системи, які дають можливість просувати продукцію та послуги, аналізуючи потреби клієнтів в цифровому інтернет просторі, в тому числі за допомогою іншої важливої технології - штучного інтелекту, оскільки значна частина задач

в роботі такої системи здійснюється із застосуванням (ШІ). Зазначимо, що впровадження цієї цифрової системи не лише є сучасною технологією управління процесами роботи з фактичними та потенційними клієнтами та споживачами, вона дає широкі можливості для оптимізації бізнес-процесів, формує нові автоматизовані комунікації із споживачами та відстежує їх потреби.



Рис. 1.3. Види та сутність сучасних інноваційних цифрових технологій в управлінні

Джерело: сформовано автором на основі [127-140]

Окремі науковці [127] звертають увагу на те, що такі системи є новими потужними платформами для організації роботи команди, оптимізують роботу з клієнтами внаслідок дослідження та здійснення цільових комунікацій в інформаційному інтернет просторі, що забезпечує можливості для зростання відсотку успішних угод та збільшення обсягів реалізації продукції, послуг підприємства.

Науковцями зазначається, що провідні світові компанії інформаційного ринку, такі як Google, Microsoft, Meta, інвестували значні обсяги капіталу в розвиток штучного інтелекту і ця цифрова технологія набуває значного поширення, як за обсягами, так і за сферами його застосування [121].

За дослідженням Н. Трушкіна, Х. Джвігол, О. Сергєєва, Ю. Шкригун значними перевагами використання технологій штучного інтелекту є можливості для аналізу великих баз даних, з різною за змістом та характеристиками інформацією, такою як інформація про постачальників, партнерів, маршрути руху, що здатна покращити взаємодію між партнерами, в тому числі і у їх співпраці в глобальному міжнародному середовищі [128].

Цифрові технології Big Data є технологіями аналітичного моделювання, яке здійснюється з використанням статистичної інформації, баз даних та інших джерел, які містять накопичену чи поточну інформацію та здатні її надати. Саме завдяки можливості автоматизованого опрацювання інформації здійснюється аналіз та оцінювання інформації та забезпечується прийняття рішень, спрямованих на оптимізацію бізнес-процесів [129]. Водночас, впровадження цієї технології в управлінні має певні складнощі, пов'язані з необхідністю наявності певного апаратного та програмного забезпечення, формування потужних каналів інформаційних цифрових комунікацій.

Технології хмарних обчислень застосовуються для формування цифрової інфраструктури, автоматизації виконання процесів у виробничій, операційній, логістичній, фінансовій, безпековій діяльності, і за рахунок цього забезпечують зменшення витрат підприємства на здійснення такої діяльності [130]. Як зазначають науковці - ця технологія є особливо доцільною для

застосування на підприємствах, яким необхідно здійснювати облік та управління значними обсягами ресурсів на різних напрямках діяльності, таких як виробництво, збут, управління складами й відповідно необхідністю управляти значними обсягами цифрової інформації та її опрацюванням.

Технології хмарних обчислень по суті є моделлю, яка забезпечує віддалений зручний доступ до всієї необхідної та визначеної інформації з будь-якої точки, що забезпечує можливість використання такої інформації в оперативному режимі для прийняття управлінських рішень, організації та здійснення фінансової, виробничої, комерційної діяльності. Така технологія забезпечує доступ до управлінської інформації оперативно і з мінімальними ресурсами, вона має значні переваги та забезпечує можливості до використання значних обсягів інформації, роботи з внутрішньою документацією та безпосередньо забезпечувати виконання бізнес-процесів, інтегрованих у цифровому інформаційному просторі.

За дослідженнями науковців, однією із провідних цифрових інноваційних технологій є штучний інтелект, з появою та використанням таких інструментів як ChatGPT, Midjourney [127]. В переважній більшості, інструменти штучного інтелекту інтегровані в процеси управління і використання здійснюється в процесі використання самого програмного забезпечення. Слід зазначити, що швидке поширення цієї технології пов'язано із здатністю штучного інтелекту до швидкого пошуку найкращих рішень в управлінських системах, які мають чітке структурування та значний обсяг інформації, що опрацьовується, від дає можливості відстежувати рух товарів, процеси просування, розподілу, виробництва, реалізації в режимі реального часу. Іншою важливою властивістю штучного інтелекту є можливості автоматизованого виконання значного обсягу одноманітних рутинних операцій, на виконання яких необхідно було б задіяти значну кількість працівників.

Важливу роль та значення штучного інтелекту як однієї із провідних технологій сучасності визначають у свої працях В. Маргасова, О. Самойлович

[102]. Зокрема, вони зазначають важливість застосування технології штучного інтелекту не лише для оптимізації логістичної маркетингової діяльності, управління складськими приміщеннями, запасами, а передусім як інструментарію оптимізації бізнес-процесів підприємств. Слід зазначити, що таке широке використання штучного інтелекту відзначається й іншими науковцями, що свідчить про подібність наукових бачень відносно ваги і значення цієї технології, яка охоплює нові сфери діяльності.

Іншою важливою технологією, яка сьогодні застосовується в забезпеченні безпеки та здійсненні логістичної діяльності, управління складами є технологія сенсорних датчиків. На думку Ю. Залозної застосування сенсорних датчиків не лише забезпечує оптимізацію процесів, воно дає можливість інтеграції даних до іншого програмного забезпечення [143]. Зазначимо, що впровадження технології сенсорних датчиків є складовою розбудови та впровадження автоматизованих систем різних рівнів та призначення, від операційної діяльності з контролем якості, відповідності обробки деталей та товарів, складського обліку до використання цих датчиків в системах охорони, безпеки, пожежної безпеки, технологічного контролю та забезпеченні інших безпекових напрямів.

Не менш важливим, з точки зору науковців, напрямом впровадження цифрових технологій є впровадження автоматизованих систем, програмного забезпечення, яке використовується для автоматизації процесів виробництва, складського господарства, управління транспортними складськими системами, забезпечення систем охорони, протипожежної безпеки, в обслуговуванні клієнтів, маркетинговій діяльності [143, 144]. Загалом, впровадження автоматизованих інтегрованих інформаційних систем забезпечує зменшення витрат та зростання ефективності операційної діяльності, надає можливості до кращої, більш ефективної взаємодії з партнерами, дає змогу оптимізувати та удосконалити виконання процесів в тих сферах, де відбувається впровадження, інтеграція таких систем. Самі програмні завдання для впровадження в таких системах можуть бути різними,

залежно від об'єкту управління. Найбільш поширеними є системи управління транспортом (TMS), системи інтелектуального управління складами (WMS), системи управління виробництвом (MES), системи управління ресурсами (ERP) та інші.

Науковці Н. Гуржій, В. Гавран, Н. Сапотницька наголошують на необхідності ланцюга взаємопов'язаних рішень цифрової трансформації суб'єктів господарювання, що забезпечуватимуть їх можливості для успішної адаптації в умовах цифровізації, а саме: розробки прийняття стратегії цифровізації, впровадження цифрових технологій, зростання обсягів даних для аналізу та аналітичного опрацювання, забезпечення кібербезпеки, трансформації в корпоративній культурі підприємства, адаптування бізнес-процесів в нових цифрових умовах, розвитку і взаємодії з клієнтами та залучення талантів [101]. Приєднуючись до такого наукового бачення авторів зазначимо, що впровадження нових цифрових технологій одночасно здійснюється за різними напрямками та складовими, в тому проявляється його системність та багатоаспектність. При цьому, всі процеси та дії, починаючи з розробки та реалізації довгострокових стратегій цифрової трансформації на різних рівнях впровадження, починаючи з макrorівня держави, завершуючи мікрорівнем підприємств і до безпосереднього проектування, адаптування чи реінжинірингу бізнес-процесів на нових цифрових основах потребують системних комплексних дій з управління, їх планування, стратегічного визначення та розбудови механізмів їх практичного впровадження.

Загалом, у прийнятій Стратегії «Цифрова Європа 2021-2027» [95]. ключовими напрямками впровадження цифровізації зазначено: розвиток цифрових навичок та освіти; створення та розбудову цифрової інфраструктури; впровадження нових цифрових технологій; впровадження цифрової трансформації підприємств; забезпечення цифрової безпеки; загальна цифровізація суспільного життя (рис. 1.4.).

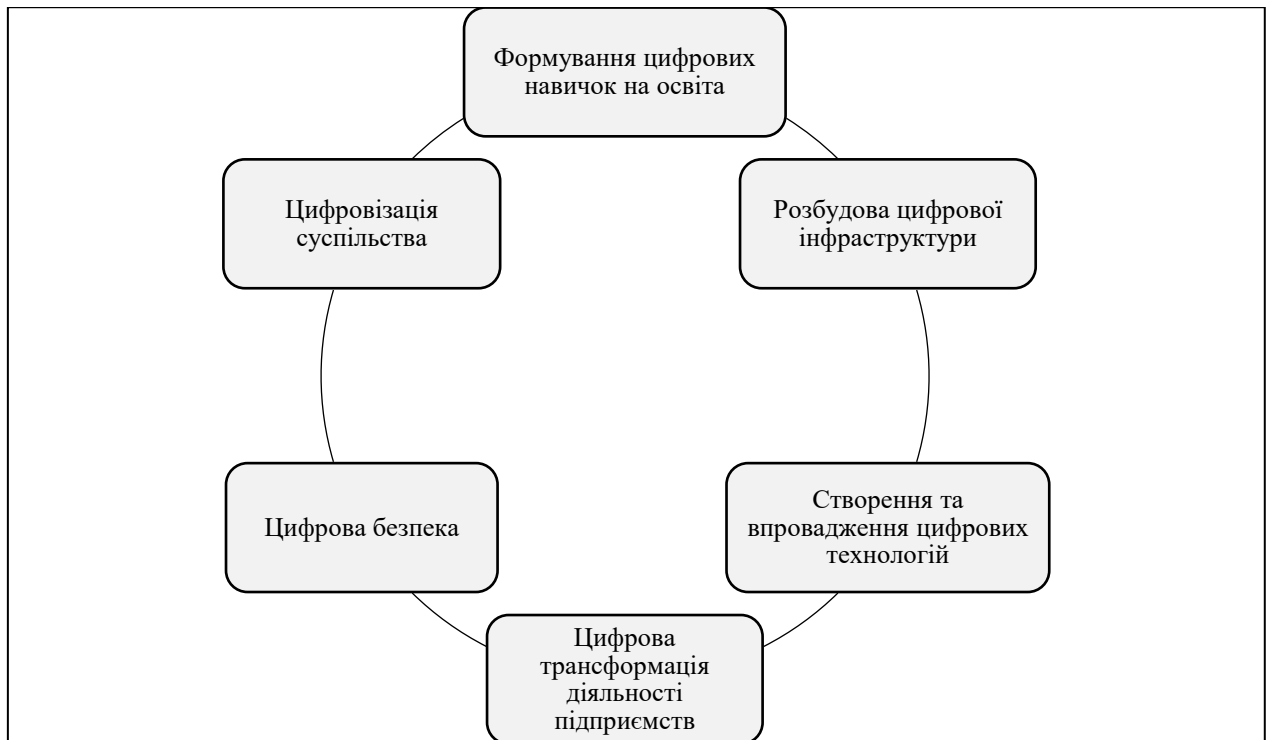


Рис. 1.4. Ключові напрями впровадження Стратегії «Цифрова Європа 2021-2027 рр.»

Джерело: [95, 142-145]

Роботизація, впровадження окремих роботів чи роботизованих систем у виробничій діяльності сервісу, на виконанні окремих операцій чи в механізмі автоматизованих систем є однією із провідних поширених цифрових технологій, що знайшли активне застосування, в тому числі в сфері безпеки. Загалом роботизація як процес впровадження роботів здійснюється з метою зростання точності, продуктивності, якості виробництва продукції, надання послуг, виконання певних, а особливо високоточних операцій та процесів. В сучасних умовах особливо важливого значення роботизація має при необхідності виконання операцій в умовах підвищених ризиків чи небезпечних умов для життя та здоров'я працівників, в умовах, де використання людської праці є небезпечним, неефективним чи неможливим. Проте, в сучасних умовах з широким впровадженням роботизації виробництва ці технології застосовуються з метою автоматизованого виконання рутинних, типових робіт, операцій чи функцій зі значними обсягами виробництва чи

охоплення споживачів, що дає можливість значно підвищити якість виконання робіт та зменшити витрати операційної діяльності, маркетингу.

Новим сучасним трендом Індустрії 4.0. Четвертої промислової революції є поєднання роботизації з широким застосуванням цифрових технологій штучного інтелекту і створенням таких званих кібер-фізичних систем, здатних поєднати фізичний світ – людину, людське мислення та роботизацію, роботизовані системи. Таке поєднання виводить процеси виконання робіт та операції за межі рутинних типових на новий рівень застосування та складності задач, які вони здатні ефективно виконувати.

Базові засади цифровізації, впровадження цифрових технологій досліджено у праці К. Єфремова, Д. Шматкова, В. Кохан, які визначили впровадження цифрових технологій як певні фундаментальні зміни в технологіях, формах та засобах здійснення праці, як зміни економічних, суспільних, культурно-соціальних відносин, які відбуваються завдяки впровадженню нових сучасних комунікаційних інформаційних технологій, цифровізації [142]. Науковці наголошували на необхідності системного підходу до впровадження таких змін у всіх сферах функціонування, як на рівні держави, так і на рівні підприємств, у зв'язку із чим цифрові технології, цифровізація визначає не лише зміни засобів виробництва чи процесів операційної, управлінської, безпекової, логістичної чи маркетингової діяльності, а загалом сукупності концентрації змін, що призводять до трансформації самих соціально- економічних систем.

Усе це разом, на думку науковців, приводить до появи та розбудови такого поняття як «цифрова економіка» [146-153]. Ядром формування такої «цифрової економіки» виступає розвиток самого інформаційно-комунікаційного сектору, який і забезпечує створення та впровадження продукування та поширення цифрових технологій, появу більш нових і нових видів цифрових технологій програмного забезпечення, інформаційно-комунікаційних систем, приладів, яке дає можливість масового впровадження нових цифрових технологій в роботі підприємств, розвитку інфраструктури,

діяльності організацій, освіти, охорони здоров'я, державного управління, житлово-комунального господарства, транспорту та загалом забезпечуючи зміну та трансформацію всього соціально-економічного життя.

Науковцями К. Єфремова, Д. Шматков, В. Кохан визначається важливість ролі та значення розбудови такої цифрової економіки та тих змін, які вона вносить в суспільно-економічне життя. Науковцями виділено три головні аспекти [142]. Першим є вплив цифрових технологій на розвиток бізнесу, що призводить до його трансформації та переходу від традиційних бізнес-процесів та бізнес-моделей діяльності до цифрових, із застосуванням таких технологій, як: роботизація операційної, виробничої діяльності та бізнес-процесів; впровадження штучного інтелекту; створення великих баз даних та робота з ними, використання інструментарію поведінкової економіки з вивченням та прогнозуванням індивідуальних потреб споживачів та намаганням новостворених систем в суспільно-економічних процесах його задовольнити. Таким чином, сама цифровізація не може розглядатися лише з позицій впровадження цифрових технологій, цифровізації окремих процесів, підрозділів, вона спрямована на зміни сутності діяльності суб'єкту та передбачає його значну стратегічну трансформацію.

Другим аспектом виступає формування, завдяки впровадженню цифровізації, нового цифрового середовища для здійснення економічної діяльності. Формування такого цифрового середовища залежить від наявних для цього ресурсів, інтеграції суб'єкту господарювання та його взаємодії з іншими стейкхолдерами зовнішнього середовища, внутрішнього та на міжнародному ринках. Загалом зазначається, що таке бізнес-середовище дає як нові можливості для масштабування бізнесу та подальшого розширення розвитку, так і генерує та створює нові ризики, небезпеки, загрози діяльності. Такими новими цифровими середовищами передусім виступають «розумні заводи», «розумні будинки» цифровізовані робочі місця персоналу і т.д.



Рис. 1.5. Трансформація систем різних рівнів із впровадженням переходу на інноваційні цифрові технології

Джерело: сформовано автором на основі [142, 152-173]

Третім аспектом є вплив впровадження цифрових інноваційних технологій на формування та розбудову цифрової економіки загалом. Цифрова економіка загалом, як зазначають науковці, формує новий тип конкурентного середовища з високим рівнем конкуренції і новими ризиками та загрозами, як глобального так і локального характеру [165-171].

Узагальнення вище зазначеного дає підставити зробити висновок про те, що цифрова трансформація підприємства відбувається поступово, від початкових етапів впровадження окремих цифрових технологій, програмного забезпечення, цифрових приладів, засобів до цифровізації робочих місць, впровадження бізнес-процесів та використання в їх роботі електронних цифрових технологій, впровадження інтегрованих інформаційних систем на підприємстві та розвитку співпраці, кооперації з партнерами, автоматизації функціональних підсистем діяльності підприємства, таких як логістична,

операційна, виробнича, транспортна складська, маркетингова та інші. Це забезпечуватиме формування певних цифрових середовищ в межах конкретного суб'єкту господарювання таких «як розумний завод», чи призвести до їх об'єднання в певній кластерній структурі, і врешті до формування загалом цифрових бізнес-моделей, формування та впровадження цифрових платформ і разом, внаслідок цифровізації переважної більшості процесів економічного функціонування, до розбудови цифрової економіки.

Одностайність наукових поглядів проявляється в розумінні самих процесів цифровізації та їх прямого чи опосередкованого впливу на всі процеси та сфери суспільно-економічного життя, види економічної діяльності. Саме адаптивність можливість для швидкого переходу на нові технології, впровадження нових цифрових рішень у виробництві, операційній діяльності, просуванні чи реалізації продукції та послуг, визначає конкурентоспроможність підприємства та його можливості до ефективного функціонування і розвитку. Однією із найбільш важливих цифрових змін, є автоматизація та цифровізація виробничої операційної діяльності підприємств, адже впровадження нових технологій веде до змін переходу від традиційних процесів та технологій виробництва до нових автоматизованих з використанням інноваційних цифрових технологій, програмного забезпечення, а отже призвело до впровадження нових цифрових процесів, які замінили традиційні.

Таким чином, впровадження нових цифрових технологій призводить до зміни самої моделі ведення бізнесу та надає інструменти для оптимізації діяльності та покращення її результатів. Окремо, слід виділити нові сервіси та можливості у просуванні та реалізації продукції, послуг та покращення комунікації зі споживачами. Провідними інноваційними технологіями у сфері маркетингу стали цифрові електронні платформи, проте вони не лише спростили процеси виходу та роботи підприємств як на внутрішньому, так і на зовнішніх ринках, адже цифрові електронні платформи мають не лише маркетингову цінність як універсальні площадки, нові віртуальні ринки

реалізації продукції та послуг. З позицій економічної безпеки важливість у їх застосуванні полягає у новому рівні безпеки, який вони забезпечують у комунікаціях з партнерами ринку завдяки активним використанню в цих платформах технологій блокчейн та багаторівневій перевірці надійності всіх учасників ринкових відносин в межах платформи. Таким чином, технології цифрових платформ, хмарних обчислень, блокчейн, забезпечують безпеку і взаємодію, персоналізацію пропозицій задоволення потреб споживачів та зростання ефективності роботи зі споживачами та стейкхолдерами.

Впровадження робототехніки та штучного інтелекту дає можливості до автоматизації виконання не лише рутинних задач та операцій, а й забезпечує перехід до автоматизації складних технологічних процесів та промислових комплексів різної потужності і масштабу. Як результат, поява сучасних «розумних заводів», «розумних складів», які забезпечують повну автоматизацію, а процеси функціонування дають високу точність та якість результатів діяльності. Проте, найбільш поширена в сучасних умовах автоматизація та цифровізація процесів виробництва, операцій, контролю якості забезпечує можливості для зростання якості та ефективності праці, безпеки виконання складних і небезпечних для життя та здоров'я людей операцій, забезпечує кращу якість, уніфікованість виробництва продукції, що позначається на зростанні рівня технологічної та виробничої безпеки підприємства. Впровадження технологій 3-Д друку дають можливість значно зменшити обсяги витрат на розробку та підготовку до виробництва продукції, прискорюють процеси виробництва та забезпечують унікальність індивідуалізацію продукції, що є особливо важливим в умовах зростання вимог до технологічності та якості. Це забезпечує можливості до зменшення витрат і зростання якості технологічності, індивідуалізації виробництва, реалізації технологічно складних, унікальних проектів зростання частки виробництва продуктів з високим рівнем доданої вартості.

1.3. Теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства

Питання цифровізації, впровадження цифрових технологій в різних сферах функціонування останнє десятиліття часто висвітлюється в публікаціях з наукових та науково-прикладних досліджень. Стрімкий динамічний розвиток технологій сучасної інформаційної економіки та впровадження нових цифрових інновацій призводить до значних трансформацій, змін економічного та суспільного життя і здійснює значний вплив на всі сфери функціонування. Нові цифрові технології є каталізатором та рушійною силою цих змін, внаслідок яких змінюються операції, процеси, системи, змінюється як сама сутність, зміст, так і вектори суспільно-економічного розвитку. Проте, впровадження нових цифрових технологій не лише забезпечує та оптимізує подальшу діяльність, воно може супроводжуватись новими викликами, загрозами та ризиками, реалізація яких негативно впливатиме на всю подальшу діяльність підприємства. Саме тому в умовах цифровізації проблеми належного рівня забезпечення економічної безпеки є принципово важливими та актуальними. Забезпечення економічної безпеки в умовах сьогодення, з впровадженням цифровізації та діджиталізації всіх сфер суспільно-економічного життя спрямоване не лише на захист ресурсів підприємства, його економічних інтересів, воно спрямоване на забезпечення розвитку, зростання конкурентоспроможності підприємства в нових ринкових умовах. Вирішення таких завдань потребує від системи економічної безпеки підприємства розбудови власних та залучення інтегрування в загальні інформаційні системи, здійснення сучасних цифрових комунікацій та широкого використання сучасних інноваційних цифрових технологій не лише в сфері безпеки, а й у всіх інших функціональних сферах діяльності підприємства, їх узгодженості та взаємодії в забезпеченні безпеки. Питання застосування інноваційних цифрових технологій в забезпеченні економічної безпеки на всіх її рівнях - на макрорівні держави, мега та

мікрорівні підприємств широко досліджувалося у працях провідних вітчизняних науковців.

Так у дослідженнях І. Чайковської, Т. Ткач, М. Чайковського розглянуто вплив цифровізації та автоматизації на економічну безпеку та виявлено два аспекти цього впливу - з позицій як отримання нових можливостей, так і впливу та дії нових ризиків [174]. Науковцями обгрунтована необхідність формування певної цифрової екосистеми, яка виступала б складовою економічної безпеки підприємства та поєднувала б застосування інноваційних цифрових технологій, таких як хмарні обчислення, інтернет речей, штучний інтелект, прогнозне моделювання та інноваційні інформаційні системи, такі як ERP, CRM, PRM, HRM, MES і таким чином надавала б можливості до опрацювання значних масивів інформації в забезпеченні економічної безпеки підприємства. Зазначимо важливість цих наукових досліджень, оскільки їм вдалося не лише представити окремі інноваційні цифрові технології та доцільність їх впровадження в забезпеченні безпеки, а й виокремити та систематизувати інноваційні цифрові системи. Їх застосовують в практичній діяльності сучасних підприємств з метою оптимізації функціонування різних функціональних сфер, таких як логістична, маркетингова, управління ресурсами, і т. д., обгрунтувавши доцільність застосування як цифрових технологій, так і інформаційних систем в забезпеченні економічної безпеки.

Важливими технологіями, які застосовуються в забезпеченні економічної безпеки підприємства зазначено технології машинного навчання, аналітики великих даних, технологій штучного інтелекту, хмарних обчислень, промислового інтернету речей, прогнозного моделювання, розширеної та віртуальної реальності [174]. Водночас, науковцями зазначається необхідність для аналізу та опрацювання значних масивів інформації, розбудови та використання цифрових інформаційних систем, здатних здійснювати збір, опрацювання, поширення використання значних обсягів даних. Слід зазначити, що наведені цифрові інновації та їх поєднання дає можливість охопити та комплексно дослідити всі аспекти та функціональні підсистеми

діяльності підприємства, що дасть можливість самій системі економічної безпеки підприємства отримувати та опрацьовувати інформацію щодо фактичних та потенціальних ризиків і загроз в режимі реального часу та вчасно здійснювати моніторинг реалізації потенційних ризиків та загроз в майбутньому.

Особливо важливим застосування нових інноваційних цифрових технологій є для впровадження систем моніторингу, здійснення аналізу та оцінювання показників і рівня економічної безпеки підприємства та планування і впровадження превентивних заходів, спрямованих на попередження виникнення та усунення наслідків дії показників загроз.

За дослідженням Є. Рудніченко, С. Суходоля, Н. Гавловської, С. Ядуха, І. Лісовського використання цифрових технологій та їх основі автоматизації економічних процесів здійснює значний вплив як на функціонування та виконання економічних процесів, так і на економічну безпеку підприємства [175, с.173-174]. Науковці звертають увагу на те, що впровадження штучного інтелекту та загальне прискорення створення та впровадження цифрових технологій збільшує динаміку зовнішніх ринкових процесів та ускладнює і збільшує ризики ринкового середовища, що призводить до зростання впливу існуючих та появи нових ризиків та загроз і в першу чергу нового цифрового середовища, появу кіберзлочинності та інших небезпек. Водночас, впровадження нових цифрових технологій та автоматизація процесів забезпечує нові можливості не лише для удосконалення операційної виробничої діяльності, це забезпечує трансформацію процесів управління, зростання продуктивності, ефективності діяльності, підвищує рівень економічної стабільності та прибутковості бізнесів.

У дослідженнях, проведених О. Панченко зазначається, як позитивні впливи на роботу підприємства та рівень його економічної безпеки пов'язані із можливостями застосовувати нові інформаційні технології для обміну інформацією, ідеями в сфері безпеки та відповідати на нові загрози та ризики, пов'язані з цією діяльністю [176]. В цілому, погоджуючись з автором

зазначимо, що позитивний вплив нових інноваційних цифрових технологій не обмежується лише новими впливами та формами комунікацій із зовнішніми партнерами з забезпечення безпеки. Комунікаційна складова представляє лише одну із складових системи безпеки підприємства, проте впровадження цифрових технологій охоплює передусім кадрову, фінансову, виробничу, безперечно інноваційну, ринкові та всі інші складові, а тому на наш погляд такий вплив доцільно розглядати як комплексний та системний, оскільки очевидним є зв'язок всіх складових підсистем системи економічної безпеки, який стає ще більш міцним та інтегрованим з впровадженням цифрових інноваційних технологій.

У працях І. Братченко, С. Войтович, І. Кулик, І. Лорві, С. Бігун та ін. зазначено, що застосування нового програмного забезпечення з метою здійснення управлінського, фінансового-господарського обліку спрощує процеси управління, аналізу, оцінювання діяльності та контролю [177, с.153]. Погоджуючись з авторами зазначимо, що здійснення управлінського та бухгалтерського обліку з впровадженням нових цифрових технологій, програмного забезпечення та розбудовою на підприємствах інтегрованих інформаційних систем управління значно удосконалює облікову аналітичну діяльність, зменшуючи витрати кадрових, фінансових, матеріальних ресурсів, забезпечує удосконалення та оптимізацію всіх внутрішніх процесів та призводить до значної економії і зменшення витрат. Щодо безпекової складової, зростання якості контролю над використанням ресурсів, ефективності аналізу та оцінки діяльності витрат ресурсів забезпечує зростання рівня фінансово-економічної та інших складових економічної безпеки підприємства. Все це разом сприяє зростанню економічної стабільності та ефективності діяльності як в поточній, так і в майбутній перспективі.

На думку О. Кухар, Ю. Кравчук, О. Бречко впровадження процесів цифровізації значно позитивніше впливає на можливості підприємства до реалізації функцій за різними напрямками діяльності, що в свою чергу

забезпечує зростання рівня економічної безпеки підприємств [178]. Таким чином, впровадження цифрових інновацій сприяє зростанню ефективності бізнес-діяльності, досягненню мети та цілей підприємства та забезпечення його економічної безпеки.

На думку І. Чайковської використання цифрових технологій, інтегрування нового корпоративного програмного забезпечення, в бізнес-процеси діяльності має значні переваги і розширює можливості підприємства щодо стратегічного управління такими процесами [179]. Слід зазначити, що в працях цієї авторки підіймається питання необхідності розробки та впровадження стратегії «цифрової безпеки», а сама цифрова безпека виділяється як окремий вид безпеки, яка потребує окремого обґрунтування та розробки на підприємстві концепції та стратегії цифрової безпеки. Визначаються принципи, на засадах яких будуватиметься така стратегія, до них віднесено: принцип унікальності, оскільки сама структура кожного підприємства є унікальною; принцип спеціалізації операційної діяльності та впровадження цифрових технологій; принцип комплексного охоплення всіх складових систем економічної безпеки як основи забезпечення цифрової безпеки; принцип єдності та ефективності концепції безпеки і заходів на її впровадження. Все це свідчить про формування в сучасних умовах нової складової економічної безпеки, а саме – цифрової безпеки та обґрунтовує її взаємозв'язок та взаємодії з іншими безпековими складовими, що на нашу думку є важливим науковим здобутком.

У роботі В. Дикань, Н. Фролова та Цзян Пань досліджено питання цифровізації та безпеки суб'єктів малого та середнього підприємництва [180, с.21]. Науковцями зазначається, що разом зі значними перевагами впровадження нових цифрових технологій в сфері МСП, розвитком комунікацій з контрагентами ринкового середовища та оптимізацією бізнес-процесів, активуванням інноваційної діяльності, комунікаційних каналів обміну бізнес-інформацією – головними ризиками, які стають значними викликами для МСП є зростання залежності від самих цифрових технологій.

У дослідженнях С. Решетова, Ю. Полусмяк увага науковців зосереджена на дослідженні ризиків впровадження цифрової трансформації загалом для економічної безпеки держави, а саме на потенційних ризиках зростання безробіття внаслідок оптимізації та автоматизації процесів та сервісів і вивільнення значної кількості працівників, а також на ризиках зростання кіберзлочинності та на недостатності на ринку праці підготовлених працівників з необхідними сформованими компетентностями, спроможних впроваджувати та використовувати сучасні цифрові технології [181, с. 12]. Загалом, погоджуючись з авторами зазначимо, що поява змін та нових можливостей для функціонування з новими цифровими технологіями традиційно супроводжується неготовністю економіки та суб'єктів господарювання до швидкого прийняття, адаптації та кращого використання цих змін. Водночас, неготовність та зростання ризиків діяльності окремих суб'єктів господарювання буде впливати на формування та генерування нових ризиків макрорівня економічній безпеці держави, оскільки між рівнями безпеки є прямий взаємозв'язок та пряма (через надходження до бюджету) і опосередкована (через загальний стан економіки) економічна кореляція та взаємозалежність.

У розгляді питань застосування сучасних цифрових технологій в забезпеченні економічної безпеки підприємства окремої уваги заслуговує дослідження В. Гончар та К. Полупанова функціональних характеристик технологій та систем, інформаційних програмних продуктів, які застосовують в діяльності із забезпечення економічної безпеки підприємства [182].

Колективом авторів Ю. Самойленко, І. Брітченко, Л. Левченко, О. Біліченко О. Боднара та ін. визначено групи основних та допоміжних технологій, необхідних для ефективного функціонування та забезпечення безпеки підприємства [183]. Систематизовано види технологій, які належать до групи основних: 1) технології ідентифікації небезпек та загроз, функціональним завданням яких є виявлення ризиків, загроз та небезпек; 2) технології тестування систем економічної безпеки підприємства, призначені

для оцінювання, наскільки система економічної безпеки підприємства здатна забезпечити йому належну безпеку; 3) технології призначені для оцінювання класу небезпек, функціональним завданням яких є оцінювання стану та рівня безпеки; 4) технології, призначені для захисту від небезпек та загроз, функціональним завданням яких є забезпечення підприємства від загроз, небезпек та ризиків внутрішнього та зовнішнього середовища.

До групи допоміжних технологій цими науковцями включено: технології облікового аналітичного забезпечення, головним функціональним завданням яких є надання обліково-аналітичних даних, необхідних для роботи системи економічної безпеки; технології контролю внутрішньогосподарської діяльності, спрямованих на забезпечення контролю відповідності рішень, які приймаються в управлінні безпековою системою; технологій забезпечення інформацією та необхідними комунікаціями, головним функціональним призначенням яких є перехід на цифрові формати документації підприємства та впровадження автоматизованих процесів збору, обробки, збереження та використання інформації, передачі інформації, документації, а також налагодження комунікацій взаємодії із зовнішніми партнерами та внутрішні комунікації між рівнями і підрозділами підприємства; безпосередньо технологій управління, головним функціональним завданням яких є забезпечення ефективного функціонування системи економічної безпеки підприємства загалом.

У дослідженнях Ю. Самойленко, І. Брітченко, Л. Левченко, О. Біліченко, О. Боднара не лише представлено цифрові технології та їх значення в забезпеченні економічної безпеки, а запропоновано поняття цифрової безпеки підприємства як стану цифровізації системи економічної безпеки, здатної забезпечити економічні та інформаційні інтереси суб'єкта господарювання на даний час та в стратегічній перспективі із застосуванням сучасних провідних цифрових технологій Індустрії 4.0. та технологій Четвертої промислової революції [183].

Слід зазначити, що таким чином науковці обґрунтовують та дають визначення новій складовій економічної безпеки підприємства, а саме цифровій безпеці, що є поняттям новим і на даний час в наукових працях з безпеки фактично не дослідженим. Таке бачення є відмінним від традиційного, за яким інноваційні цифрові технології та їх впровадження досліджують як складову інноваційної безпеки та складові інформаційної безпеки в системі економічної безпеки підприємства. Водночас, поширеним та загальним є розуміння цифрових інформаційних технологій як засобів інформаційно-аналітичного забезпечення, які і забезпечують як технічну так і аналітичну складові роботи з інформацією в сучасних умовах. Слід нагадати, що саме інформаційно-аналітичне забезпечення надає всю необхідну інформацію для проведення моніторингу, аналізу та оцінювання стану та рівня економічної безпеки підприємства, ідентифікації загроз економічній безпеці, виявлення джерел виникнення та інтенсивності дії загроз, небезпек, ризиків та дає можливість для організації і впровадження превентивних заходів, програм та організації належної протидії загрозам що виникли, оскільки саме інформаційне забезпечення має як аналітичну, інформаційну, прогнозну, так і облікові функції в системі економічної безпеки підприємства.

У працях Г. Мельничук та В. Мамалиги розглядаються питання можливостей та загроз в діяльності суб'єктів господарювання в нових умовах діджиталізації, переходу до цифрової економіки, визначається особлива роль в цих процесах долучення підприємств до процесів цифрової трансформації та набуття здатності протидії новим викликам та загрозам цифрової економіки [184]. Слід зазначити, що питання цифровізації загалом відкриває для підприємств нові перспективи та можливості для розвитку і водночас є новим високоактивним джерелом впливу нових небезпек та загроз, і в першу чергу загроз кіберзлочинності. Протидія таким загрозам можлива лише на відповідному техніко-технологічному рівні, а тому впровадження цифрових технологій у функціонуванні підприємств стає питанням номер один для забезпечення економічної безпеки підприємства.

Авторське бачення та обґрунтування цифрової безпеки представлено у працях колективу авторів Н. Касьянова, М. Біличенко, А. Севериненко які визначають цифрову безпеку на трьох рівнях: держави, рівні підприємств та на рівні громадян [185]. На рівні держави загальний цифрова безпека визначається як стан захисту інформаційного цифрового середовища держави здатний забезпечити формування розбудову та розвиток цього середовища, дотримуючись інтересів всієї держави, її підприємств та громадян. На рівні підприємств автори визначають цифрову безпеку як стан захисту інформаційних ресурсів суб'єктів господарювання з метою протидії ризикам та загрозам нового цифрового середовища та задля забезпечення впровадження нових технологій та інноваційного розвитку підприємств. На нашу думку, таке розуміння, обґрунтування сутності цифрової безпеки є важливим здобутком, який надає чіткі обґрунтовані визначення цьому новому малодослідженому поняттю. Проте, на наш погляд, дискусійним залишається питання розгляду цифрової складової як невід'ємної складової системи економічної безпеки підприємства, яке і визначає її роль та значення в цій системі, взаємозв'язку та взаємодії з іншими функціональними складовими та в забезпеченні економічної безпеки, як в системах макро, так і мікрорівнів загалом. Складається враження, що автори розглядають цифрову безпеку як окрему наукову категорію, спрямовану на протидію загрозам та ризикам самого цифрового середовища як систему, зосереджену на вирішення певних конкретних цифрових завдань відокремлено від загальної системи безпеки, впливів чи взаємодії з іншими складовими.

Досліджуючи поняття цифрової безпеки, науковці розглядають питання розбудови системи цифрової безпеки, при створенні якої досліджено такі об'єкти як цифрові технології, інформаційні системи, ресурси цих інформаційних систем, мережі зв'язку, програмне забезпечення та автоматизовані системи [185]. Об'єктами захисту такої системи виступатиме сама інформація та інформаційні процеси. Зазначено, що на розбудову системи цифрової безпеки впливатиме низка вагомих факторів, таких як:

наявні загрози цифрового середовища, їх виникнення та дія; ризики цифрового середовища та потенційні збитки від настання ризикових подій; вразливість самої системи цифрової безпеки підприємства та інші.

На думку М. Саврук цифрова безпека є певним станом захисту інформації, яка дає можливість забезпечити принципово важливі інтереси суб'єкта господарювання та суспільні інтереси загалом [186]. Таким чином, цифрова безпека визначається автором з позицій захисту саме інформаційної безпеки на всіх її рівнях, що дещо обмежує на наш погляд, самі можливості такої системи адже цифрові небезпеки та загрози в сучасних умовах здатні здійснювати негативні впливи не лише на інформаційну складову системи безпеки, а й на здійснення її виробничої, операційної, фінансової діяльності чи фізичної безпеки внаслідок втручання електронними засобами в різні системи функціонування підприємств, що також потребують належного захисту в умовах цифровізації.

У праці Т. Передерій обгрунтовується поняття цифрової безпеки та необхідність розробки та впровадження стратегії цифрової безпеки як певного драйвера, здатного забезпечити пришвидшення цифрової трансформації економіки [187]. Таким чином, автором досліджено питання забезпечення цифрової безпеки на макрорівні та мікрорівні, та обгрунтовано взаємозв'язок макрорівня та мікрорівня економічної безпеки підприємств в їх стратегічній протидії новим загрозам та ризикам цифрового середовища в період цифрової трансформації економіки країни.

У роботі Краус К., Краус Н., Штепа О. [188] підіймаються питання цифрової трансформації змін кібербезпеки, яка виходить на новий рівень впливу та є особливо актуальною в сучасних умовах, в умовах воєнного стану.

Загалом, наковці визначають цифрову безпеку як певний стан цифровізації, що забезпечує економічні інтереси підприємства в поточний період та в стратегічній перспективі. Визначають відмінність цифрової та інформаційної безпеки.

Науковцями І. Чайковською, Т. Ткач, Б. Поперечним представлено проактивний підхід до забезпечення економічної безпеки підприємства з впровадженням нових цифрових технологій [189]. З позицій проактивного підходу одним із головних завдань із забезпечення безпеки з впровадженням цифрових технологій є виявлення та прогнозування потенційних загроз, небезпек та впровадження, прогнозування та впровадження превентивних заходів з попередження їх реалізації. Обґрунтовують впровадження такого проактивного підходу необхідністю захистити цифрові активи підприємства та пом'якшити агресивні впливи зовнішніх факторів реалізації ризиків та загроз в умовах швидких динамічних змін, в тому числі і в самому цифровому технологічному середовищі, що в першу чергу пов'язано із кіберзагрозами – кібератаками, загрозами аварійного відключення, пошкодження цифрових систем та ін.

Дослідники наголошують на безперервності процесу впровадження цифрових технологій, що передбачає необхідність регулярного оновлення самих програмних продуктів, інформаційних систем та технологій, крім цього необхідним є постійне планування та впровадження навчання персоналу задля формування навичок, вмінь та компетенцій, необхідних для роботи з новими цифровими технологіями, щоб забезпечувати покращення, удосконалення якості роботи працівників та позитивно впливатиме на результати їх роботи [189]. На нашу думку, слушно підіймається питання про зміни самої культури ведення бізнесу, на що суттєво впливає зміна форматів діяльності, особливо серед підприємств, що безпосередньо конкурують із споживачами в сфері сервісу. Впровадження цифрових систем та технологій здатне швидко адаптувати підприємство під нові ринкові реалії та виклики, проте і самі впровадженні технології, персонал що з ними працює також повинні своєчасно адаптуватися до змін, які виникатимуть в зовнішньому та внутрішньому середовищах, забезпечити оновлення зростання рівня знань та технологій в умовах динамічних зовнішніх змін.

За дослідженням В. Проскура, Т. Черничко, Д. Верецького саме поняття цифровізація підприємства є формуванням системи управління, координування та моніторингу, стеження за економічною діяльністю суб'єкта господарювання підприємства з використанням цифрових інформаційних технологій, цифрових рішень з метою забезпечення безпеки діяльності підприємства в майбутньому та досягнення цілей його розвитку [190]. Таке впровадженням цифрових технологій в системі економічної безпеки досліджено авторами як комплекс загального процесу цифровізації діяльності підприємств з цифровізацією процесів у всіх функціональних підсистемах, в тому числі і безпеки, а цифрові рішення застосовуються задля вирішення задач та досягнення цілей діяльності підприємства.

Водночас, науковцями здійснено важливі наукові напрацювання в питаннях діагностики оцінювання рівня економічної безпеки підприємства із впровадженням цифрових технологій та виділено наукові підходи до діагностики та відповідні методи такого оцінювання: ресурсно-функціональний підхід, підхід на основі теорії ризиків, програмно-цільовий підхід, комплексний підхід та методи пороговий, інтегрального оцінювання [190]. На нашу думку, всі вище зазначені підходи та методи представлено в сучасній науці безпекології, вони успішно застосовують як для діагностики аналізу оцінювання стану та рівня економічної безпеки підприємств на більш вищих, мезо та макрорівнях економічної безпеки. Проте їх адаптація сприяла формуванню, за авторством цих науковців, «скоригованої на цифровізацію» методики оцінки економічної безпеки підприємств МСП в умовах цифровізації з зазначенням низки нових важливих показників-індикаторів оцінювання цифрових процесів в системі економічної безпеки.

Досліджуючи питання цифрових технологій в забезпеченні економічної безпеки підприємства В. Проскура, Т. Черничко, Д. Верецький також висувують тезу про те, що забезпечення економічної безпеки в сучасних цифрових умовах має бути забезпечене відповідним рівнем цифрової безпеки, що свідчить про виділення обґрунтування такої цифрової безпеки [190]. Таким

чином, цифрова безпека є окремою сукупністю якісно нових факторів, що забезпечуватимуть формування в межах підприємства єдиної інформаційної системи, функціонування якої спрямоване на забезпечення економічної безпеки та зменшення впливу небезпек та ризиків внутрішнього та зовнішнього середовищ.

У праці Т. Ткачук представлено визначення поняття цифрової безпеки як забезпечення безпеки об'єктів від дії інформаційних загроз та захисту від нерозголошення даних, які становлять комерційну таємницю підприємства [191]. Таким чином, акцентується увага саме на інформаційній безпеці, інформаційних загрозах, і таким чином складається враження, що і джерелом загроз і об'єктом захисту виступає інформація, тобто представлено всі ознаки інформаційної безпеки, що дещо на нашу думку спрощує складні процеси, пов'язані із впровадженням цифрових технологій, їх потужний вплив на діяльність підприємства та стан його безпеки загалом.

У дослідженнях Н. Аванесової, О. Мордовцева, Т. Колодяжної також наголошується на ознаках та дії цифрової безпеки і представлено трактування, за яким цифрова безпека виступає головною складовою інформаційної безпеки, спрямованою на комплексне впровадження заходів, які забезпечують захист, конфіденційність, доступність та цілісність інформаційних ресурсів підприємства та їх захист від несанкціонованого впливу та вірусних атак [192]. Таким чином представлено новий, відмінний від інших науковців, авторський погляд на цифрову безпеку як невід'ємну складову інформаційної безпеки підприємства, що на нашу точку зору більше відповідає дійсності, хоч і не розкриває взаємозв'язку цифрової безпеки з іншими безпековими складовими в системі економічної безпеки підприємства, а отже залишає більше запитань, ніж відповідей.

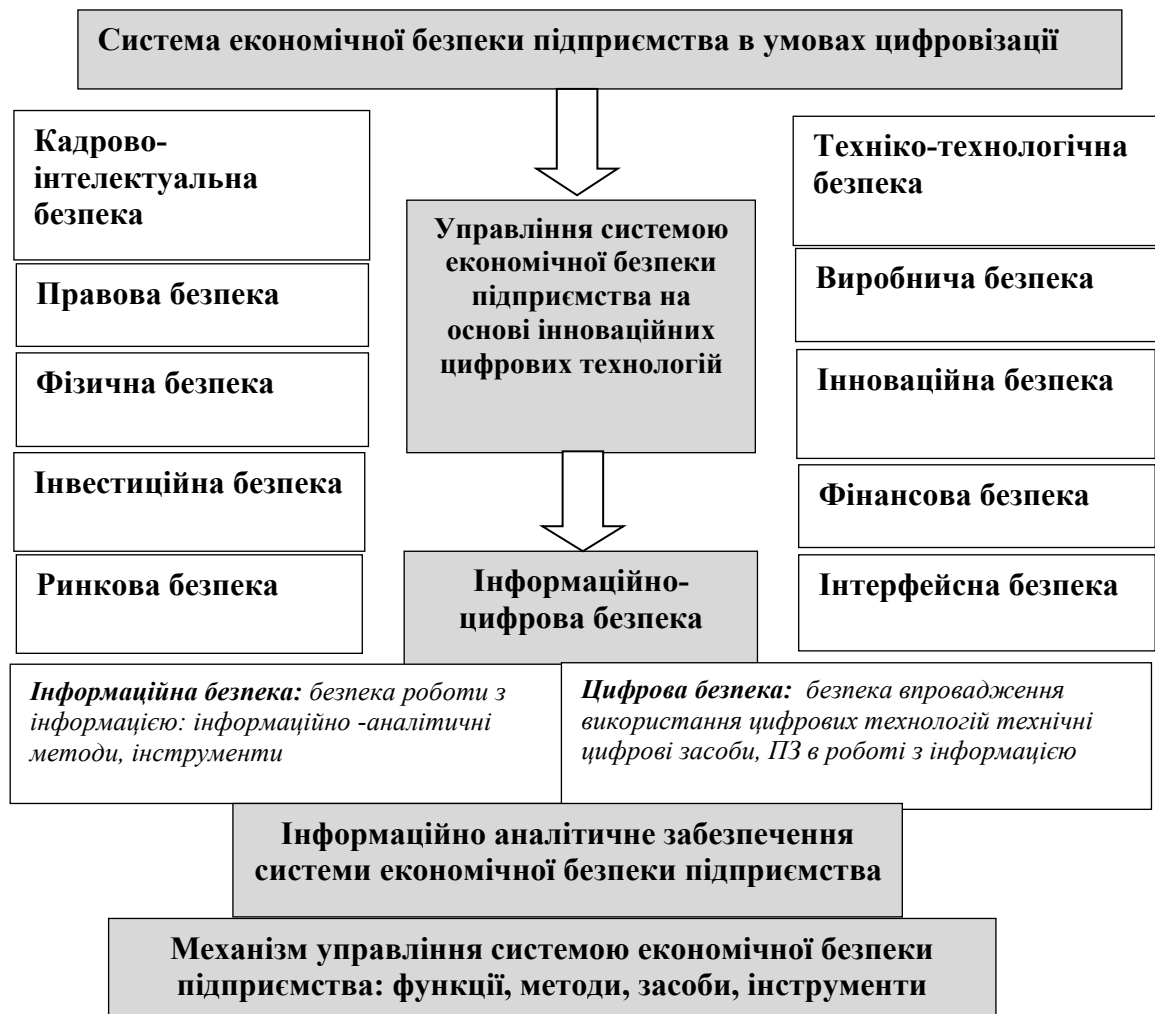


Рис. 1.6. Управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій

Джерело: сформовано автором на основі [193-215]

Дослідження сутності і значення інноваційних цифрових технологій та їх зв'язок з іншими складовими, роль та значення в системі економічної безпеки дає можливість констатувати наявність, очевидність функціональних ознак поєднання інформаційної складової системи економічної безпеки та нової цифрової безпеки, що дає можливість зробити висновок про наявність інформаційно-цифрової складової як невід'ємної частини системи економічної безпеки підприємства, яка поєднує в собі показники, за якими можна виміряти стан та рівень як інформаційної, так і цифрової безпеки підприємства, а також технічні, інформаційні та цифрові засоби, які дають

можливість забезпечувати належний рівень економічної безпеки підприємства в умовах цифровізації та масового впровадження нових цифрових технологій.

Таким чином, в роботі визначено сутність інформаційно-цифрової складової системи економічної безпеки підприємства, яка поєднує в собі ознаки та функції інформаційної складової системи економічної безпеки та їх зв'язку з новою цифровою складовою, що разом надають технології, інструменти та засоби і мають значно ширші можливості для впровадження ефективного інформаційно-аналітичного забезпечення та надають комплексний дієвий захист підприємства, адаптований до протидії реалізації небезпек і загроз зовнішнього ринкового та внутрішнього середовища в умовах впровадження технологій Четвертої промислової революції, Індустрії 4.0. та нових технологічних викликів і змін.

До показників, за якими доцільно здійснювати аналіз та оцінку цифрової безпеки науковці відносять показники: частки співробітників, які здійснюють свою роботу з віддаленим доступом завдяки якому є зрозумілим наскільки працівники які працюють віддалено залучені, застосуванням інноваційних технологій в безпосередні процеси виконання робіт [190]. Наступним показником науковці визначають коефіцієнт застосування наскрізних технологій, таких як роботизація, штучний інтелект, нейротехнології, великі дані, блокчейн, нових виробничих технологій. Відповідно, за цим показником оцінюється застосування підприємством зазначених технологій та здійснення активного трансферу інновацій та також визначаються можливості підприємства до успішної адаптації в умовах, що змінюються.

Наступним показником, визначеним науковцями, є показник застосування цифрового маркетингу, який визначається як відношення наявного інструментарію цифрового маркетингу до загального обсягу інструментів, які використані маркетингом цього господарського суб'єкту. Водночас, під поняттям цифрового маркетингу науковці розуміють застосування нових цифрових технологій, інтерактивного маркетингу в процесі просування та продажу продукції [190]. Наступним показником

цифрової безпеки виділено показник залучення до реалізації діджітал-проектів, який визначає ефективність впровадження суб'єктом господарювання цифрових інноваційних технологій з метою виконання задач операційної чи соціальної діяльності. Його розрахунок здійснюється експертним методом, а методикою розрахунку є методичні рекомендації Програми ЄС ««EU4Digital: підтримка цифрової економіки та суспільства у Східному партнерстві» [216, 217]. Цей показник застосовується для вимірювання результатів прискореного впровадження цифрових інноваційних технологій в економічній та соціальній сферах, а тому є показником широкого застосування для суб'єктів господарської діяльності у всіх сферах економічної діяльності. На нашу точку зору, запропоновані наразі авторами показники не надають можливості для ґрунтовного аналізу стану впровадження інноваційних цифрових технологій на підприємстві загалом та в системі його економічної безпеки зокрема, а тому на наш погляд ця проблема залишається невирішеною і потребує впровадження подальших наукових досліджень.

Втім, на нашу думку, зазначені показники-індикатори впровадження інноваційних цифрових технологій які представлено як індикатори нової цифрової безпеки не повною мірою відображають саме безпекові аспекти їх застосування в аналізі та оцінюванні впровадження цифрових технологій в забезпеченні безпеки. Тоді як ключовою перевагою застосування таких нових інноваційних цифрових технологій з позицій безпеки є можливість підприємства своєчасно на відповідному рівні виявляти ризики, загрози та небезпеки сучасного динамічного інформаційного, ринково-суспільного середовища, здійснювати оперативний і водночас точний аналіз цих нових загроз та ризиків, джерел їх походження та розширити методи й інструментарії своєчасної адекватної протидії цим ризикам, загрозам та нейтралізації впливу їх негативних наслідків, найбільш оптимізовано з позиції найкращого результату за найбільш оптимізованої, мінімальної витрати всіх видів ресурсів: кадрових, фінансових, часових, матеріальних, технологічних. На наш погляд, саме це робить застосування сучасних цифрових технологій в

забезпеченні безпеки підприємств життєво необхідним, оскільки за умов переходу до технологій Четвертої промислової революції така цифрова трансформація системи безпеки із впровадженням нових технологій є не питанням вибору, а питанням виживання, об'єктивної необхідності. Водночас, впровадження інноваційних цифрових технологій та забезпечення належного захисту підприємств в існуючих умовах здатне забезпечувати економію всіх видів ресурсів за кращу результативність безпекових дій, заходів, зменшувати витрати, забезпечувати належний рівень технологічної та ринкової конкурентоспроможності підприємства, його продукції, відповідність вимогам і потребам часу ринку та вимогам, очікування споживачів, а отже забезпечувати стабільність, прибутковість розвитку бізнесу в довготривалій перспективі.

Узагальнено завдання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства можна представити наступним чином (рис. 1.7).

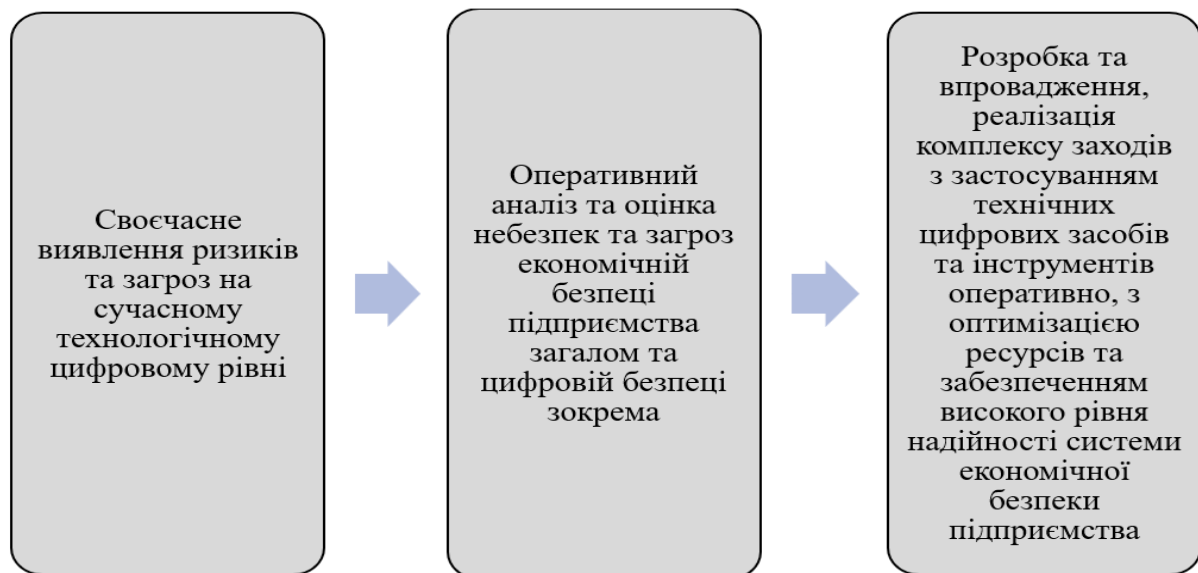


Рис.1.7. Завдання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства

Джерело: сформовано автором на основі: [218-229]

Узагальнюючи зазначимо, що головними завданнями впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства є: (1) своєчасне виявлення ризиків та загроз на сучасному технологічному цифровому рівні; (2) оперативний аналіз та оцінка небезпек та загроз економічній безпеці підприємства загалом та цифровій безпеці зокрема; (3) розробка та впровадження, реалізація комплексу заходів з застосуванням технічних цифрових засобів та інструментів, з оптимізацією ресурсів та забезпеченням високого рівня надійності системи економічної безпеки підприємства.

На думку М. Белобородової в сучасних економічних умовах фактично відбувається формування нового цифрового середовища, осередками якого стають безпосередньо підприємства [230]. Складовими такого середовища виступає автоматизація процесів виробництва продукції та її подальшої реалізації із застосуванням цифрових систем та технологій, автоматизацією, цифровізацією бізнес-процесів та впровадження систем е-комерції, формування нових комунікацій взаємодії з державними органами та структурами через державні цифрові портали надання послуг та отримання звітності, впровадження так званої концепції «спільного споживання» та систем забезпечення цифрової безпеки. Водночас, формування такого цифрового середовища підприємства спонукає до необхідності впровадження нових регламентів в системах роботи, внутрішніх та зовнішніх комунікаціях підприємств, в забезпеченні економічної безпеки та функціонуванні самих безпекових систем.

Однією із нових загроз сьогодення науковцями визначається зростання залежності від інформаційних систем та технологій, це пов'язано передусім з широким використанням автоматизації процесів виробництва продукції чи виконання операцій в автоматизованих системах [189]. Важливою перевагою сучасних цифрових систем називають можливість опрацювання значних обсягів інформації за короткі інтервали часу, що забезпечує також можливості керування даними, в тому числі із застосуванням технологій віддаленого

доступу. Цифрові технології застосовуються для розбудови сучасних систем ведення обліку та звітності, здійснення управлінського обліку. Зазначимо, що комбінування нових цифрових технологій, інструментів таких як штучний інтелект, технологій машинного навчання і аналітики даних, дають можливість ефективно дослідити внутрішньогосподарські процеси та здійснювати контроль за діяльністю. Водночас, вони дають можливість аналізу, оцінки зовнішніх ринкових процесів, конкурентного середовища, виявлення та дослідження потреб та поведінки споживачів, тенденцій та зміни ринкового попиту.

З позицій безпеки в стратегічній перспективі впровадження таких цифрових технологій забезпечує можливості до визначення стратегічних напрямів розвитку та впровадження відповідної структурної, товарної політики, яка забезпечуватиме як довготривалий ефективний розвиток та стабільність підприємств, так і відповідно забезпечуватиме належний високий рівень економічної безпеки. З позицій тактичного, ситуативного управління використання цифрових електронних технологій в системі економічної безпеки дає можливість здійснювати моніторинг, стеження за параметрами зовнішнього та внутрішнього середовища та своєчасно виявляти тактичні, потенційні загрози та ризики на етапах їх перших проявів, що сприяє прийняттю та реалізації термінових заходів щодо протидії потенційним чи тактичним ризикам та загрозам, їх своєчасній нейтралізації. Найбільш поширеною є думка про те, що найкращий захист підприємства від небезпек та загроз - це впровадження превентивних дій та недопущення можливостей для їх практичної реалізації.

Цифрові технології є тим універсальним і водночас унікальним інструментарієм та засобами безпеки, комплексне та окреме застосування яких дає нові, значно ширші можливості для розбудови та функціонування дієвої системи економічної безпеки здатної ефективно забезпечити захист та стабільне функціонування об'єктів господарювання в довгостроковій перспективі в умовах сучасних соціально-економічних змін та викликів.

Впровадження системи моніторингу стану та рівня економічної безпеки підприємства успішно вирішує комплексне застосування таких технологій як машинне навчання, штучний інтелект, аналітика великих даних, здатних здійснити швидке опрацювання значних обсягів інформації, що не під силу здійснити окремим працівникам чи цілим підрозділам, виявити тенденції і здійснити математичне моделювання та подальше прогнозування розвитку подій. Впровадження таких цифрових технологій здатне забезпечити моніторинг ринкових змін, поведінки споживачів та зміни конкурентного ринкового середовища в режимі реального часу, що дають можливість до оперативної зміни в процесах, оперативного прийняття рішень та завдяки об'єктивному обґрунтуванню суттєво покращують якість та своєчасність прийняття управлінських рішень у всіх сферах функціонування, що загалом підвищує об'єктивність роботи всього підприємства та забезпечує зростання рівня його економічної безпеки.

Проте, на застосування цих технологій також впливають нові для підприємств небезпеки та ризики, такі як кіберзлочинність, технологічні зупинки, помилки, які можуть відбуватися у функціонуванні систем та значна нестабільність ринкового середовища, що робить його складно прогнозованим навіть для потужних аналітичних методів роботи з інформацією, що загалом здатне посилити ризики економічній безпеці підприємства.

Зазначимо, що сучасний рівень цифровізації та цифрові трансформації, які очікують в майбутньому докорінно змінюють як внутрішні процеси здійснення фінансової, операційної, виробничої та управлінської діяльності, так і зовнішні бізнес-процеси взаємодії із стейкхолдерами, державними органами та структурами, споживачами на внутрішньому та міжнародному ринках, відкриваючи нові можливості та демонструючи нові загрози. Саме тому впровадження цифрових технологій в забезпеченні безпеки надає сучасні засоби та інструменти, необхідні для ефективного функціонування підприємства та забезпечення високого рівня безпеки.

Сучасні інформаційні системи створюють платформи, на яких здійснюється збереження, робота з інформацією та відображається подальша передача та поширення цієї інформації. Зазначимо, що впровадження таких інформаційних цифрових платформ дає можливість вивільнити кадрові ресурси працівників з рутинних одноманітних задач, передати їх виконання автоматизованим системам, ботам, штучному інтелекту, натомість кадрові ресурси працівників перерозподіляються для виконання більш складних задач, які потребують формування відповідних компетентностей працівників, а отже зростають вимоги до якості кадрових ресурсів. Все це разом дає можливість оптимізувати витрати та забезпечити зростання ефективності діяльності та забезпечити подальший розвиток підприємств.

Висновки до Розділу 1.

Узагальнюючи дослідження праць науковців з питань формування теоретично-методичних засад розбудови та функціонування систем економічної безпеки підприємства слід зазначити наявність та дію трьох рівнів підходів: а саме: (1) наукових підходів до розуміння поняття економічної безпеки підприємства таких як: захисний, стійкісний, гармонізаційний, адаптивний, конкурентний, підхід з позицій реалізації власних стратегічних економічних інтересів, комплементарний та комплексний; (2) наукових підходів до розуміння системи економічної безпеки підприємства таких як: системний, цільовий, процесний, структурний, комплексний, функціональний та ситуаційний наукові підходи; (3) управління системою економічної безпеки підприємства здійснюється на засадах ресурсно-функціонального, програмно-цільового, ситуаційного, стратегічного, системного та інституційного підходів.

У роботі обґрунтовано новий технологічний підхід до управління системою економічної безпеки підприємства як сукупності підсистем,

складових та елементів, взаємодія яких реалізується із застосуванням сучасних цифрових технологічних засобів та технологій, що забезпечує ефективне функціонування механізму системи безпеки та використання методів, інструментів, технологій управління, найбільш оптимальне раціональне використання її кадрових, фінансових, матеріальних ресурсів та зростання рівня безпеки підприємства завдяки широкому використанню технологічних можливостей і зростанню ролі та значення інформаційно-аналітичного забезпечення системи економічної безпеки підприємства в прийнятті управлінських рішень.

Систематизовано наукові концепти сутності та узагальнено функції застосування цифрових технологій в управлінні: облікову, логістичну, безпекову, інформаційно-аналітичну, комунікаційну, операційну, маркетингову функції, застосування яких забезпечує можливість впровадження цифровізації, цифрової трансформації бізнес-процесів у всіх функціональних сферах діяльності підприємства та формуванні якісно нових комунікацій співпраці і взаємодії з партнерами, стейкхолдерами зовнішнього, глобального середовища, що дасть можливість оптимізувати та зменшити витрати, забезпечити зростання економічної та ринкової ефективності діяльності підприємства.

В роботі визначено сутність інформаційно-цифрової складової системи економічної безпеки підприємства, яка поєднує в собі ознаки та функції інформаційної складової системи економічної безпеки та цифрової складової, що разом надають технології, інструменти та засоби і мають значно ширші можливості для впровадження ефективного інформаційно-аналітичного забезпечення та надають комплексний дієвий захист підприємства, адаптований до протидії реалізації небезпек і загроз зовнішнього ринкового та внутрішнього середовища в умовах впровадження технологій Четвертої промислової революції, Індустрії 4.0. та нових технологічних викликів і змін.

З метою забезпечення економічної безпеки суб'єктів господарювання в умовах цифровізації необхідним є формування певної інформаційно-цифрової

системи, яка водночас виступатиме складовою системи економічної безпеки підприємства. Ця нова інформаційно-цифрова екосистема, має поєднувати використання нових технологій, таких як аналітика великих даних, хмарні обчислення, штучний інтелект, віртуальна реальність, машинне обчислення, промисловий інтернет речей та нові інформаційні системи ERP, CRM, HRM, SCM, MES, PRM, що дасть широкі можливості до опрацювання значних обсягів інформації та отримання кращого результату. Водночас, отримана таким чином інформація забезпечуватиме можливості для управління ризиками, що виникають у функціонуванні кадрової, фінансової, технологічної, виробничої, ринкової та інших складових системи економічної безпеки підприємства та самого управління такою системою, що забезпечить зростання рівня економічної безпеки підприємства в умовах цифровізації.

Результати проведених досліджень та розробок висвітлено у працях автора: [231, 232, 233, 234].

РОЗДІЛ 2. ХАРАКТЕРИСТИКА СТАНУ ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1. Аналіз стану впровадження інноваційних цифрових технологій в діяльності підприємств

Дослідження стану та рівня впровадження інноваційних цифрових технологій в діяльності підприємств слід розпочати з основи, яка створює можливості використання інноваційних цифрових технологій загалом – це наявності та доступу до мережі Інтернет.

На перший погляд складається враження, що користування мережами Інтернет є абсолютно доступним для всіх у країні без винятку, як населення, приватних користувачів, так і організацій. Проте, розгляд інформації, представленої в зведених даних Державної служби статистики свідчить про те, що такого загального, стовідсоткового всеосяжного покриття мережами Інтернет всіх користувачів не існує, а відсоток використання Інтернет на підприємствах і різних напрямках економічної діяльності має значні відмінності. З позицій економічної безпеки сама відсутність доступу до Інтернет з робочих місць користувачів може становити загрозу, оскільки будуть відсутні можливості використання сучасних цифрових технологій та їх переваг у впровадженні виробничої, операційної, облікової, комерційної та всіх інших видів діяльності підприємств. Водночас, наявність доступу до мережі Інтернет не забезпечує міцної безпеки, скоріше навпаки, без належного рівня впровадження безпекових заходів доступ до Інтернет-ресурсів користувачів, працівників підприємств збільшує ризики зовнішніх агресивних дій та несе в собі нові кібер-загрози для підприємства, яке до цього виявляється неготовим та не зданим протидіяти.

В таблиці 2.1. представлено інформацію щодо кількості підприємств, які мають доступ до мережі Інтернет за видами економічної діяльності.

Таблиця 2.1.

Кількість підприємств, які мають доступ до мережі Інтернет за видами економічної діяльності

Види економічної діяльності	Кількість підприємств, які мають доступ до мережі Інтернет, одиниць					
	2018	2019	2021	2022	2023	2024
Усього	43303	43785	44508	42785	34204	33547
Переробна промисловість	10878	11089	11323	11072	8540	8530
Виробництво харчових продуктів, напоїв і тютюнових виробів	2071	2046	2065	2051	1722	1765
Текстильне виробництво	890	927	963	921	660	659
Виготовлення виробів з деревини, паперу та поліграфічна діяльність	1264	1305	1352	1311	940	959
Виробництво коксу та продуктів нафтоперероблення	47	39	42	40	21	28
Виробництво хімічних речовин та хімічної продукції	419	460	458	438	371	411
Виробництво фармацевтичних препаратів	104	103	109	101	84	106
Виробництво гумових і пластмасових виробів	1628	1608	1662	1645	1326	1210
Металургійне виробництво, виробництво металевих виробів	1290	1315	1372	1327	1040	972
Виробництво комп'ютерів, електронної та оптичної продукції	248	258	260	254	165	191
Виробництво електричного устаткування	345	383	358	349	268	292
Виробництво машин і устаткування	906	924	912	907	670	650
Будівництво	4783	4883	5141	4714	3522	3315
Оптова та роздрібна торгівля	10759	10742	10630	10229	8656	8532
Транспорт, складське господарство, поштова та кур'єрська діяльність	3462	3553	3590	3422	3185	3159
Тимчасове розміщення і організація харчування	1279	1261	1293	1240	770	688
Інформація та телекомунікації	1949	1946	1971	1935	1466	1455
Телекомунікації (електрозв'язок)	363	368	384	375	305	305
Комп'ютерне програмування	875	917	937	919	794	771
Операції з нерухомим майном	2704	2697	2796	2591	2153	1997
Професійна, наукова та технічна діяльність	2636	2685	2638	2597	1854	1827
Наукові дослідження та розробки	303	302	301	297	199	202
Інформаційно-комунікаційні технології, загалом	1456	1567	1670	1621	1390	1363

Джерело: сформовано на основі даних [235]

Досліджуючи підприємства в різних сферах економічної діяльності слід зазначити, що поширення доступу до мережі Інтернет протягом 2018-2014 рр. в різних галузях та сферах економічної діяльності відбувалося нерівномірно, проте в жодній із сфер економічної діяльності станом на кінець 2024 р. впровадження доступу до Інтернет-мереж серед працівників підприємств галузі не досягнуло 100%. Так, станом на 2018 р. найвищим рівень доступу до Інтернет спостерігався в сфері виробництва комп'ютерів, електронної та оптичної продукції та становив 95,8% від загальної кількості підприємств цього виду економічної діяльності, а станом на 2024 р. рівень доступу до Інтернет робочих місць працівників підприємств досягнув 97,2%.

В сфері ремонту комп'ютерів, обладнання та зв'язку показники доступу працівників до мережі Інтернет також є одними із найвищих. Станом на 2018 р. доступ до Інтернет мали 94,1%, станом на 2024 р. цей показник досягнув 99,7% від загальної кількості підприємств цієї сфери. Один із найвищих показників доступу до Інтернет є в сфері інформаційно-комунікаційних технологій та зв'язку, і якщо станом на 2018 р. частка підприємств з доступом до Інтернет становила 89,9%, то до 2024 р. ця частка зросла до 97,3%.

Рівень доступу підприємств до мережі Інтернет є високим у галузі телекомунікацій та електрозв'язку зі зростанням частки охоплених мережею Інтернет підприємств з 95,3% у 2018 р. до 99,2% підприємств у 2024 р. В сфері комп'ютерного програмування та консультування відсоток підприємств, що мають доступ до мережі Інтернет та використовують його є також значним та демонструє зростання із показника 86,2% у 2018 р. до 97,7% від загальної кількості підприємств в сфері комп'ютерного програмування у 2024 р.

Незважаючи на важливе значення доступу до Інтернет-мереж та можливості отримання необхідної наукової інформації, доступу до баз даних, обміну знаннями, досягненнями науки та техніки для підприємств, що проводять наукові дослідження та розробки загалом частка таких підприємств з доступом до Інтернету з 2018 р. до 2024 р. навпаки зменшилася, з 91,5% у 2018 р. до 86,8% у 2014 р., що може бути викликано в тому числі і вимогами

щодо підвищення рівня безпеки та особливості проектів, над якими працюють підприємства та значного зменшення самої чисельності реально працюючих станом на 2024 р. підприємств в цій сфері діяльності.

Низьким є рівень доступу до Інтернету в сфері професійної наукової та науково-технічної діяльності. Так, станом на 2018 р. доступ до Інтернет мали 88,4% організацій в сфері професійної, науково-практичної діяльності, а станом на 2024 р. цей показник зріс до 90,2% від всієї кількості організацій в цій сфері.

Серед підприємств переробної промисловості частка підприємств, що впровадили доступ до Інтернет є високою і станом на 2024 р. в середньому становила 94%. Взагалі, аналізуючи відсоток підприємств, що мають доступ до мережі Інтернет у всіх сферах діяльності слід зазначити, що їх кількість станом на 2018 р. становила 43303 підприємства, а загальна частка 88% від загальної кількості підприємств, що працюють в економіці загалом. Проте, протягом 2018-2024 рр. сама кількість підприємств значно зменшилася. Станом на 2024 р. частка підприємств, що мають доступ та використовують мережу Інтернет становила 33547, або 93,8% від загальної чисельності підприємств.

Іншими важливими даними, які можуть свідчити про активність впровадження сучасних цифрових технологій є кількість працівників підприємств, що мають доступ до мереж Інтернет та активно використовують їх у здійсненні своєї професійної діяльності. Цей показник ми визначаємо як рівень комп'ютеризації робочих місць(табл. 2.2.).

Досліджуючи дані щодо кількості працівників, які мають доступ до мереж Інтернет та можуть використовувати їх виконуючи свою професійну діяльність зазначимо, що загалом частка таких підприємств є критично малою та недостатньою для забезпечення ефективного функціонування. Досліджуючи представлені в таблиці 2.2. показники зазначимо, що найбільш доступними мережі Інтернет є для працівників сфери інформаційно-комунікаційних технологій, у яких станом на 2019 р. доступ до мереж Інтернет

мали 78% співробітників, а станом на 2021 р. – 86,5% працівників. За період 2022-2024 рр. частка працівників, що мають доступ до Інтернет значно зменшилася і на 2024 р. становить 72,6%, проте причиною таких змін є не саме згортання Інтернет активності компаній, а зменшення чисельності працівників, які активно працюють в сфері ІТ у зв'язку з військовою агресією, зменшенням території країни та значним згортанням активності у всіх сферах та видах економічної діяльності суб'єктів господарювання.

Таблиця 2.2

Кількість зайнятих працівників, які мають доступ до мережі Інтернет, за видами економічної діяльності та з розподілом за кількістю зайнятих працівників у 2018, 2019, 2021-2024 рр.

Види економічної діяльності	Кількість зайнятих працівників, які мають доступ до мережі Інтернет, осіб					
	2018	2019	2021	2022	2023	2024
Усього	1064745	1090035	1133069	1105857	1103801	1104748
У %	27,1	28,4	28,0	28,2	32,8	35,5
Переробна промисловість	255685	257644	261207	271624	278603	275929
У %	19,2	19,9	20,6	22,5	27,6	29,8
Виробництво харчових продуктів, напоїв і тютюнових виробів	58825	58815	59839	69165	83783	79778
У %	19,2	19,4	19,7	23,5	32,1	31,9
Легка промисловість	9021	9861	9869	10624	12479	11598
	10,9	12,2	13,4	15,4	20,1	19,3
Оптова торгівля	179210	183532	190909	178291	207983	186184
У %	52,0	51,7	52,2	48,8	64,9	63,8
Роздрібна торгівля	130408	139406	141502	148463	152689	169154
У %	32,6	35,4	31,7	32,2	36,4	45,7
Професійна, наукова та технічна діяльність	77246	80347	82355	71758	66750	58210
У %	60,6	60,2	60,9	59,4	65,2	61,4
Інформаційно-комунікаційні технології	70076	57807	59281	61072	60388	65882
У %	73,3	78,0	86,5	61,9	67,3	72,6
Наукові дослідження та розробки	12354	13157	13290	10759	11289	8629
У %	42,1	44,7	46,1	41,9	53,0	42,2

Джерело: сформовано на основі даних [235]

Другим за активністю напрямом використання мереж Інтернет є оптова торгівля, оскільки частка працівників у сфері оптової торгівлі, працівники якої використовують Інтернет на 2018 р. становила 52%, а станом на 2024 р. зросла до 63,8% від загальної кількості працівників, задіяних в цій сфері економічної діяльності. При цьому, частка використання мереж Інтернет працівниками підприємств оптової торгівлі в період 2022-2024 рр. всупереч загальній тенденції не зменшилася, а навпаки зросла, що пов'язано із активним розвитком інтернет-торгівлі та віртуалізацією оптових ринків переходом цієї сфери діяльності на роботу з використанням електронних цифрових платформ.

Третім за активністю використання напрямком є сфера професійної наукової та технічної діяльності де доступ до мереж Інтернет, станом на 2018 р. мали 60,6% працівників. При цьому, в період 2019-2024 рр. ця частка залишалася фактично стабільною та лише станом на 2023 р. зазнала незначного зростання до 65,2%, а на 2024 р. доступ до мереж Інтернет мали 61,4% від загальної кількості працюючих. Значно нижчим цей показник є серед організацій в сфері наукових досліджень та розробок. Так, станом на 2018 р. частка працівників, які мають доступ та використовують Інтернет мережі в своїй професійній діяльності становила 42,1%. За період 2019-2022 рр. ця частка фактично не зменшилась, у 2023 р. зросла до 53%, а у 2024 р. знову зменшилася до свого попереднього рівня – 42,2%.

Значно нижчою є активність використання мереж Інтернет працівниками в галузях легкої промисловості – від 10,9% станом на 2018 р. до 19,3% у 2024 р. Загалом, в галузях переробної промисловості станом на 2018 р. доступ до мереж Інтернет мали 255685 працівників, що становило 19,5% від загальної чисельності працюючих. За період 2019-2024 рр. ця частка зросла до 275929 осіб та склала 29,8% від загальної кількості працюючих на підприємствах переробної промисловості країни. Підсумовуючи зазначимо, що загалом в економіці країни в період 2018-2024 рр. частка працівників, що мають доступ до мереж Інтернет зросла у 2018 р. до 35,5% у 2024 р. та охопила 110448 осіб, проте незважаючи на певну позитивну динаміку, залишається

незначною, що свідчить про низький рівень використання мереж Інтернет, програмного забезпечення, інформаційних технологій в операційній та виробничій діяльності підприємств, низького рівня впровадження цифровізації, автоматизації процесів та операцій виробництва.

Частка підприємств, що мають мобільні додатки для просування та реалізації продукції послуг за видами економічної діяльності у 2024 р. представлена на рис. 2.1.

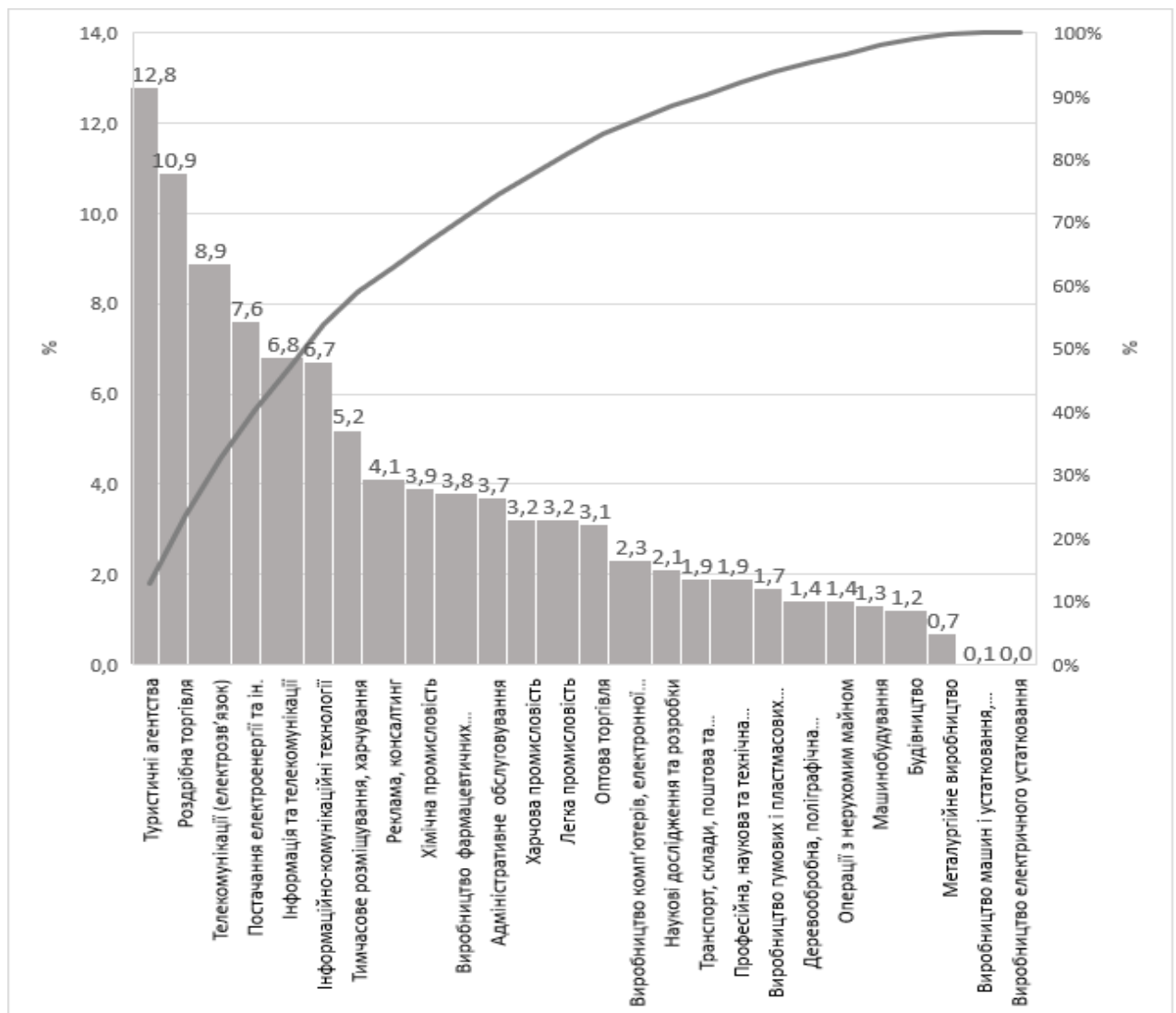


Рис. 2.1. Частка підприємств, що мають мобільні додатки для просування і реалізації продукції та послуг за видами економічної діяльності у 2024 р.

Джерело: сформовано на основі даних [235]

Одним із найбільш активних напрямів впровадження та використання інформаційно-комунікаційних технологій серед підприємств в різних сферах економічної діяльності є створення та використання мобільних додатків для роботи з клієнтами, просування та реалізації продукції чи послуг. Мобільні додатки стали фактично головною ланкою, яка забезпечує доступ до фінансових послуг, які надають банки та інші фінансові організації; заклади в сфері здоров'я, оскільки саме завдяки мобільному додатку здійснюється запис на прийом, обстеження, отримання ліків за рецептами та інші операції медичного обслуговування; в освіті з метою здійснення онлайн навчання та інших сферах. Саме тому складається загальне враження про високу активність організацій у розробці та впровадженні мобільних додатків, проте дані Державної служби статистики України наведені на рис. 2.1 свідчать про те, що загальний рівень відповідної активності підприємств у всіх сферах економічної діяльності загалом залишається низьким, а дієвість у впровадженні та використанні мобільних додатків суттєво залежить від сфери економічної діяльності суб'єктів господарювання. Так, найвищим є рівень активності використання мобільних додатків серед підприємств туристичної сфери 12,8% від загальної кількості підприємств в цій сфері економічної діяльності.

На другому місці за активністю поширення та використання мобільних додатків є роздрібна торгівля, де мобільні додатки є у 10,9% підприємств. Мобільні додатки станом на 2024 р. мають 8,9% підприємств сфери телекомунікацій (електрозв'язку) та 6,8% підприємств, що працюють в сфері інформаційних та телекомунікаційних технологій. Активно використовують мобільні додатки в роботі із своїми користувачами та абонентами підприємства в сфері електропостачання, газу, теплової енергетики мобільні додатки мають 7,6% від загальної кількості підприємств. Проте загалом, рівень використання мобільних додатків підприємствами переробної промисловості є дуже низьким та становить 2% від загальної кількості підприємств. Найнижчим, менше 1%, є рівень використання мобільних

додатків підприємствами машинобудування, що обумовлено цілком об'єктивними чинниками специфіки їх економічної діяльності. Проте, є сфери такі як транспорт, складське господарство, надання поштових та кур'єрських послуг чи будівництво, які за своїми особливостями, характером діяльності потребують значно ширшого використання мобільних додатків як інструменту просування продукції та послуг, але станом на 2024 р. використовують ці інструменти на вкрай низькому рівні.

В сучасному інформаційному середовищі невід'ємним елементом та візитівкою для будь-якого бізнесу є наявність власного сайту.

В таблиці 2.3. представлено дані щодо частки кількості підприємств, які мають веб-сайт серед загальної кількості підприємств за відповідними сферами діяльності.

На перший погляд складається враження, що Інтернет-сайти, сайти, візитівки наповнені всілякою комерційною інформацією та спрямовані не лише на коротке ознайомлення, а на підтримку бізнес-процесів просування та реалізації продукції є фактично у кожного підприємства. Проте, це далеко не так і про це свідчать статистичні дані.

Так, серед підприємств харчової промисловості часом на 2018 р. власні сайти мали 35,4% підприємств, а за період 2019-2024 рр. їх частка зросла та на 2024 р. становила 40,5% від загальної кількості підприємств харчової промисловості. Значно нижчим цей показник є для підприємств легкої промисловості, де станом на 2024 р. власні сайти є у 32,6% підприємств.

Одним із найбільш високих є показник наявності сайтів у підприємств, що працюють в сфері телекомунікацій та електрозв'язку, оскільки у 2019 р. частка таких підприємств становила 72,2%, а до 2024 р. зросла до 73,6% від загальної кількості підприємств. Станом на 2024 р. власні сайти мають 60,3% підприємств, які працюють в видавничому бізнесі чи виробництві кінопродукції.

Таблиця. 2.3.

Частка підприємств, що мають веб-сайт, у загальній кількості підприємств за видами економічної діяльності

Види економічної діяльності	Частка підприємств, які мають веб-сайт, у загальній кількості підприємств за видами економічної діяльності, %			
	2018	2019	2021	2024
Усього	35,6	35,2	35,3	38,2
Переробна промисловість	43,7	43,2	44,1	46,7
Харчова промисловість	35,4	35,4	35,3	40,5
Легка промисловість	26,9	27,8	28,3	32,6
Деревообробна промисловість	37,9	36,6	37,0	38,4
Виробництво коксу та продуктів нафтопереробки	40,7	39,5	41,7	43,9
Виробництво хімічних речовин і хімічної продукції	49,8	50,4	49,9	53,0
Фармацевтична промисловість	62,4	64,3	66,7	70,6
Виробництво гумових і пластмасових виробів	45,0	42,7	47,2	47,6
Металургія	48,5	48,4	50,3	50,5
Виробництво комп'ютерів, електронної продукції	70,3	67,9	68,6	71,0
Виробництво електричного устаткування	62,0	61,6	62,0	62,2
Виробництво машин і устаткування, н.в.і.у.	61,4	61,4	61,4	62,1
Виробництво автотранспортних засобів	61,5	61,6	62,1	62,3
Меблева промисловість	40,8	39,4	38,2	42,8
Постачання електроенергії, газу, пари	30,3	31,9	28,8	35,3
Постачання електроенергії, газу, пари та повітря	42,2	43,0	41,8	46,8
Водопостачання; каналізація, поводження з відходами	22,8	25,0	24,3	27,0
Будівництво	25,1	24,0	23,6	25,9
Оптова торгівля	41,2	40,3	41,9	47,1
Роздрібна торгівля	20,7	21,2	22,1	27,4
Транспорт, складське господарство, поштова діяльність	22,4	22,1	21,4	21,4
Тимчасове розміщування	63,3	62,0	60,2	65,6
Інформація та телекомунікації	57,4	57,1	57,1	57,3
Видавнича діяльність; виробництво кіно	58,8	58,3	60,1	60,3
Телекомунікації (електрозв'язок)	72,2	72,9	72,9	73,6
Комп'ютерне програмування, консультування	50,7	50,3	49,3	49,4
Операції з нерухомим майном	23,4	24,5	23,6	23,8
Професійна, наукова та технічна діяльність	44,6	43,6	43,8	47,5
Консалтингові послуги	43,3	41,4	41,1	45,4
Наукові дослідження та розробки	52,3	53,5	53,8	54,0
Рекламна діяльність, наукова та технічна діяльність	45,0	45,6	47,7	52,1
Діяльність туристичних агентств	66,5	66,3	64,3	66,7
Ремонт комп'ютерів і обладнання зв'язку	58,8	59,7	54,9	55,0

Джерело: сформовано на основі даних [235]

Одним із найвищих рівнів зростання у розробці та впровадженні власних веб-сайтів мають підприємства в сфері виробництва комп'ютерів, електронної та оптичної продукції. Так, серед цих підприємств станом на 2024 р. сайт мають 71% підприємств. Значною є частка наявності власних веб-сайтів серед підприємств фармацевтичної промисловості, станом на 2024 р. – 70,6% від загальної кількості фармацевтичних підприємств, що свідчить про значну публічність та соціальну орієнтованість їх діяльності, турботу про формування позитивного іміджу та ділову репутацію, адже такої операційної потреби у них немає.

Незважаючи на критичну необхідність публічності інформаційної роботи з клієнтами станом на 2024 р. сайти є лише у 23,8% підприємств, які працюють в сфері операцій з нерухомістю, що свідчить про низький рівень активності на цих ринках. Критично низькою є частка підприємств, що мають веб-сайти серед підприємств сфери транспорту, складського господарства, поштової та кур'єрської діяльності станом на 2024 р. – 21,4% від загальної кількості підприємств, що значно менше ніж реальна потреба в таких сайтах, в тому числі з метою активування операційної діяльності цих підприємств. Не об'єктивно низькою є частка наявності власних веб-сайтів серед підприємств в сфері будівництва – лише 25,9% станом на 2024 р., адже від прозорості їх діяльності, ділової репутації, іміджу, який формується на ринку значною мірою залежать обсяги залучених інвестиційних коштів та можливості здійснення їх економічної діяльності. Не менш суперечливими є показники наявності власних веб-сайтів на підприємствах роздрібно́ї торгівлі, серед яких станом на 2025 р. лише 27,4% підприємств мають власні веб-сайти, на відміну від сфери оптової торгівлі, де такий показник є значно вищим і становить 47,1% від загальної кількості підприємств. Вище наведені дані аналізу свідчать про низький рівень загальної активності в розробці власних веб-сайтів, які на сьогоднішній день не лише активують їх комерційну діяльність на ринку, а і значною мірою впливають на формування іміджу, репутації підприємств на

ринку та сприяють активуванню її збутових процесів і здійснюють прямий чи опосередкований вплив на ефективність їх економічної діяльності.

Іще одним важливим показником, за яким можна оцінювати активність використання підприємствами в різних сферах, видах економічної діяльності сучасних цифрових технологій є показник використання соціальних медіа. Частка підприємств, які використовують соціальні медіа, у загальній кількості підприємств за видами економічної діяльності, у % представлена в таблиці 2.4.

Таблиця 2.4

Частка підприємств, які використовують соціальні медіа, у загальній кількості підприємств за видами економічної діяльності, %

Види економічної діяльності	Частка підприємств, що використовують соціальні медіа у % до загальної чисельності підприємств відповідного напрямку			
	2018	2019	2022	2024
Усього	29,7	30,1	29,1	30,0
Переробна промисловість	28,5	29,4	28,3	29,7
Харчова промисловість	28,7	28,8	28,7	33,1
Легка промисловість	24,8	24,9	24,7	25,2
Деревообробна промисловість	26,8	28,8	27,4	27,4
Нафтохімічна промисловість	29,4	29,7	29,3	29,5
Виробництво коксу та продуктів нафтопереробки	29,6	25,6	25,4	25,5
Хімічна промисловість	30,5	32,8	30,7	30,9
Фармацевтична промисловість	40,2	37,4	37,1	39,4
Металургія	29,1	30,4	28,9	29,0
Машинобудування	29,1	30,9	29,5	29,8
Виробництво комп'ютерів, електронної та оптичної продукції	32,4	32,1	31,8	32,0
Виробництво електричного устаткування	29,9	30,7	29,4	29,4
Виробництво машин і устаткування	33,8	34,1	33,9	34,1
Постачання електроенергії, газу, пари	29,8	30,8	29,7	32,4
Будівництво	25,9	25,1	24,9	25,0
Оптова торгівля	31,4	31,4	31,2	31,4
Роздрібна торгівля	27,2	28,7	27,3	28,8
Транспорт, складське господарство, поштова та кур'єрська діяльність	23,0	23,5	23,0	23,0
Тимчасове розміщення й організація харчування	41,0	40,6	40,2	40,4
Наукові дослідження та розробки	28,7	30,3	27,9	30,5
Інформаційно-комунікаційні технології	44,7	44,4	44,0	44,7

Джерело: сформовано на основі даних [235]

В сучасному житті соціальні медіа займають значне місце та набувають все більшого значення як віртуальні медіа не лише для соціального спілкування та комунікацій, а і як нові віртуальні площадки для просування та реалізації продукції, які відкривають широкі можливості впливу на споживачів з сучасними інструментами контекстної реклами, прихованої пропаганди та інших маркетингових інструментів, що активно застосовуються завдяки сучасним соціальним медіа. Проте, незважаючи на загальне розуміння, необхідність та значимість використання соціальних медіа в розбудові сучасних маркетингових комунікацій, проведений аналіз та деталі, представлені в таблиці 2.4. свідчать про недостатній рівень активності підприємств-товаровиробників в їх використанні.

Аналізуючи період 2019-2024 рр. слід зазначити, що найвищий рівень активності у використанні соціальних медіа загалом проявляють фармацевтичні підприємства. Частка фармацевтичних підприємств, що використовують соціальні медіа становила у 2019 р. 40,2% і незважаючи на зменшення у 2024 р. до 39,5%, має один із найвищих рівнів використання серед всіх сфер економічної діяльності. Найвищий рівень використання соціальних медіа демонструють підприємства в сфері інформаційних та комунікаційних технологій, оскільки частка використання соціальних медіа серед цих підприємств становить 44,7 %, при цьому цей показник залишався стабільним на протязі 2019-2024 рр.

Значну активність у використанні соціальних медіа проявляють підприємства, що працюють в сфері тимчасового розміщення та організації харчування. Частка цих підприємств, які використовують соціальні медіа станом на 2019 р. становила 41% і до 2024 р. вона зменшилася до 40,4% і залишається стабільною. У сфері транспорту, складського господарства, поштової та кур'єрської служб частка підприємств, що використовують соціальні медіа станом на 2014 р. становила 23%; невисокий рівень роботи з соціальними медіа у будівельних компаній – 25% від загальної кількості підприємств цієї галузі.

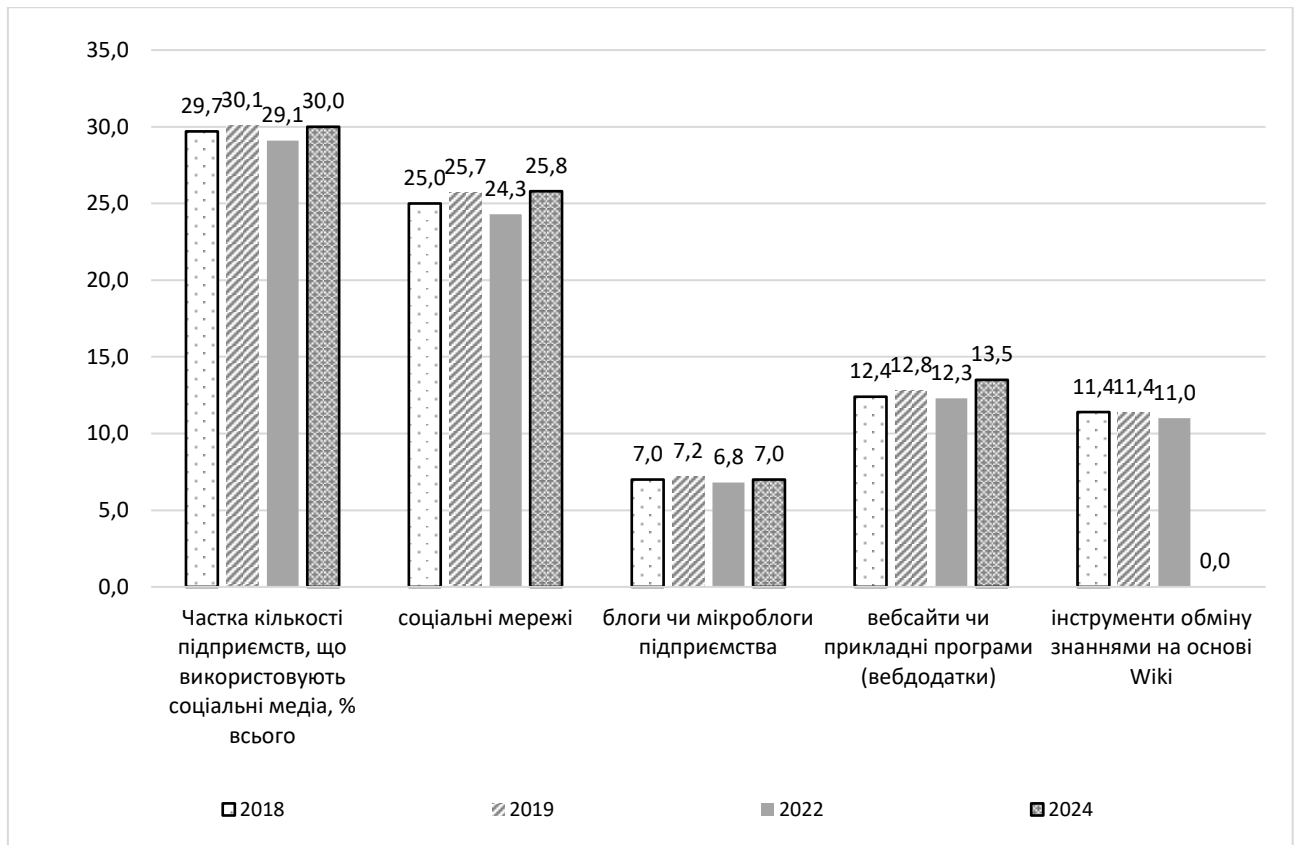


Рис. 2.2. Використання соціальних медіа на підприємствах за видами економічної діяльності у 2018-2024 рр.

Джерело: сформовано на основі даних [235]

Досліджуючи використання соціальних медіа за окремими напрямками в період 2018-2024 рр. слід зазначити, що загалом соціальні медіа у 2018 р. використовували 29,7% підприємств за всіма сферами та напрямками економічної діяльності (рис. 2.2.), до 2024 р. цей відсоток дещо зріс до рівня 30%. При цьому різні інструменти соціальних медіа використовуються підприємствами з різною активністю. Так, найбільш активного застосування (25-25,8%) мають соціальні мережі, реєстрація в них та розміщення безпосередньо інформації про підприємства. Значно менше поширення серед підприємств всіх сфер та напрямів діяльності мають веб-сайти чи веб-додатки для обміну мультимедійним контентом, оскільки кількість підприємств, що використовували їх станом на 2024 р. становила 13,5%. Значно меншого

поширення набуло використання підприємствами блогів та мікроблогів, станом на 2024 р. їх використовували всього 7% підприємств.

Забезпечення зростання ефективності функціонування, впровадження бізнес-процесів, їх оптимізації, зростання ефективності, використання ресурсів підприємства невід’ємно пов’язані з використанням ERP, CRM та BI бізнес-технологій із встановленням, впровадженням, застосуванням відповідного програмного забезпечення. При цьому активність застосування цих технологій між підприємствами різних сфер та напрямів економічної діяльності має значні відмінності.

Досліджуючи частку підприємств, які використовують ERP-технології зазначимо, що активність їх використання протягом 2022-2024 рр. загалом значно зросла з показника 5,9% у 2022 р. до 15,2% у 2024 р. При цьому, за різними напрямками ця активність має значні відмінності.

Найвищий відсоток активності у впровадженні ERP- технологій мають підприємства, які працюють в сфері інформаційно-комунікаційних технологій. Частка цих підприємств у 2024 р. становила 26,5% підприємств цієї сфери економічної діяльності. Не менш активними у застосуванні ERP-технологій є фармацевтичні підприємства, частка яких станом на 2024 р. склала 27,8%. Значну активність у використанні ERP-систем мають підприємства нафтохімічної промисловості 25,2% від загальної кількості підприємств цієї сфери; підприємства, що працюють в сфері виробництва комп’ютерів електронної та оптичної продукції, частка яких станом на 2024 р. становила 26,2% від загальної чисельності підприємств, що працюють в цих сферах економічної діяльності.

Водночас, досить низьким рівень використання ERP-технологій залишається серед підприємств легкої промисловості (12,4%), деревообробної промисловості та поліграфії (10,5%), на будівництві (10,3%) та серед підприємств металургійного комплексу (11,9%).

Таблиця. 2.5.

Частка підприємств, що використовують програмне забезпечення ERP, CRM та BI для бізнесу, у загальній кількості підприємств за видами економічної діяльності у 2022-2024 р.

Види економічної діяльності	Частка підприємств, що використовують програмне забезпечення ERP, у загальній кількості підприємств, цього виду %		Частка підприємств, що використовують програмне забезпечення CRM, у загальній кількості підприємств, цього виду %		Частка підприємств, що використовують програмне забезпечення BI, у загальній кількості підприємств, цього виду %
	2022	2024	2022	2024	2024
Усього	5,9	15,2	3,0	7,4	3,9
Харчова промисловість	7,1	18,8	2,8	4,5	5,5
Легка промисловість	5,6	12,4	3,1	6,3	1,8
Виготовлення виробів з деревини, паперу та поліграфічна діяльність	6,2	10,5	2,0	5,2	2,1
Нафтохімічна промисловість	5,9	25,2	2,9	—	3,2
Хімічна промисловість	8,5	17,1	3,5	6,4	2,2
Фармацевтика	14,0	27,8	3,6	19,6	12,0
Металургійний комплекс	7,1	11,9	1,8	5,7	0,4
Виробництво комп'ютерів, електронної та оптичної продукції	5,9	26,2	2,8	12,0	1,0
Виробництво електричного устаткування	10,2	19,7	4,4	2,5	5,3
Виробництво машин, устаткування	8,4	20,4	2,7	7,3	2,4
Постачання електроенергії, газу	4,7	18,8	1,4	7,6	5,2
Будівництво	4,3	10,3	1,4	3,1	1,1
Оптова торгівля	6,4	16,6	4,3	12,7	5,9
Роздрібна торгівля	5,7	19,6	3,4	9,5	6,5
Транспорт, складське гос-во	6,2	14,6	2,4	5,4	3,2
Тимчасове розміщування, харчування	5,8	9,3	3,2	4,6	1,9
Інформація та телекомунікації	9,5	22,8	6,9	16,4	8,3
Операції з нерухомим майном	4,5	12,7	1,4	2,9	2,6
Професійна, наукова та технічна діяльність	5,9	13,9	4,5	8,7	5,4
Консалтингова діяльність	6,8	14,6	5,0	6,9	4,2
Наукові дослідження та розробки	7,7	12,8	6,7	4,5	4,5
Діяльність туристичних агентств	12,3	12,8	9,0	16,8	6,4
ІКТ	13,8	26,5	11,7	17,5	8,5

Джерело: сформовано на основі даних [235]

Враховуючи те, що впровадження ERP-систем має значні перспективи для діяльності підприємств-товаровиробників, оскільки дає можливість автоматизувати бізнес-процеси в різних сферах діяльності і має широке застосування в управлінні виробництвом, операційною діяльністю, фінансовими потоками, постачанні чи в формуванні взаємодії з покупцями та клієнтами такий низький рівень впровадження цих технологій серед підприємств різних сфер та напрямів діяльності свідчить про технічну та технологічну неготовність до їх впровадження та нерозуміння керівниками всіх можливостей та переваг, які надають підприємствам впровадження ERP-систем в їх діяльності.

Іншою важливою технологією, впровадження якої має значні перспективи є CRM-системи. Ці системи являють собою програмне забезпечення, призначене для управління процесами взаємодії із контрагентами: споживачами, замовниками, постачальниками послуг.

За сучасних умов CRM-технології здатні значно пришвидшити та оптимізувати ці процеси, забезпечити їх прозорість та суттєво вплинути на зменшення витрат, пов'язаних із процесами обслуговування. Проте, як свідчать дані, приведені в таблиці 2.5. застосування цих технологій вітчизняними підприємствами всіх напрямів та сфер діяльності не має значної активності та поширення. Таким чином, на 2022 р. загалом лише 3% підприємств впровадили ці технології в своїй діяльності, в період 2023-2024 рр. цей відсоток значно зріс до 7,4%, проте загалом показник впровадження CRM-системи в діяльності підприємств залишається критично низьким. При цьому, дослідивши впровадження технологій серед підприємств різних напрямів та видів економічної діяльності, виявили певну неоднорідність. Так, найвищим є рівень впровадження CRM-систем серед підприємств фармацевтичної галузі – 19,6%. При цьому, як свідчать наведені дані, впровадження цих технологій підприємствами фармацевтичної галузі відбулося в період 2023-2024 рр., оскільки ще у 2022 р. відсоток впровадження фармацевтичними підприємствами цих технологій становив 3,6%. Також,

високим є рівень впровадження CRM-технологій серед підприємств в сфері інформаційно-комунікаційних технологій – 17,5% від загальної кількості підприємств. В сфері інформаційно-комунікаційних технологій частка підприємств, що впроваджували CRM-системи у 2024 р., становила 16,4% від загальної кількості підприємств.

Серед підприємств туристичної сфери впровадження CRM-системи становить 16,8% від загальної кількості підприємств; серед підприємств оптової торгівлі та підприємств з виробництва комп'ютерів та електронної продукції цей показник становить по 12% -12,7% відповідно.

Відповідно до наведених в таблиці 2.5. даних, широке використання вітчизняними підприємствами програмного забезпечення ВІ-технологій розпочиналося у 2024 р. Технологія ВІ являє собою комплекс програмного забезпечення, яке дає можливість проводити бізнес-аналітику (ВІ) і дає можливості до формування звітів з інформаційних панелей та забезпечення інтерактивної візуалізації даних. Це програмне забезпечення є важливим інструментом цифрових технологій, здатним забезпечити ефективну управлінську діяльність в різних сферах та видах економічної діяльності. Незважаючи на всі значні переваги та можливості цього програмного забезпечення та враховуючи його новизну в роботі на ринку станом на 2024 р., загалом лише 4,9% від всієї кількості підприємств за всіма видами економічної діяльності впровадили цю технологію в своїй роботі. При цьому, слід зазначити, що лідерами впровадження цих технологій, як і інших цифрових технологій які вже аналізувалися, є підприємства фармакологічної галузі, 12% з яких впровадили ВІ в своїй роботі. Частка впровадження ВІ в діяльності підприємством інформаційно-комунікаційних технологій становить 8,5%.

Одним із найбільш поширених процесів, які широко застосовуються вітчизняними підприємствами всіх видів економічної діяльності та водночас зазнали значних змін, пов'язаних із впровадженням та застосуванням нових цифрових технологій, мереж Інтернет, є технології електронного обміну даними з партнерами, контрагентами, в тому числі з постачальниками,

покупцями, посередниками, державними, фіскальними та регуляторними органами.

Частка підприємств за видами економічної діяльності, що здійснюють електронний обмін інформацією в ланцюгах постачання з партнерами, постачальниками чи покупцями в 2024 р. представлена на рис. 2.3.



Рис. 2.3. Частка підприємств за видами економічної діяльності, що здійснюють електронний обмін інформацією в ланцюгах постачання з партнерами, постачальниками чи покупцями, 2024 р.

Джерело: сформовано на основі даних [235]

Такими цифровими інструментами обміну даними загалом є електронна пошта, месенджери та спеціалізоване програмне забезпечення, яке може використовуватися між партнерами, які співпрацюють, в тому числі на постійних засадах, здійснюючи взаємодію в ланцюгах постачання. Використання нових сучасних цифрових технологій для роботи з

документацією та обмін документацією (рахунками, накладними, заявками, договорами з контрагентами, звітною документацією чи іншими документами) значно пришвидшити процеси управлінської, маркетингової діяльності, ведення обліку та звітності. Аналізуючи дані наведені на рис. 2.3 обмін електронними даними з постачальними чи клієнтами в ланцюгу постачання станом на 2024 р. здійснює незначна кількість - 17,6% від загальної кількості підприємств за всіма видами та сферами економічної діяльності. Слід зазначити, що наявність загалом низького відсотку пов'язана передусім із загальною частотою участі підприємств в ланцюгах постачання. Деталізуючи дані за окремими видами економічної діяльності слід зазначити, що значно вищу ніж зазначена середню активність проявляють підприємства харчової промисловості, оскільки 28,2% впровадили електронний обмін даними з партнерами в ланцюгах постачання.

Значною, в 25%, є частка підприємств хімічної промисловості, де ланцюги постачання також мають досить високий рівень поширення. Аналогічно, 25,1% становить частка підприємств, які впроваджують електронний обмін з партнерами в сфері постачання електроенергії, газу та інших енергетичних ресурсів. Високою, у 28,1%, є частка підприємств, які застосовують електронний обмін інформацією з контрагентами серед підприємств роздрібної торгівлі, що пов'язано із широким застосуванням Інтернет-торгівлі та використанням цифрових електронних платформ для здійснення постачання чи реалізації продукції. Досить високою, в 26,4%, є частка використання технологій обміну інформацією з партнерами в ланцюгах постачання підприємств туристичної сфери, а також 23,5% становить частка таких підприємств в сфері інформаційно-комунікаційних технологій.

Частку в 20,5% має використання цифрових технологій для роботи в ланцюгах постачання серед підприємств фармацевтичної галузі. Найменш поширеним застосуванням цифрового обміну інформацією в ланцюгах постачання є в сфері наукових досліджень та розробок, всього 6,6% та в сфері будівництва – 10,2%.

Іншим важливим показником який визначає впровадження нових цифрових технологій на підприємствах є впровадження аналізу «Великих даних» з різною метою та з виконанням різних завдань операційної, виробничої чи комерційної діяльності (рис. 2.4.).



Рис. 2.4. Частка підприємств, які здійснюють аналіз "великих даних", у загальній кількості підприємств у 2024 р.

Джерело: сформовано на основі даних [235]

Так, 6,6% підприємств здійснюють аналіз «Великих даних» з метою аналітики інформації про здійснення транзакцій, платежів, даних реалізації. Збір та аналіз інформації про клієнтів, їх попит, уподобання, запити, сегментування за географічними та іншими ознаками, рівнем доходу та використання цього аналізу в своїй маркетинговій діяльності здійснюють 6,8% підприємств. Проведення аналізу та використання інформації із соціальних медіа та інтернет ресурсів підприємств проводять в роботі 6,3% підприємств. Значно вищим є рівень використання підприємствами інформації з великих баз даних державних органів, реєстрів, адже таку інформацію аналізують та використовують 8,3% від загальної кількості підприємств. Значно рідше підприємства використовують в своїй діяльності дані з пристроїв та датчиків,

відповідно частка підприємств, що застосовують таку інформацію становить лише 2,8% від загальної чисельності підприємств, ще меншою – 2,3% є частка підприємств, які у своїй діяльності використовують аналітику супутникових даних. Слід зазначити, що загалом станом на 2024 р. аналіз та використання «великих даних» впровадили у своїй роботі 15,2% підприємств всіх сфер та напрямів економічної діяльності.

Сучасні цифровізація та інформатизація процесів функціонування підприємств, операційної діяльності, обміну інформацією невід’ємно пов’язана із використанням хмарних технологій (табл. 2.6, рис. 2.5).

Таблиця 2.6.

Частка кількості підприємств, що купують послуги «хмарних обчислень», у загальній кількості підприємств за видами послуг хмарних обчислень у 2018-2024 рр.

Види послуг «хмарних обчислень»	2018	2019	2021	2022	2024
частка підприємств, що купують послуги хмарних обчислень, загалом, %	9,8	10,3	10,2	9,8	13,7
електронна пошта	5,2	5,9	6,6	6,1	9,8
офісне програмне забезпечення	4,3	4,8	4,6	4,7	7,5
хостинг/бази даних підприємства	3,4	4,0	4,2	4,0	6,3
зберігання файлів	3,6	4,2	5,3	4,6	7,9
прикладне програмне забезпечення бухгалтерського обліку, фінансів	5,3	5,9	5,5	5,1	7,4
програмне забезпечення CRM	2,5	2,9	2,8	1,8	2,7
програмне забезпечення ERP	...	...	...	0,8	1,6
обчислювальна потужність для запуску ПЗ	3,1	3,5	3,5	1,5	3,7
програмне забезпечення для безпеки (антивірусна програма, контроль доступу до мережі, тощо)	...	...	...	4,0	6,1
обчислювальна платформа для розробки, тестування або розгортання додатків	...	...	...	1,1	2,2

Джерело: сформовано на основі даних [235]

При цьому частка підприємств, які купують та використовують в своїй діяльності послуги «хмарних обчислень» з 2018 р. по 2024 р. зазнала суттєвого зростання, з частки 9,8% у 2018 р. до 13,7% у 2024 р. Сама структура послуг, що входить до послуг «хмарних обчислень» є різною і відповідно має різну частку впровадження.

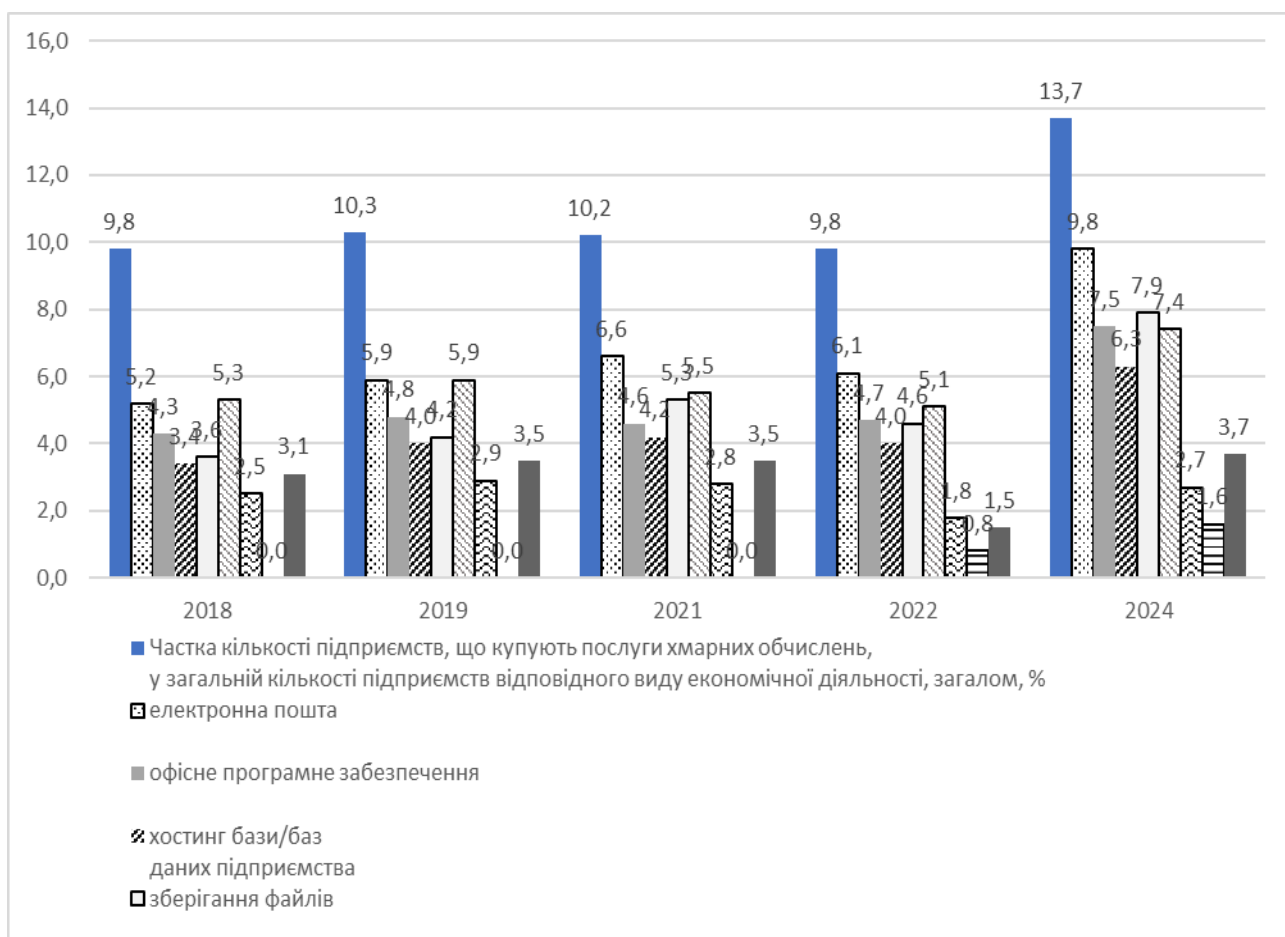


Рис. 2.5. Динаміка впровадження технологій «хмарних обчислень», у загальній кількості підприємств за видами послуг «хмарних обчислень» у 2018-2024 рр.

Джерело: сформовано на основі даних [235]

Так, станом на 2024 р. 5,2% купують послуги «хмарних обчислень» з метою розміщення електронної пошти, 7,5% підприємств використовують ці цифрові технології з метою розміщення офісного програмного забезпечення, ще 6,35% розміщують на них хостінги та бази даних підприємств; 7,9% підприємств використовують послуги «хмарних технологій» для зберігання файлів; 7,4% підприємств використовують «хмарні технології» для розміщення спеціалізованого програмного забезпечення підприємства, в тому числі програм бухгалтерського, фінансового обліку; 2,7% підприємств використовують технології «хмарних обчислень» для програмного забезпечення CRM-систем, та 1,6% підприємств розміщують у «хмарах»

інформацію своєї ERP-системи. Незначна кількість підприємств, 3,7% від загальної чисельності, використовують хмарні технології для запуску програмного забезпечення підприємства. Застосування технологій «хмарних обчислень» в забезпеченні кібербезпеки підприємств також наразі має незначну частоту застосування.

Лише 6,1% підприємств використовують «хмарні технології» для розміщення антивірусних програм та контролю доступу до мережі з метою захисту інформаційних ресурсів підприємства від цифрових загроз та несанкціонованих впливів. Іще 2,2% підприємств станом на 2024 р. використовують «хмарні технології» як обчислювальні платформи для розроблення, тестування та розміщення додатків. Загалом, слід зазначити, що частка підприємств які впроваджували «хмарні технології» в своїй діяльності є незначною та не відповідає реальним потребам підприємств, що свідчить про низький рівень цифровізації процесів управління та функціонування підприємств загалом.

Іншим важливим показником впровадження сучасних цифрових технологій в діяльності підприємств є використання цифрових електронних платформ для здійснення просування та реалізації продукції підприємств (табл. 2.7).

Так загалом станом на 2018 р. обсяги електронної торгівлі за всіма видами та напрямками економічної діяльності здійснювало 3,5% від всієї кількості підприємств. В період з 2018 р. по 2024 р. частка підприємств, що використовують цифрові електронні платформи як на внутрішньому ринку так і для виходу на міжнародні економічні ринки зросла до 5,7% від загальної кількості підприємств. Проте, за окремими сферами економічної діяльності впровадження цих технологій є значно вищим. Так у сфері транспорту, готельного бізнесу та послуг поштових діяльності обсяг послуг реалізований засобами електронної торгівлі в загальному обсязі реалізації становить 19,1%; у туристичній діяльності 31,7% це третина від загального обсягу фінансових надходжень. У сфері інформаційно-комунікаційних технологій частка

надходжень від реалізації послуг засобами електронної комерції становить 10,3% від загального обсягу реалізації.

Таблиця. 2.7.

Обсяг реалізованої продукції (товарів, послуг) підприємств, отриманий від електронної торгівлі

Види економічної діяльності	у % до загального обсягу реалізованої продукції (товарів, послуг) підприємств відповідного виду економічної діяльності					
	2018	2019	2020	2021	2022	2023
Усього	3,5	4,5	5,0	5,3	5,9	5,7
Переробна промисловість	2,7	3,1	3,1	3,2	5,9	4,8
Харчова промисловість	5,2	5,7	5,2	5,3	10,1	8,8
Легка промисловість	3,4	3,1	3,3	3,3	8,1	4,2
Деревообробна промисловість та поліграфічна діяльність	2,4	2,8	3,5	3,4	4,1	3,4
Хімічна промисловість	2,3	2,1	2,2	2,3	к/с	1,5
Виробництво комп'ютерів, електронної та оптичної продукції	2,5	3,0	3,3	3,4	3,3	1,9
Виробництво електричного устаткування	0,8	1,6	1,8	1,9	1,9	1,6
Виробництво меблів, іншої продукції	1,2	1,1	1,0	1,1	1,4	2,0
Будівництво	0,6	0,7	0,7	0,6	0,4	0,2
Оптова торгівля	5,0	3,3	4,7	4,9	8,3	8,2
Роздрібна торгівля	3,5	3,9	3,4	3,7	3,5	5,2
Транспорт, складське господарство, поштова та кур'єрська діяльність	7,1	25,7	31,1	30,9	23,6	19,1
Тимчасове розміщування і харчування	6,8	8,2	11,6	12,0	13,2	7,6
Комп'ютерне програмування, консультування	4,1	5,1	5,0	5,2	5,3	5,8
Операції з нерухомим майном	1,7	0,2	0,7	0,9	1,2	1,2
Наукові дослідження та розробки	2,1	4,2	3,9	4,0	3,1	1,6
Діяльність у сфері адміністративного та допоміжного обслуговування	7,6	3,7	4,1	4,5	2,8	3,4
Туристична діяльність	39,8	11,8	33,2	34,1	35,9	31,7
Інформаційно-комунікаційні технології	7,7	10,5	9,3	10,2	8,6	10,3

Джерело: сформовано на основі даних [235]

Незважаючи на поширення продажу продукції через електронні платформи та інтернет-магазини частка реалізації продукції електронними засобами в оптовій торгівлі станом на 2023 р. становила лише 8,2% від загального обсягу реалізації, а частка надходжень від електронних продажів у роздрібній торгівлі є ще меншою – 5,2% від загального обсягу реалізації

продукції. На нашу думку це свідчить про поступовість розвитку електронних ринків які на даний час лише розширюють сферу діяльності і є перспективним напрямками реалізації продукції у майбутньому. Водночас, мають значення засоби електронної торгівлі за якими буде здійснюватися реалізації продукції. Такими засобами виступають власні веб-сайти, веб-додатки підприємства, використання цифрових електронних платформ для просування та реалізації продукції, послуг та реалізації продукції послуг з використанням повідомлень типу EDI, що передбачає обмін стандартизованими електронними повідомленнями між підприємствами та дає можливість автоматизувати бізнес-процеси.

Одним із прогресивних інноваційних цифрових технологій є штучний інтелект (ШІ). Як свідчать дані представлені на рис. застосування технологій «штучного інтелекту» може мати форми та призначатися для вирішення різних завдань діяльності (рис. 2.6).

Досліджуючи застосування технологій штучного інтелекту в період 2022 р. та 2024 р. за видами технологій слід зазначити, що частка підприємств які загалом використовують ШІ у своїй роботі у 2022 р. становила 5,4% від загальної кількості підприємств. До 2024 р. ця частка дещо зменшилася до 5,2% а загалом технологія залишається мало поширеною. Серед технологій ШІ які найчастіше використовують підприємства частку у 3% має технологія проведення аналізу писемної мови, іще 2,1% підприємств використовують ШІ для автоматизації робочих процесів та як технологічний засіб у прийнятті рішень.

Впровадження технологій штучного інтелекту на підприємствах з різних сферах напрямках економічної діяльності у 2024 р. здійснювалося з метою: маркетингу та реалізації продукції послуг – 2,9% від загальної кількості підприємств; оптимізації процесів виробництва – 1,7%; впровадження процесів адміністрування – 2%; удосконалення процесів логістичної діяльності – 1,1%; ведення бухгалтерського обліку, звітності, контролю –

1,7%; та з метою проведення досліджень – 0,7% від загальної кількості підприємств.

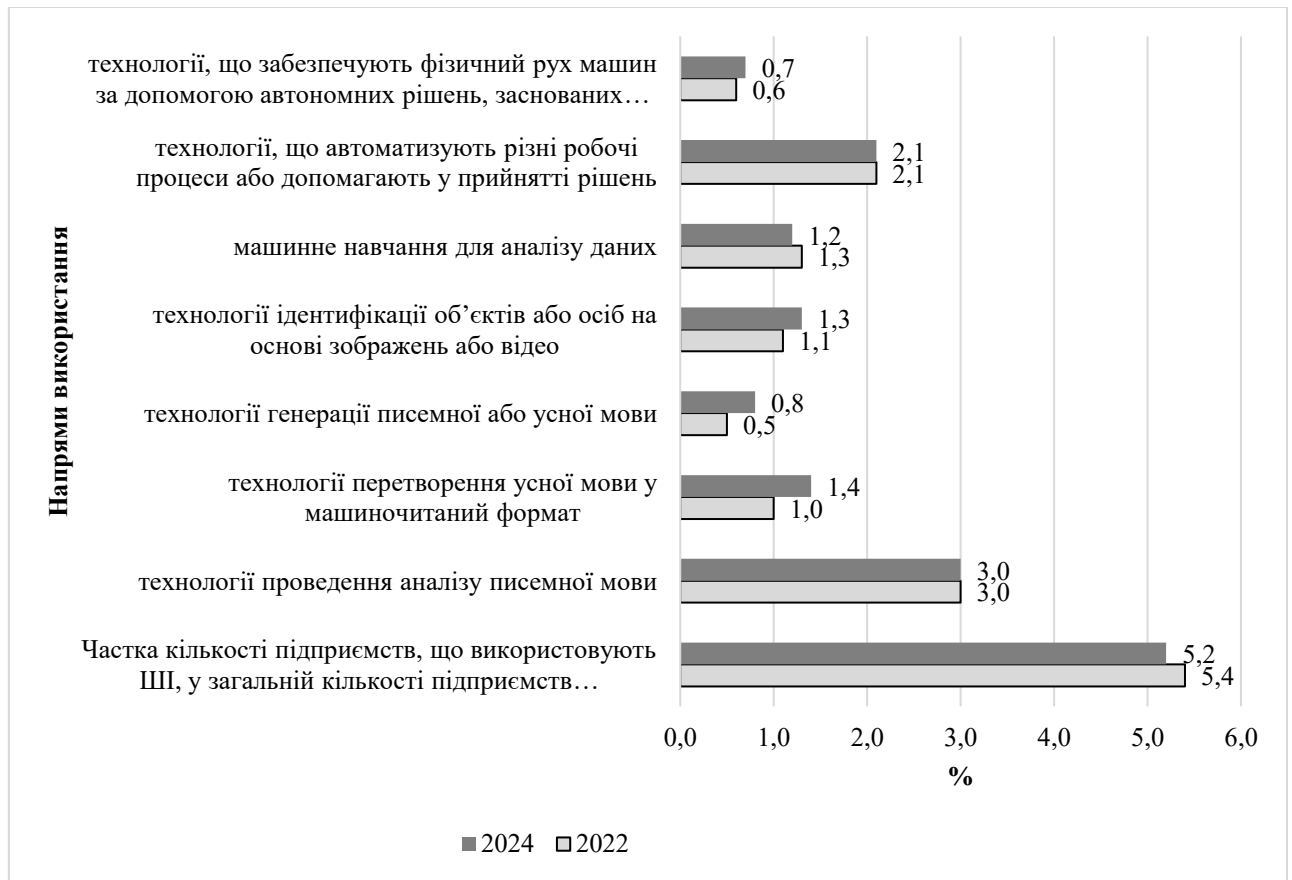


Рис. 2.6. Види та частки використання технологій штучного інтелекту в діяльності підприємств у 2022 та 2024 рр.

Джерело: сформовано на основі даних [235]

Таким чином, «штучний інтелект» стає універсальною технологією широкого застосування яка здатна вирішувати різні задачі у роботі підприємства для оптимізації зменшення витрат та забезпечення оптимізації процесів у різних сферах діяльності підприємства.

Результати проведеного аналізу дають можливість сформулювати проєкцію використання інноваційних цифрових технологій в діяльності підприємств, що складається з трьох головних складових.

Проєкція впровадження сучасних цифрових технологій в діяльності підприємства представлена на рис. 2.7.

Узагальнення результатів проведеного аналізу дає можливість зробити висновок про те, що цифровізація використання інформаційних цифрових технологій в діяльності підприємств проходить декілька головних етапів – складових її впровадження.



Рис. 2.7. Проекція впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства

Джерело: сформовано автором

Основою та початковим етапом такої цифровізації є початок використання підприємством технологій загального використання, підключення підприємства до мережі Інтернет та використання Інтернет технології в операційній, управлінській, фінансовій діяльності підприємства,

комп'ютеризації та підключення до мереж Інтернету робочих місць працівників, розробки підприємством та оприлюднення власного веб-сайту; початку використання соціальних медіа, відкриття сторінок підприємств в соціальних мережах, впровадження на підприємстві цифрового обміну інформацією, документацією, даними з клієнтами, постачальниками та іншими контрагентами; впровадження системи «клієнт-банк» та використання цифрових технологій для проведення фінансових операцій підприємства. Таким чином, проходження першого етапу цифровізації формує основу для подальшого впровадження більш складних спеціалізованих цифрових технологій для удосконалення оптимізації документообігу, просування та реалізації продукції, послуг, оптимізації управління ресурсами. На другому етапі процесів цифровізації в діяльності підприємства переходять на використання цифрових технологій професійного спрямування: впровадження ERP-технологій, CRM-технологій, BI-технологій, застосування «хмарних обчислень» та спеціалізованого програмного забезпечення, використання «великих даних» для аналізу, роботи з інформацією, застосовують технології «хмарних обчислень» та «штучного інтелекту» та використовують мобільні додатки для роботи з клієнтами, споживачами. Впровадження цифрових технологій загального спрямування та спеціалізованого призначення дає можливість забезпечити відповідність технологій, які використовує підприємство тим новим цифровим вимогам та реаліям, які висуває зовнішнє ринкове середовище, відповідності загальному рівню цифровізації та забезпечує можливості для конкуренції та взаємодії з контрагентами на належному техніко-технологічному рівні. Відповідно, це створює умови для використання нових цифрових технологій в забезпеченні економічної безпеки підприємств, в тому числі в можливості протидії кіберзлочинності з використанням спеціалізованого програмного забезпечення та інших технічних засобів, призначених для забезпечення безпеки інформаційних ресурсів підприємства. Все це дає підстави говорити про формування проєкції впровадження інноваційних цифрових технологій в діяльності підприємств,

яка складається з трьох етапів проектування: перший етап із впровадженням на підприємстві цифрових технологій загального використання, що загалом формує загальний базис, цифрову технічну базу для подальшої цифровізації та забезпечує загальні можливості для роботи з інформацією, обміну інформацією з контрагентами та дає можливості підприємствам загалом взаємодіяти та функціонувати в сучасних ринкових умовах; другий етап – із впровадженням специфічних, професійних та більш складних цифрових технологій, впровадження яких забезпечує оптимізацію використання ресурсів підприємства, оптимізує бізнес-процеси діяльності та забезпечує можливості для отримання значно кращих результатів роботи та забезпечує зростання конкурентоспроможності; на третьому етапі проєкції відбувається безпосереднє впровадження та використання цифрових технологій для забезпечення безпеки інформаційних ресурсів, протидії кібератакам та кіберзлочинності. Як наслідок, впровадження цифрових технологій першого та другого етапів забезпечує цифрові можливості для стабільного функціонування підприємства, зростання його фінансової стійкості, рівня конкурентоспроможності та можливості для подальшого зростання, що разом створює основу для стабільності та забезпечення належного рівня економічної безпеки підприємства. Таким чином, зазначена проєкція цифрових інструментів та їх впровадження забезпечує та виступає основою використання цифрових технологій в управлінні системою економічної безпеки підприємств.

2.2. Показники впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства

Одним із важливих напрямів застосування інноваційних цифрових технологій на підприємстві є економічна безпека. Використання нових цифрових технологій, програмного забезпечення інноваційних технічних

засобів та приладів в діяльності служб економічної безпеки та з метою забезпечення безпеки здійснюється відповідно до стратегії, планів впровадження превентивних заходів в забезпеченні безпеки та у відповідь на негативні впливи, загрози та небезпеки зовнішнього і внутрішнього середовищ, що виникають в діяльності. Важливе значення в плануванні та реалізації безпекових заходів має забезпечення інформаційно-цифрової безпеки, оскільки саме ця безпека забезпечує внутрішні цифрові трансформації на підприємстві, забезпечує засоби протидії новим цифровим викликам зовнішнього середовища та забезпечує можливості для підприємства працювати в єдиному цифровому полі.

Впровадження цифрових технологій та розбудова сучасних і належних з позицій безпеки інформаційних цифрових комунікацій передусім потребує розробки та прийняття в системі економічної безпеки підприємства документів, які регламентують, визначають та регулюють безпекові питання використання інформаційно-комунікаційних технологій.

Такими документами виступають положення, накази та інструкції, які визначають та регламентують безпеку використання ІКТ на підприємствах як загалом, так і за конкретними напрямками.

Одним із таких аспектів використання, який потребує регламентування є розробка та прийняття на підприємстві документів, що регламентують питання безпеки ІКТ під час роботи працівників на віддаленому доступі. На рисунку 2.8 представлено статистичні дані щодо того, яка частка підприємств має документи, які регламентують безпеку віддаленого доступу при роботі з інформаційно-комунікаційними технологіями.

Представлені статистичні дані свідчать, що загалом кількість підприємств що розробила та затвердила відповідну безпекову документацію є незначною, оскільки загалом серед підприємств всіх сфер та напрямів економічної діяльності відповідну документацію, яка регламентує безпеку роботи на віддаленому доступі має лише 23,7% від всієї кількості підприємств. Найбільш активно в цьому питанні працюють підприємства, які здійснюють

комп'ютерне програмування та консультування, оскільки відповідну документацію мають 51,5% підприємств. Частка підприємств, які мають відповідну регламентуючу документацію та затверджені норми та регламенти становить 45% серед підприємств інформації та телекомунікацій; 42,8% серед підприємств телекомунікацій та електрозв'язку; 44,6% підприємств туристичної сфери; у 44,4% є частка серед підприємств, які здійснюють ремонт комп'ютерів та засобів електрозв'язку. Слід зазначити, що окрім туристичної сфери максимально інформаційно інтегрованої в зовнішнє економічне середовище всі ці підприємства працюють в сфері інформаційних технологій та є високотехнологічними. Серед підприємств сфери виробництва ці показники є значно нижчими.

Так, відповідні затверджені безпекові документи та регламенти з питань віддаленого доступу мають 37,1% підприємств нафтохімічної галузі та 38,1% фармацевтичної галузі, 31% підприємств, що здійснюють консалтингову діяльність в різних сферах та напрямках та 32,6% серед підприємств, які здійснюють професійну та науково-технічну діяльність. В сфері оптової торгівлі відповідну регламентуючу безпекову документацію мають 30,9% та 24,6% підприємств в сфері роздрібної торгівлі.

Найнижчий рівень активності у питаннях документального нормування регулювання безпекових аспектів роботи на віддаленому доступі виявлено серед підприємств, що здійснюють виробництво комп'ютерів, електронної та оптичної продукції – 12,1%, серед будівельних компаній – 16,1%; серед підприємств в сфері адміністративного та допоміжного господарства – 15,2%. Така низька активність серед цих підприємств пов'язана із незначними потребами в роботі з віддаленим доступом як таким і відповідно відсутністю необхідності впровадження безпекових норм та регламентів.

Водночас, для підприємств сфери інформаційно-комунікаційних технологій, консалтингу, консультування та серед підприємств з активним використанням цифрової комерції застосування норм та регламентів безпеки віддаленого доступу є принципово необхідним.



Рис. 2.8. Частка підприємств, в яких прийнято документи, що регулюють безпеку роботи на віддаленому доступі співробітників при використанні ІКТ

Джерело: сформовано на основі даних [235]

Наступним важливим безпековим показником є частка підприємств, які розробили та затвердили регламенти забезпечення безпеки інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу із застосуванням Інтернет.

Частка підприємств, які впровадили регламенти, що визначають безпеку інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу із застосуванням Інтернет представлена на рис. 2.9.

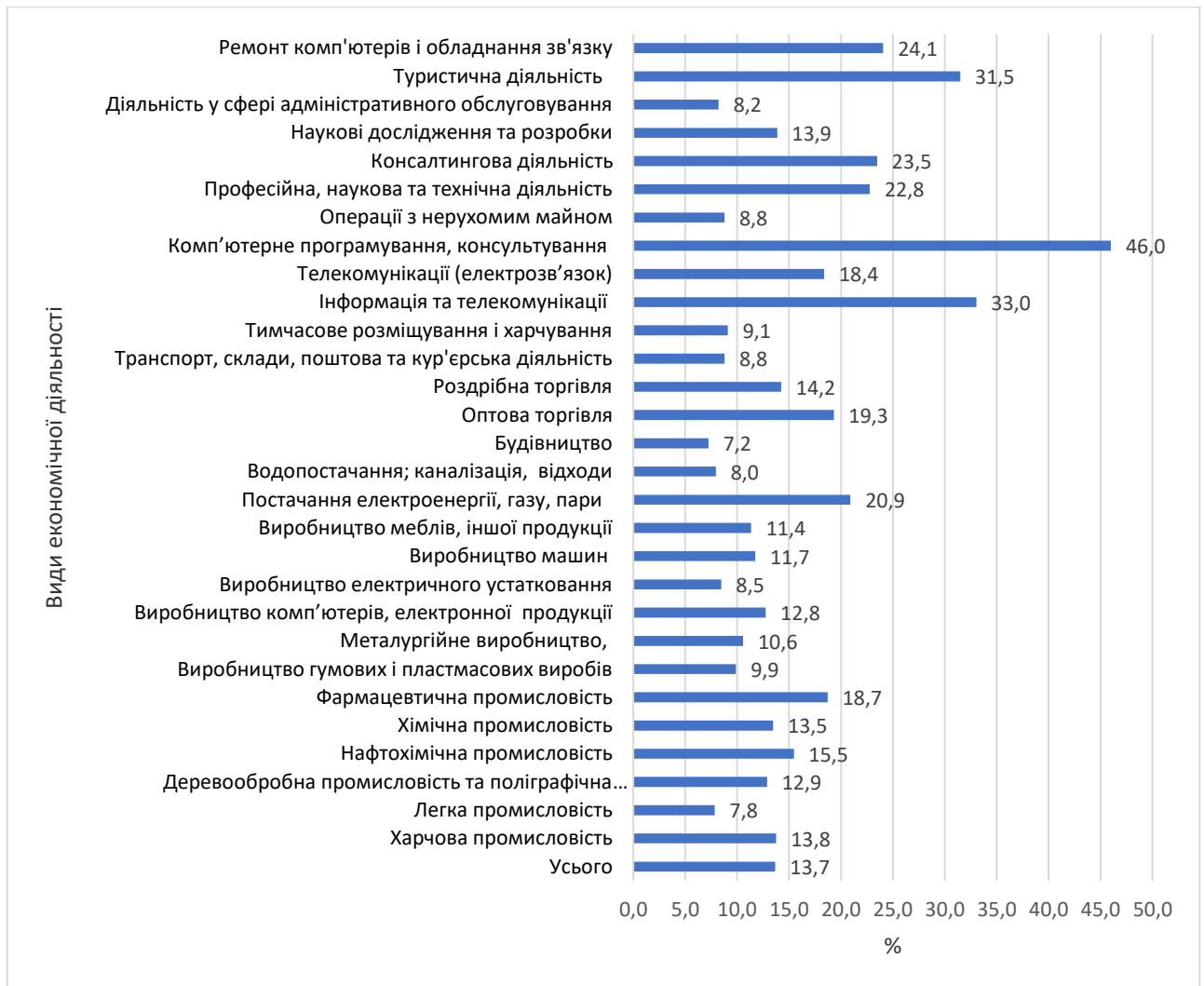


Рис. 2.9. Частка підприємств, які впровадили регламенти, що визначають безпеку інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу із застосуванням Інтернет

Джерело: сформовано на основі даних [235]

Аналізуючи дані державної статистичної служби за період 2023 р. слід зазначити, що частка підприємств які впровадили регламенти, що визначають безпеку інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу із застосуванням мереж Інтернет є досить низькою. Передусім, це пов'язано із самими обсягами проведення відео-конференцій, онлайн-конференцій та інших заходів із використанням онлайн-зв'язку із метою бізнес-діяльності. Переважна більшість невеликих промислових підприємств такої необхідності та доцільності фактично немає. Так, частка

підприємств які впровадили регламенти, що визначають безпеку інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу із застосуванням Інтернет в легкій промисловості становить 7,8%; у харчовій промисловості – 13,8%; у виробництві гумових та пластмасових виробів – 9,9% та у металургійному виробництві 10,6%. Також низька активність щодо впровадження регламентів, які визначають безпеку інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу із застосуванням Інтернет спостерігається у сфері будівництва 7,2% від загальної кількості підприємств цієї сфери; у сферах транспорту, складського господарства, поштової та кур'єрської діяльності – 8,8%; у сфері нерухомості – 8,8%; в діяльності сфери адміністративного обслуговування – 8,2%, та в інших сферах економічної діяльності.

Натомість, потреба в проведенні таких онлайн-заходів та забезпеченні їх належного рівня конфіденційності та безпеки є у підприємств, які працюють в сфері інформаційних та телекомунікаційних технологій, здійснюючи комп'ютерне програмування та консультування, серед яких регламенти, що визначають безпеку інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу із застосуванням Інтернет мають 46% підприємств; в сфері інформації та телекомунікацій – 33%. Слід зазначити, що в туристичній сфері в зв'язку із специфікою повної інтегрованості в зовнішні економічні ринки та необхідності постійної роботи з партнерами, включаючи відео зв'язок та конференції регламенти які визначають безпеку інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу із застосуванням Інтернет мають 31,5% від загальної кількості туристичних компаній.

Наступним показником, який дає можливість досліджувати стан та рівень забезпечення безпеки підприємства є наявність на підприємстві безпосередньо програмного забезпечення, яке забезпечує захист, безпеку віддаленого доступу (рис. 2.10). Цей показник є особливо важливим для підприємств, що активно використовують віддалений доступ для здійснення

своїї операційної діяльності. Передусім це стосується всіх економічних напрямів діяльності сфери високих технологій, інформації та телекомунікацій, адже забезпечення такого захисту необхідне для забезпечення результатів їх безпосередньої операційної діяльності, розробки ПЗ, інших продуктів, розробки та реалізації проектів та їх ефективності.



Рис. 2.10. Наявність ПЗ для захисту безпеки віддаленого доступу

Джерело: сформовано на основі даних [235]

Так, найвищий рівень використання спеціалізованого програмного забезпечення для захисту безпеки віддаленого доступу – 8,5% мають підприємства, які здійснюють ремонт комп'ютерів та засобів зв'язку; 6,9% складова частка підприємств в сфері інформаційно-комунікаційних

технологій загалом та 6,5% підприємств, що працюють в сфері телекомунікацій, електрозв'язку. Програмне забезпечення для захисту віддаленого доступу також використовують 8,4% організацій, які працюють в сфері професійної науково-технічної діяльності, а також 7,7% підприємств, в сфері консалтингу.

Слід зазначити, що досить високим є відсоток застосування спеціалізованого програмного забезпечення для захисту, безпеки віддаленого доступу на підприємствах хімічної промисловості – 7,9% від загальної кількості підприємств цієї галузі, та за напрямком виробництва електричного устаткування та обладнання – 7,7% від загальної кількості підприємств.

Проте, незважаючи на позитивні зміни та поступове впровадження і використання підприємствами програмного забезпечення для захисту, безпеки віддаленого доступу загальна частка підприємства, які його використовують в своїй практичній діяльності на 2023 р. становила лише 4%, що є критично низьким показником, якій свідчить про відсутність належного захисту підприємств при роботі на віддаленому доступі та неспроможності підприємства захищати свої інформаційні ресурси, програми та додатки на належному цифровому техніко-технологічному рівні.

В сучасному світі все більше поширення, як в діяльності підприємства має впровадження та застосування технології штучного інтелекту. Підприємства мають різні напрямки використання в своїй діяльності, аналіз цих напрямів детально представлено в попередньому підрозділі, проте окреме вагоме значення за сучасних умов має застосування штучного інтелекту для вирішення задач забезпечення економічної безпеки підприємства (рис. 2.11).

При цьому, саме впровадження, використання штучного інтелекту для забезпечення безпеки інформаційно-комунікаційних технологій на підприємствах за різними напрямами, сферами діяльності вирішується по різному.

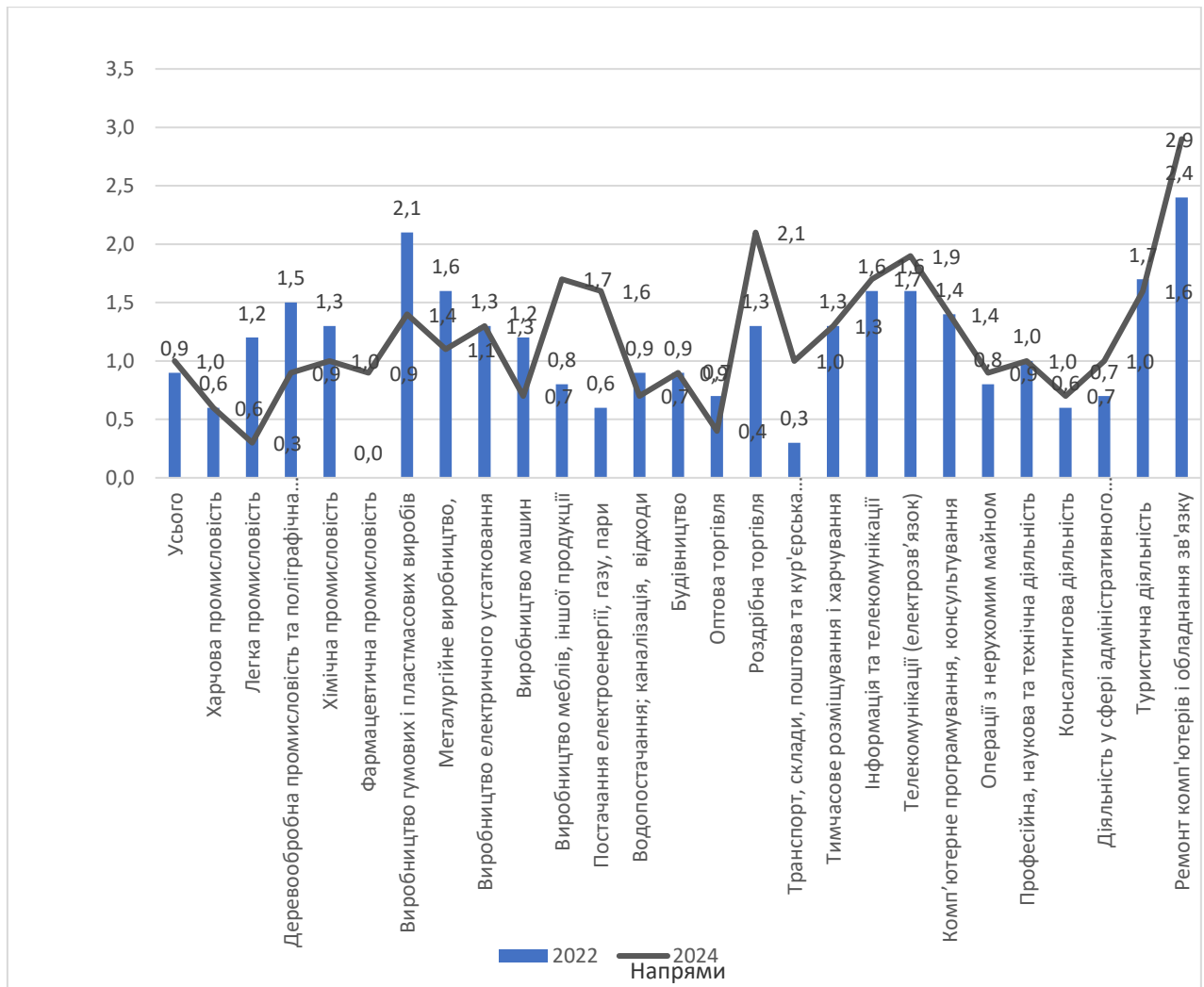


Рис. 2.11. Впровадження, використання штучного інтелекту для забезпечення безпеки ІКТ на підприємствах за напрямками економічної діяльності

Джерело: сформовано на основі даних [235]

Так, досліджуючи впровадження, використання штучного інтелекту для забезпечення безпеки інформаційно-комунікаційних технологій у період 2022-2024 рр. слід зазначити, що загалом його використання підприємствами з метою забезпечення безпеки ІКТ має дуже низький рівень активності. Так, станом на 2022 р. загальна частка підприємств, які використовували штучний інтелект для забезпечення безпеки ІКТ становила лише 0,9%, в наступні роки ця частка дещо зросла та станом на 2024 р. становила 1% від загальної кількості підприємств. Дослідивши окремі галузі види економічної діяльності та динаміку застосування штучного інтелекту для потреб забезпечення

безпеки інформаційно-комунікаційних технологій слід зазначити відмінності. Так, найбільш високою є частка використання ІІІ для забезпечення безпеки ІКТ станом на 2024 р. на підприємствах, що займаються ремонтом комп'ютерів та обладнанням зв'язку – 2,9%; на підприємствах роздрібною торгівлі – 2,1%; в сфері телекомунікацій (електрозв'язку) -1,9%; на підприємствах що працюють в сфері інформації та телекомунікацій – 1,7%; у виробництві меблів та іншої продукції – 1,7%. Проте, є сфери та галузі де за період з 2022 р. по 2024 р. частка використання підприємствами ІІІ для забезпечення безпеки інформаційно-комунікаційних технологій навпаки скоротилася. Так, відбулося скорочення частки підприємств, що використовують ІІІ в безпекових цілях на підприємствах деревообробної та поліграфічної промисловості з 1,5% у 2022 р. до 0,9% у 2024 р.; на підприємствах легкої промисловості з 1,2% у 2022 р. до 0,3% у 2024 р.; в сфері виробництва гумових та пластмасових виробів з 2,1% у 2022 р. до 1,4% в 2024 р.; у металургійному виробництві з 1,6% у 2022 р. до 1,1% у 2024 р. У сфері комп'ютерного програмування та консультування використання штучного інтелекту для забезпечення безпеки інформаційно-комунікаційних технологій протягом 2022-2024 рр. є незмінним, але залишається на низькому рівні – 1,4% від загальної кількості підприємств, що працюють в цій сфері. На наш погляд, зменшення активності та часу використання цих технологій в період 2022-2024 рр. пов'язано із станом війни, в якому перебуває країна, що позначилося загальною на активності та ефективності роботи цілої низки галузей та сфер діяльності, в яких наразі згорнуто нові проекти та активність, в тому числі і в сфері впровадження передових цифрових технологій. Зазначимо, що аналіз стану та рівня економічної безпеки підприємств необхідно проводити детально досліджуючи проблеми підприємств, що виникають через випадки порушення безпеки інформаційно-комунікаційних технологій.

В таблиці 2.8 представлено статистичні дані щодо джерел виникнення безпекових проблем в сфері ІКТ та характеру ознак їх проявів для підприємств за різними видами економічної діяльності у 2023 р.

Таблиця 2.8

Частка підприємств в яких виникали проблеми, пов'язані із безпекою використання ІКТ, у 2023 р.

Види економічної діяльності	Частка підприємств, що мали проблеми через інциденти безпеки ІКТ, у загальній кількості підприємств, %	З них за видами проблем через інциденти безпеки ІКТ		
		недоступність послуг ІКТ через збої апаратного забезпечення чи програм	недоступність послуг ІКТ через кібератаки та відмови в обслуговуванні (DoSattack)	знищення чи пошкодження інформації внаслідок збоїв у роботі апаратного або ПЗ
Усього	24,7	21,8	3,9	5,9
Харчова промисловість	24,0	20,1	4,6	5,7
Легка промисловість	19,4	18,1	2,0	3,0
Деревообробна промисловість	19,2	15,2	2,9	5,7
Нафтохімічна промисловість	46,3	33,9	15,5	15,5
Хімічна промисловість	30,0	27,7	3,8	4,8
Фармацевтика	42,2	40,2	1,0	2,1
Металургійне виробництво	26,4	24,1	4,8	5,3
Виробництво комп'ютерів, електронної продукції	25,6	23,8	5,5	7,2
Виробництво електричного устаткування	19,7	19,0	1,0	3,7
Виробництво машин	23,9	21,5	1,3	3,8
Виробництво меблів	23,7	21,9	3,3	4,0
Постачання електроенергії, газу	29,4	26,7	1,8	6,2
Будівництво	18,4	16,8	3,0	4,1
Оптова торгівля	27,0	24,1	3,5	6,4
Роздрібна торгівля	32,1	27,2	7,6	10,7
Транспорт, склади, поштова та кур'єрська діяльність	23,9	20,9	4,8	5,5
Тимчасове розміщення	26,1	22,6	5,3	7,9
Інформація та телекомунікації	28,3	20,7	11,0	14,1
Телекомунікації	23,1	20,2	10,2	10,9
Комп'ютерне програмування	31,3	21,6	11,3	16,0
Операції з нерухомим майном	22,6	21,9	2,5	3,3
Професійна, наукова діяльність	26,1	21,8	3,2	6,5
Консалтингова діяльність	26,4	22,3	3,1	6,1
Наукові дослідження розробки	30,1	29,7	5,7	5,7
Діяльність в адмініструванні	20,7	18,1	1,8	4,6
Туристична діяльність	40,0	28,9	9,2	11,8
Ремонт комп'ютерів	31,0	26,8	6,2	6,4

Джерело: сформовано на основі даних [235]

Так, загалом станом на 2023 р. у 24,7% підприємств виникали проблеми, пов'язані із безпекою використання ІКТ. Так, найбільш поширені проблеми пов'язані із безпекою використання ІКТ є на підприємствах нафтохімічної промисловості – частка таких підприємств становить 46,3% та на підприємствах фармацевтичного виробництва – 42,2%. Причиною виникнення таких проблем в діяльності цих підприємств є недоступність послуг ІКТ через збої апаратного або програмного забезпечення. Окрім зазначеного фактору підприємства нафтохімічної промисловості мають значні проблеми через недоступність послуг ІКТ, через атаку ззовні (атаки програм-вимагачів, відмови в обслуговуванні (DDoS attack) – 15,5% підприємств та через знищення чи пошкодження інформації внаслідок збоїв у роботі апаратного або ПЗ.

Таким чином, однією із основних причин виникнення проблем пов'язаних із безпекою використання ІКТ на підприємствах є порушення апаратного забезпечення чи програмного забезпечення, внаслідок яких послуги інформаційно-комунікаційних технологій стають недоступними. За статистичними даними загалом з цією проблемою стикаються 21,8% підприємств. Як вже зазначалося, найбільш з цією проблемою в роботі інформаційно-комунікаційних технологій зіштовхуються підприємства нафтохімічної промисловості – 27,7% від загальної кількості підприємств галузі; підприємства фармацевтичної галузі – 40,2%.

Проблеми з недоступністю послуг ІКТ через збої апаратного забезпечення чи програмного забезпечення призводили до деструктивних процесів у діяльності 20,1% підприємств харчової промисловості; 18,1% підприємств легкої промисловості; 27,7% підприємств нафтохімічної промисловості; 24,1% підприємств металургійного комплексу; 23,8% підприємств з виробництва комп'ютерів електронної, оптичної продукції.

Слід зазначити, що ці проблеми пов'язані із використанням інформаційно-комунікаційних технологій торкнулися фактично всіх галузей та сфер економічної діяльності, тому загальний показник – 21,8% підприємств

що мали проблеми пов'язані із недоступністю послуг ІКТ через збої апаратного забезпечення чи програм є фактично усередненим значенням. Таким чином, ця проблема є однією з найбільш поширених, що потребує вирішення в комплексі забезпечення цифрової безпеки підприємств.

Іншою проблемою, що також має значне поширення та частоту проявів та завдає значних фінансових збитків підприємствам активуючі й інші ризики та загрози в їх діяльності є недоступність отримання інформаційно-комунікаційних послуг внаслідок кібератаки чи відмови в здійсненні обслуговування.

Слід зазначити, що загалом кібератаки не є постійним явищем, оскільки загальна частка підприємств, які зазнавали кібератак та мали проблеми у відмові обслуговування становить 3,9% від загальної кількості підприємств. Проте, аналізуючи статистичні дані слід зазначити, що загрози кібератак та проблеми які виникають в діяльності підприємств, спрямовані переважно на конкретні галузі та види економічної діяльності. Станом на 2023 р. такими цифровими «мішенями» проведення кібератак стали галузі нафтохімічної промисловості – де атак та відмов обладнання протягом року зазнали – 15,5%; сфера інформації та телекомунікацій – 11 % підприємств, що зазнали кібератак; у галузі комп'ютерного програмування з цією проблемою стикалися – 11,3% підприємств; а у сфері телекомунікацій та електрозв'язку – 10,2% підприємств.

Іншими загрозами, які дестабілізують роботу підприємств є знищення чи пошкодження інформації внаслідок збоїв у роботі апаратного чи програмного забезпечення. Так, цю проблему мали 5,9% підприємств всіх сфер та напрямів діяльності. Серед галузей діяльності, де зафіксовано інциденти знищення та пошкодження інформації протягом 2023 р. це нафтохімічна промисловість – 15,5%, роздрібна торгівля – 10,7%; у сфері інформації та телекомунікацій – 14,1%, у сфері виробництва програмного забезпечення – 14%, у туристичній сфері – 11,8%. Таким чином, проблеми зі знищення чи пошкодження інформації внаслідок збоїв у роботі апаратного або

ПЗ виникають у сферах діяльності безпосередньо пов'язаних з інформацією чи енергетичним забезпеченням.

Слід зазначити, що традиційно низько-технологічні чи середньо-технологічні галузі значно менш залежні від впливів та дії цифрових ризиків і загроз в своїй діяльності. Можливо це пов'язано із загальним, значно нижчим рівнем впровадження процесів цифровізації в діяльності цих підприємств та меншою залежністю від безпосередньої роботи програмного забезпечення та можливості обміну інформацією, тобто ті підприємства чий бізнес – процеси діяльності, зосереджений у внутрішньому середовищі підприємства на даний час менш вразливі до впливу зовнішніх ризиків та загроз, безпеки ІКТ, ніж ті підприємства чий бізнес-процеси інтегровані в зовнішнє ринкове середовище.

Досліджуючи проблеми, які виникають в діяльності підприємств внаслідок інцидентів порушення безпеки інформаційно-цифрових технологій слід зазначити, що однією із таких причин є знищення чи пошкодження інформації внаслідок зараження вірусним ПЗ чи несанкціонований вхід в інформаційні ресурси підприємства.

Однією із найбільш поширених проблем діяльності підприємств пов'язаних із використанням інформаційно-комунікаційних технологій є вірусні атаки та зараження вірусами програмного забезпечення підприємства з метою знищення, пошкодження інформації чи здійснення несанкціонованих входів в бази даних та до інформації підприємства. Загальна частка підприємств, що зазнавали відповідного вірусного зараження у 2023 р. становила 2,2% від загальної кількості підприємств, проте частота проявів цих загроз для різних видів економічної діяльності є різною. Так, найбільш страждали від вірусного зараження програмного забезпечення підприємства, що працюють в сфері туристичної діяльності, частка таких підприємств становить 5% від загальної кількості підприємств; організації, що працюють в сфері телекомунікацій та електрозв'язку 6% від загальної кількості підприємств; в сфері інформації та телекомунікацій – 4% підприємств.

Іншими причинами, через які підприємства зазнають загроз розкриття конфіденційної інформації є фармінг та фішингові атаки. Так, за статистичними даними, протягом 2023 р. таких атак зазнало 0,6% від загальної кількості підприємств всіх сфер діяльності. Проте, в сферах: туристичної діяльності, телекомунікацій, комп'ютерного програмування та консультування цей показник вищий та становить по 2% від загальної кількості підприємств відповідної сфери економічної діяльності.

Іншими загрозами, з якими стикаються підприємства при використанні інформаційно-комунікаційних цифрових технологій є розкриття конфіденційної інформації через випадкові ненавмисні дії співробітників. Так, загальна частка підприємств, які зазнавали таких загроз становить 0,7% від загальної кількості підприємств. При цьому, за окремими напрямками економічної діяльності цей показник є вищим: в хімічній промисловості – 1,3%, комп'ютерному програмуванні – 2%; сфері інформації та телекомунікацій – 1,3%; в консалтинговій діяльності – 1,5%. Проте, найбільш часто відповідні помилки допускають працівники туристичної сфери, оскільки так частото ненавмисного розголошення конфіденційної інформації працівниками сягає 3,9% від загальної кількості підприємств цієї сфери.

Отже, в цілому випадки порушення безпеки використання інформаційно-комунікаційних технологій внаслідок вірусного зараження програмного забезпечення чи баз даних, розкриття конфіденційної інформації внаслідок фармінгу, фішингових атак чи внаслідок випадкового її розголошення працівниками самих суб'єктів господарювання має низький незначний відсоток проявів, що свідчить про добре налагоджену системну роботу відповідних фахівців інформаційно-комунікаційних технологій, здатних належним чином захистити підприємства та їх інформацію від загроз при роботі у новому цифровому середовищі.

Таблиця 2.9

Частка підприємств, в яких виникали порушення безпеки ІКТ у 2023 р.

Види економічної діяльності	З них за видами проблем через інциденти безпеки ІКТ		
	знищення чи пошкодження інформації внаслідок зараження вірусним ПЗ чи несанкціонований вхід в інформаційні ресурси підприємства	розкриття конфіденційної інформації внаслідок проникнення, фармінг, фішингову атаку	розкриття конфіденційної інформації через випадкові ненавмисні дії співробітників
Усього	2,2	0,6	0,7
Переробна промисловість	2,4	0,8	0,7
Харчова промисловість	3,5	0,9	0,7
Легка промисловість	1,4		0,5
Деревообробна, поліграфічна промисловість	1,2	0,4	0,6
Хімічна промисловість	2,6	1,3	1,3
Фармацевтика	1,0	1,0	
Металургійне виробництво	1,3	0,8	0,3
Виробництво комп'ютерів, електронної продукції	1,2	1,2	
Виробництво машин і устаткування	3,0	0,6	0,6
Виробництво меблів	3,0	1,4	0,7
Будівництво	1,7	0,4	0,7
Оптова торгівля	1,7	0,0	0,3
Роздрібна торгівля	3,4	1,0	1,0
Транспорт, складське господарство, поштова та кур'єрська діяльність	2,7	0,2	0,5
Інформація та телекомунікації	4,0	1,7	1,3
Телекомунікації (електрозв'язок)	6,0	2,0	
Комп'ютерне програмування	3,0	2,0	2,0
Операції з нерухомим майном	1,8	1,4	0,7
Професійна, науково-технічна діяльність	1,2	0,0	1,1
Консалтингова діяльність	1,6		1,5
Наукові дослідження та розробки	0,4	0,4	0,4
Діяльність у сфері адміністрування	1,5	0,1	0,4
Туристична діяльність	5,9	2,0	3,9
Ремонт комп'ютерів і обладнання зв'язку	2,1	0,0	2,1

Джерело: сформовано на основі даних [235]

Як вже зазначалося, однією із провідних сучасних цифрових технологій, які активно почали використовуватися підприємствами є технології «інтернету речей». Широке використання цих технологій передусім спрямоване на роботу з просування та збуту продукції, проте ця технологія успішно застосовується для вирішення задач забезпечення безпеки приміщень (рис. 2.12).

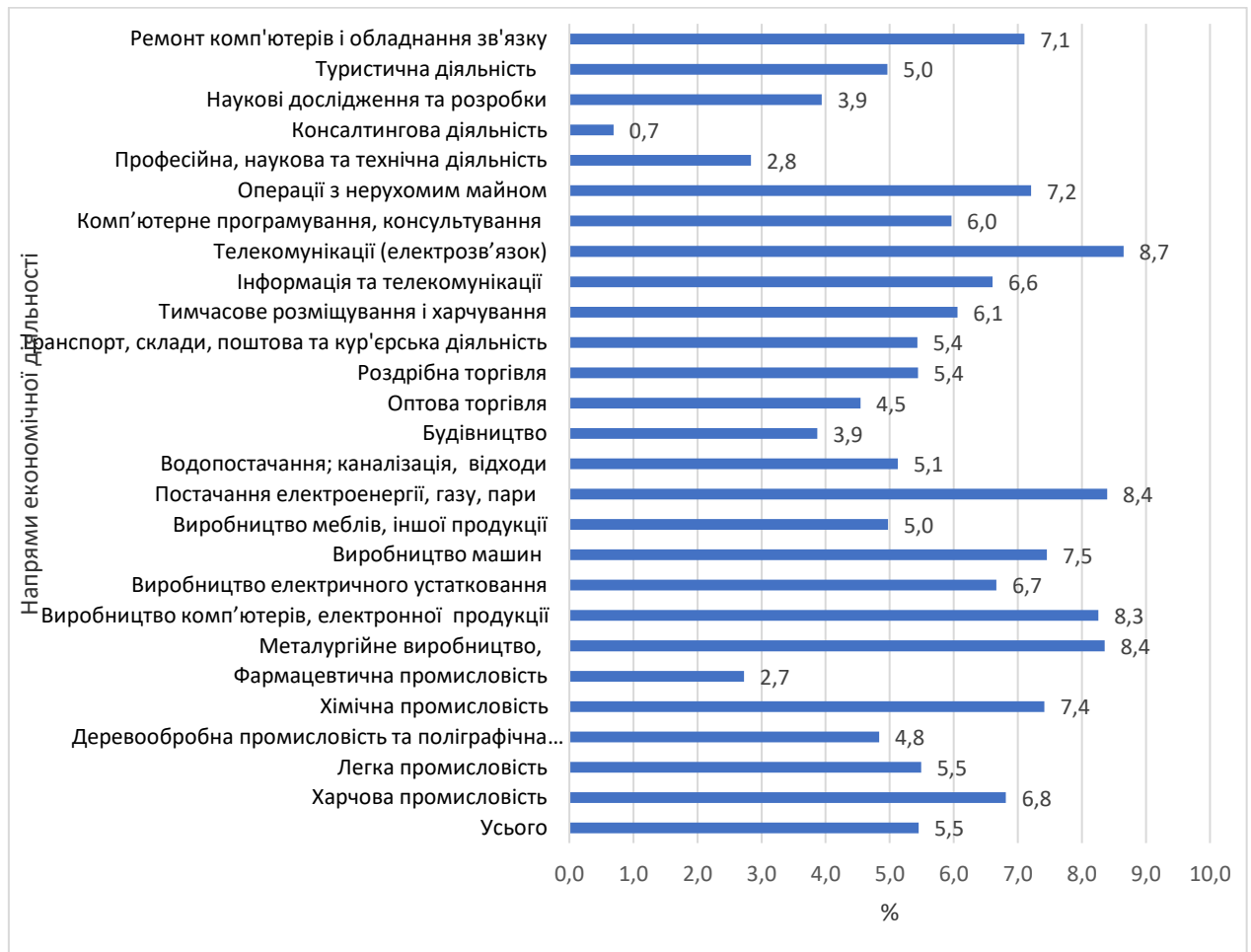


Рис. 2.12. Використання інтернету речей для забезпечення безпеки приміщень

Джерело: сформовано на основі даних [235]

Підприємства різних напрямів економічної діяльності застосовують цю технологію в охороні приміщень з різною інтенсивністю. Так, найбільш активно інтернет речей в забезпеченні безпеки приміщень використовується підприємствами в сфері телекомунікацій – 8,7% від загальної кількості

підприємств усієї сфери; у металургійному виробництві – 8,4% від загальної кількості підприємств; у сфері постачання електроенергії, газу та пари – також 8,4%; в сфері виробництва комп'ютерів та електронної техніки – 8,3%; у хімічній промисловості – 7,4% та у виробництві машин, обладнання – 7,5% від загальної кількості підприємств цієї сфери. Як бачимо, значний відсоток використання цих технологій для забезпечення безпеки приміщень характерний для об'єктів критичної інфраструктури, стратегічних, високотехнологічних підприємств, таких як хімічна промисловість, тощо. В першу чергу, це пов'язано із необхідністю забезпечення високого рівня безпеки, захисту в діяльності цих підприємств. Проте, і в традиційних сферах діяльності, таких як харчова промисловість, частка підприємств, які впровадили «інтернет речей» для забезпечення безпеки приміщень становить 6,8% від загальної кількості підприємств, що свідчить про поступовий рух до більш широкого використання сучасних цифрових технологій не лише в операційній, управлінській, маркетинговій, а й у безпековій діяльності підприємств.

Аналізуючи загальні показники застосування заходів безпеки у функціонуванні інформаційно-комунікаційних систем підприємства зазначимо, що загалом заходи безпеки в роботі інформаційних систем використовують 73,2% підприємств. При цьому, використання різних заходів має різну частоту, представлену на рис. 2.13.

Так, найбільш поширеними заходами безпеки ІКТ системах підприємств є автентифікація користувачів з використанням паролів для входу в систему. Частота використання підприємствами всіх напрямів діяльності цього заходу становить 66,3% від загальної кількості підприємств. Іншим загально поширеним заходом є резервне копіювання інформації в окремі сховища – цей захід проводять 52,7% від загальної кількості підприємств. Іншим поширеним безпековим заходом серед підприємств вважається контроль доступу до мережі, який у 2023 р. впровадили 44,6% підприємств.

Частина організацій намагається забезпечувати безпеку своєї інформаційної системи із впровадженням шифрування даних, документації підприємства – 23% підприємств запровадили цей засіб, іще 21,4% підприємств використовують VPN з метою забезпечення інформації в ІКТ системах.

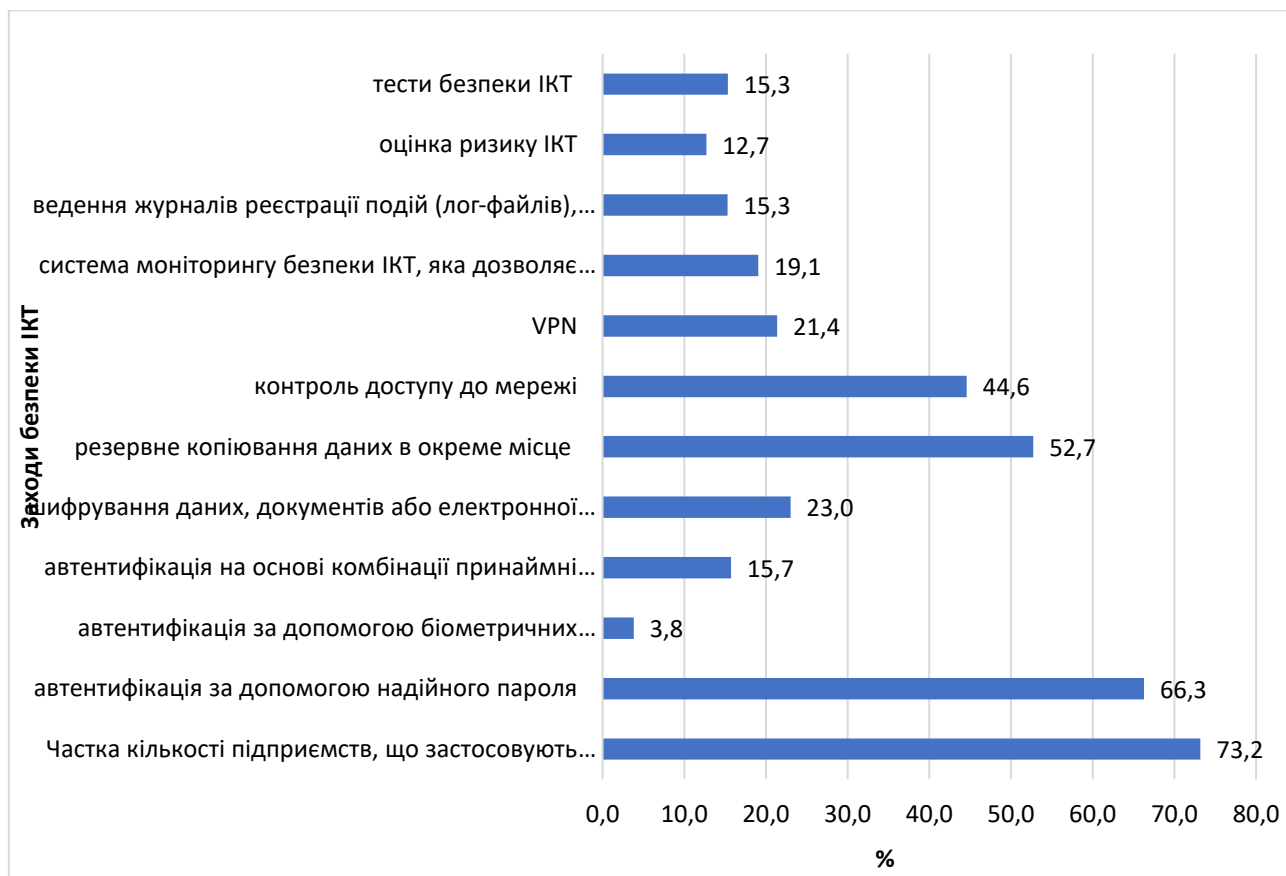


Рис. 2.13. Частота проведення заходів безпеки ІКТ загалом в інформаційних системах підприємств різних напрямів економічної діяльності у 2023 р.

Джерело: сформовано на основі даних [235]

Іншими засобами забезпечення безпеки інформаційних систем підприємства при використанні ІКТ технологій виступають ведення журналів реєстрації подій (лог-файлів), які дають можливість здійснювати аналіз після інцидентів безпеки ІКТ. Ці заходи впровадили 15,3% підприємств; 12,7% впроваджують оцінювання ризиків використання ІКТ, ще 15,3% використовують в своїй діяльності тестування безпеки ІК-технологій.

З метою зростання безпеки доступу до інформаційних систем при використанні інформаційних технологій підприємства впроваджують в ІКТ автентифікацію користувачів, використовуючи при цьому різні засоби безпеки. Так, 15,7% підприємств у 2023 р. використовували автентифікації на основі комбінування двох та більше механізмів автентифікації, а 3,8% підприємств впровадили автентифікацію за допомогою біометричних методів, проте на сьогоднішній день біометричні методи незважаючи на їх високу ефективність, поки що не мають широкого використання в забезпеченні безпеки інформаційно-комунікаційних систем підприємств.

Впровадження ефективних безпекових заходів та забезпечення належного рівня економічної безпеки при роботі з інформацією, використанням інформаційно-комунікаційних технологій, потребує залучення до цього процесу всіх працівників підприємства, що мають доступ до комп'ютерів та їх використовують, технічні цифрові засоби, інформацію в своїй роботі. Відповідно, важливим є своєчасне системне доведення до відома працівників всіх норм та правил безпеки при роботі з ІКТ, певних вимог яких вони повинні дотримуватися і водночас з наданням працівникам інформації для розуміння ними важливості та особистої відповідальності за порушення цих вимог. Це дасть можливість забезпечувати впровадження своєчасних превентивних дій, заходів та убезпечитися від настання ризикових подій та подальших негативних наслідків для діяльності підприємства. Таким чином, доведення до працівників підприємств інформації з питань безпеки ІКТ (табл. 2.10) може розглядатися як невід'ємна складова впровадження превентивних безпекових дій та заходів з забезпечення безпеки ІКТ.

Досліджуючи статистичні дані щодо доведення до працівників підприємства інформації з питань безпеки ІКТ, 2023 р. за різними напрямками економічної діяльності слід зазначити, що 59,8% від загальної кількості підприємств застосовують щодо цього самостійне навчання працівників чи поширюють внутрішню корпоративну інформацію щодо вимог безпеки.

Таблиця 2.10

Способи доведення до працівників підприємств інформації з питань безпеки ІКТ, 2023 р.

Види економічної діяльності	Частка кількості підприємств, що інформують співробітників з питань, безпеки ІКТ, у загальній кількості під-в за способами інформування, %		
	самостійне навчання або внутрішня доступна інформація	проходження обов'язкових навчальних курсів чи вивчення інструкцій	за контрактом
Усього	59,8	6,1	8,0
Переробна промисловість	58,8	5,4	8,3
Харчова промисловість	63,1	5,6	7,5
Легка промисловість	49,0	3,9	7,0
Деревообробна промисловість	52,0	4,6	5,3
Нафтохімічна промисловість	40,2	6,3	0,0
Хімічна промисловість	63,1	4,4	10,9
Фармацевтична промисловість	70,2	14,9	7,7
Металургійне виробництво	58,3	6,0	11,5
Виробництво комп'ютерів, електронної продукції	66,9	7,8	9,2
Виробництво елек.устаткування	64,4	4,7	3,7
Виробництво машин	58,7	5,5	10,4
Постачання електроенергії, газу	69,7	16,4	4,7
Будівництво	54,3	3,2	5,5
Оптова торгівля	63,6	5,9	7,2
Роздрібна торгівля	61,0	7,3	8,3
Транспорт, кур'єрська діяльність	58,8	4,4	8,2
Тимчасове розміщення, харчування	55,5	4,0	6,0
Телекомунікації (електрозв'язок)	79,8	8,2	18,0
Комп'ютерне програмування, консультування	69,7	25,9	26,9
Операції з нерухомим майном	64,2	4,1	5,4
Професійна, наукова діяльність	62,8	12,0	12,7
Консалтингова діяльність	64,6	10,0	13,7
Наукові дослідження та розробки	41,1	13,4	17,9
Туристична діяльність	64,9	7,2	9,8
Інформаційно-комунікаційні технології	73,5	19,0	19,8

Джерело: сформовано на основі даних [235]

При цьому, найбільш високим показник використання самонавчання чи поширення між працівниками інформації є на підприємствах фармацевтичної промисловості – 70,2% від загальної кількості підприємств; підприємствах що працюють в сфері телекомунікацій – 79,8%; організацій що працюють в сфері інформаційно-комунікаційних технологій – 73,5%; підприємств туристичної сфери – 64,9%; різних напрямів та видів консалтингової діяльності – 64,6%; в сфері операцій з нерухомістю – 64,2%; в сфері постачання електроенергетики, газу, пари – 69,7% підприємств; та в інших сферах.

Іншими заходами, є проходження працівниками обов’язкових навчальних курсів чи вивчення інструкцій. Загальний відсоток підприємств, які використовували у 2023 р. цей спосіб інформування працівників є незначним і становить 6,1% від загальної кількості підприємств.

При цьому, найбільш поширеним цей спосіб інформації є для працівників підприємств фармацевтичної галузі – 14,9% від всієї кількості підприємств; на підприємствах, що працюють в сфері постачання електроенергії та газу – 16,4% підприємств; в сфері комп’ютерного програмування та консультування – 25,9% підприємств та загалом в сфері інформаційно-комунікаційних технологій – 19% від загальної кількості підприємств. Іншим способом доведення до працівників підприємств інформації з питань безпеки ІКТ, є «спосіб за контрактом» який у 2023 р. загалом застосували 8% підприємств. Проте, частка застосування цього способу є вищою для підприємств металургійного виробництва та становить 11,5%; хімічної промисловості – 10,9%; комп’ютерного програмування та консультування – 26,9%; загалом серед підприємств сфери інформаційно-комунікаційних технологій – 19,8% підприємств; у сфері наукових досліджень – 17,9% , та у сфері телекомунікацій – 18% від загальної кількості підприємств.

Одним із важливих етапів діяльності із забезпечення безпеки інформаційних систем підприємства з плануванням і впровадженням безпекових заходів є розробка та затвердження документації, яка регламентує проведення заходів, дій чи процедур дотримання забезпечення безпеки ІКТ.

Дані щодо чисельності кількості підприємств, які мають відповідну документацію працюючи в різних напрямках економічної діяльності представлено на рис. 2.14.



Рис. 2.14. Частка підприємств, що мають документацію, яка регламентує проведення заходів, процедур з дотримання забезпечення безпеки ІКТ %

Джерело: сформовано на основі даних [235]

Так, найбільш активною сферою економічної діяльності, в якій підприємства мають розроблену документацію, що містить норми регламенти та вимоги щодо забезпечення безпеки використання ІКТ є комп'ютерне програмування та консультування, частка підприємств, що мають відповідну документацію в цій сфері діяльності становить 26,9% від загальної кількості підприємств. У сфері інформації та телекомунікацій частка підприємств які

володіють відповідною документацією становить 20,1% підприємств. У сфері інформаційно-комунікаційних технологій загалом цей показник становить 19%, що свідчить про високий рівень активності підприємств сфери інформаційно-комунікаційних технологій щодо підготовки та наявності відповідної безпекової документації.

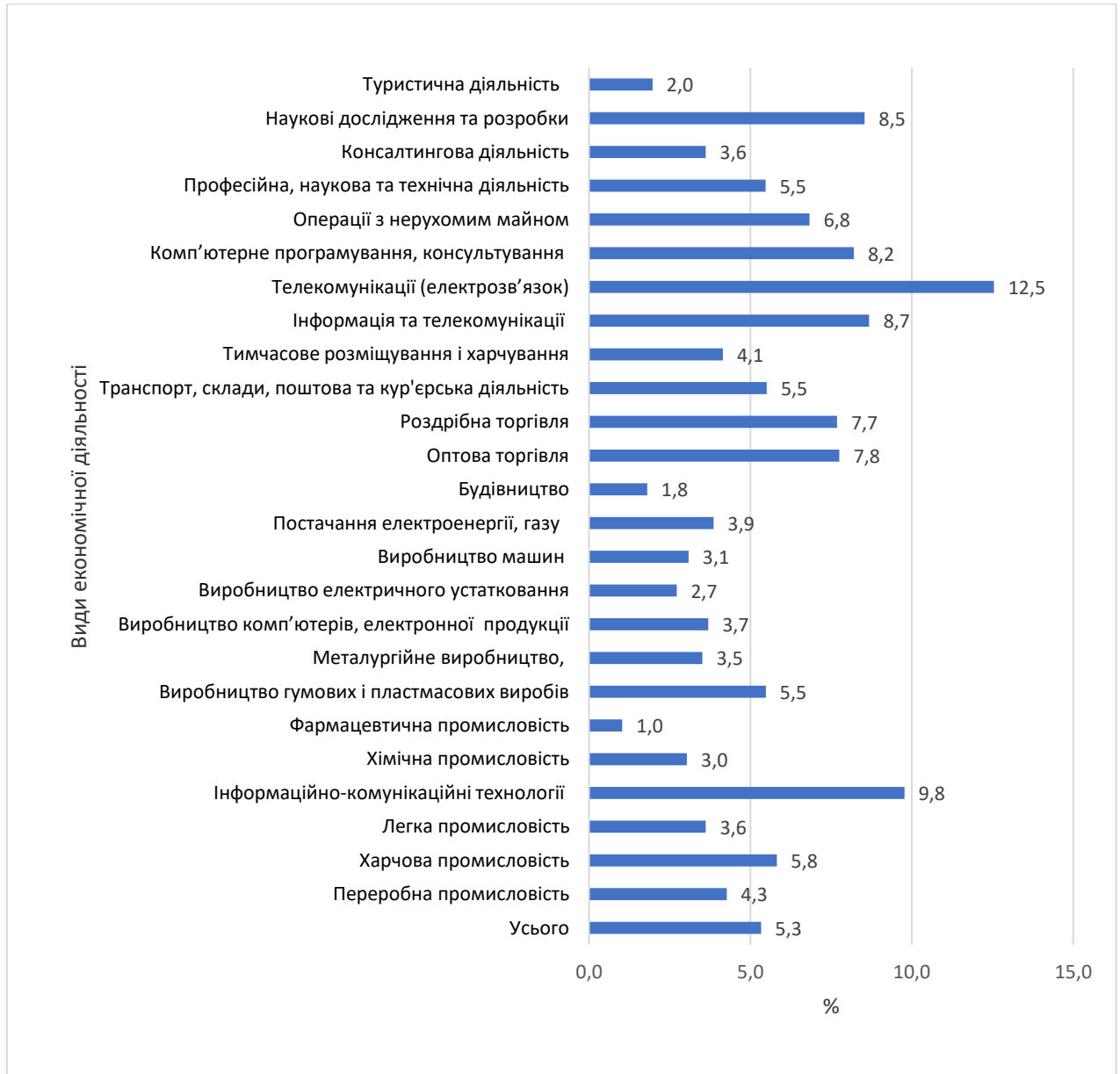


Рис. 2.15. Частка підприємств, які застосовують страхування від безпекових ризиків роботи з ІКТ, 2023 р.

Джерело: сформовано на основі даних [235]

В інших сферах економічної діяльності частка підприємств, що мають документацію яка регламентує проведення заходів, дій чи процедур дотримання забезпечення безпеки інформаційно-комунікаційних технологій є порівняно невисокою та коливається в межах від 2,7% до 16% від загальної кількості підприємств відповідного напрямку економічної діяльності.

Шукаючи різні шляхи та засоби забезпечення економічної безпеки в роботі з інформаційними системами підприємств при використанні інформаційно-комунікаційних технологій частина підприємств використовує в тому числі страхування від безпекових ризиків (рис. 2.15). Цей засіб забезпечення безпеки ІКТ не є поширеним і загалом його використовують 5,3% від загальної кількості підприємств.

Проте, серед підприємств в окремих видах економічної діяльності використання страхування набуло більш широкого використання. Так, у сфері телекомунікацій та електрозв'язку страхування від безпекових ризиків роботи з інформаційно-комунікаційними технологіями використовують 12,5% підприємств; страхування від ризиків роботи з ІКТ застосовують 9,8% підприємств в сфері самих інформаційно-комунікаційних технологій; 8,7% підприємств в сфері інформації та телекомунікацій загалом; 7,7% підприємств в сфері оптової торгівлі та 7,7% підприємств в сфері роздрібною торгівлі; 8,5% підприємств, що працюють в сфері інноваційних досліджень та розробок.

В переважній більшості використання страхування від ризиків роботи ІКТ застосовується при розробці та реалізації інноваційно-інвестиційних проектів, стартапів та є важливим дієвим засобом забезпечення безпеки в управлінні ризиками, який в майбутньому, з розвитком страхового ринку України, буде набувати більшого поширення та використання.

В результаті проведених досліджень ідентифіковано та узагальнено показники впровадження інноваційних цифрових технологій в управління системою економічної безпеки підприємства представлені на рис. 2.16.

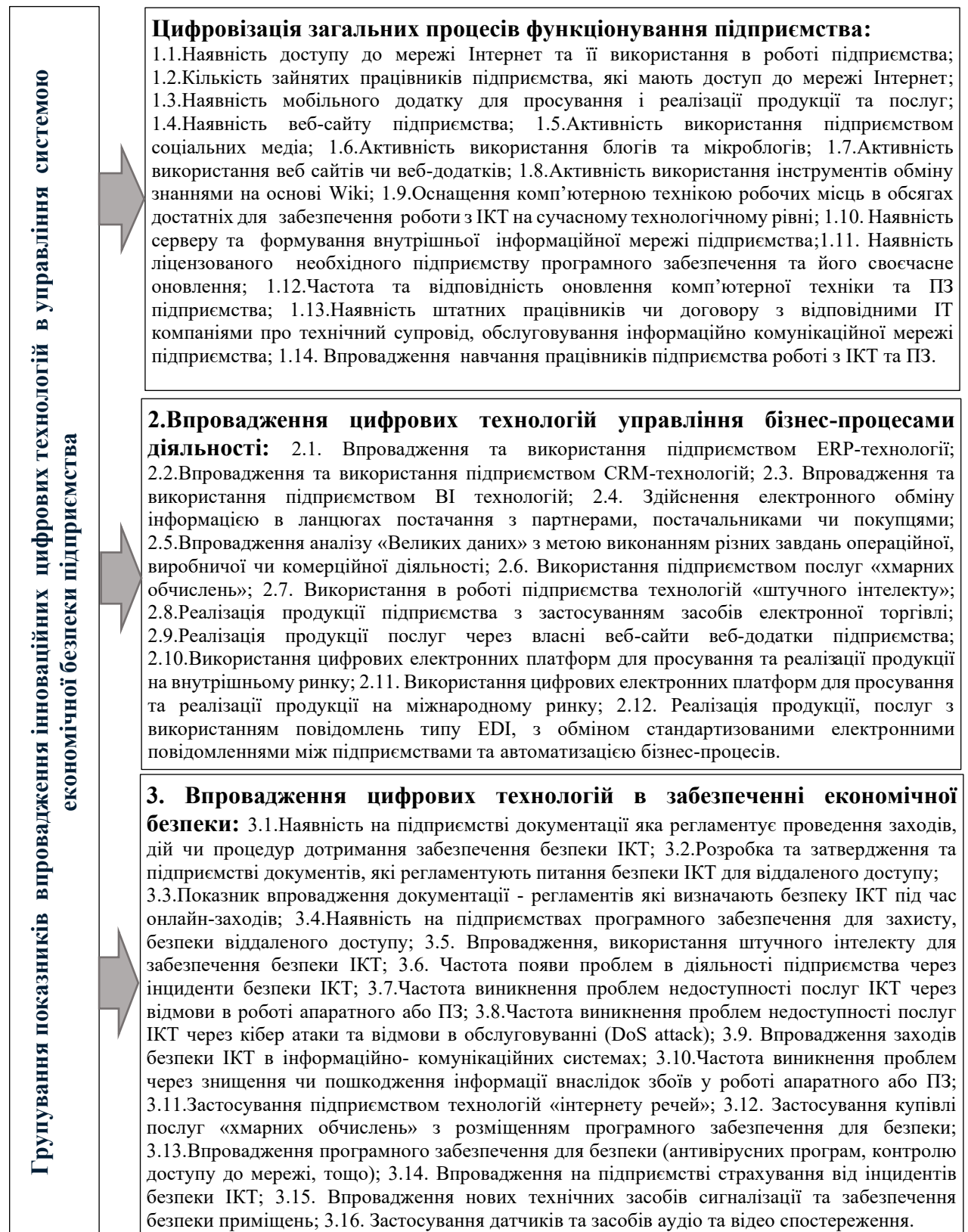


Рис. 2.16. Групування показників впровадження інноваційних цифрових технологій в управління системою економічної безпеки підприємства

Джерело: сформовано автором

Узагальнюючи результати проведеного дослідження ідентифіковано та систематизовано три групи показників: цифровізації загальних процесів функціонування підприємства; показників впровадження цифрових технологій для управління бізнес-процесами діяльності; показників впровадження цифрових технологій в забезпеченні економічної безпеки до складу яких віднесено п'ятдесят три показника комплексний системний аналіз яких забезпечує можливості для комплексного дослідження та аналізу проаналізувати процесів впровадження інноваційних цифрових технологій цифрового базису сучасного управління та на основі отриманих даних показників впроваджувати моніторинг та здійснювати подальше всебічне та системне оцінювання процесів управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

2.3. Оцінка процесів впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства

В сучасних складних турбулентних умовах функціонування прийняття виважених та обґрунтованих управлінських рішень набуває нової важливої ролі та значення. Кожне рішення керівників має ґрунтуватися на результатах детально проведеного об'єктивного неупередженого аналізу та оцінки та основі зібраних та опрацьованих фактологічних даних. Проте, незважаючи на значку кількість представлених в управлінні методик та моделей аналіз та оцінювання управління системою економічної безпеки підприємств на основі використання нових цифрових технологій є питанням новим та актуальним, яке потребує окремого розгляду та опрацювання.

Передусім, слід зазначити, що проведення такого аналізу та оцінювання потребує формування, розробки нової моделі, сформованої на засадах використання комплексного та системного підходів, оскільки сама економічна безпека та її забезпечення є поняттям комплексним, стосується всього

підприємства та всіх аспектів його функціонування, а не лише результатів, виконаних функцій, задач працюючого чи новоствореного підрозділу економічної безпеки. Як детально досліджувалось в першому розділі дисертації, саме поняття забезпечення економічної безпеки, стан безпеки включають мультисистемність та багатоаспектність підходів, оскільки сама економічна безпека та досягнення високого рівня її забезпечення виступають результатом ефективного захисту підприємства від зовнішніх та внутрішніх загроз із впровадженням комплексу превентивних заходів, забезпеченням ефективного використання ресурсів та досягнення високого рівня конкурентоспроможності, фінансової стійкості та ефективності діяльності підприємства, гармонізації та налагодження ефективних комунікацій із зовнішніми стейкхолдерами та під дією інших факторів.

Внаслідок цього формування такої моделі актуалізує питання комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

З цією метою в роботі пропонується розробка відповідної моделі та алгоритму розрахунку інтегрального індексу комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

Таким чином, з метою забезпечення такої комплексності необхідним є загальне охоплення функціонування не лише економічної безпеки, а й всіх інших складових, які прямо чи опосередковано впливають на діяльність підприємств, їх результати та можливості демонструвати належний рівень економічної безпеки та високу здатність протидіяти зовнішнім та внутрішнім ризикам і загрозам.

Проведення оцінювання рівня впровадження нових цифрових технологій має здійснюватися зі збиранням даних, дослідженням, аналізом та оцінюванням безпосередньо процесів загального використання цифрових інформаційних технологій в діяльності підприємств; впровадженням спеціалізованого програмного забезпечення цифрових технологій, які дають

можливість оптимізувати удосконалити та цифровізувати окремі процеси чи напрямки сфери функціональної діяльності підприємства; оцінити рівень впровадження нових цифрових технологій в забезпеченні економічної безпеки підприємства. Все це разом дає можливість для проведення комплексного оцінювання, впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

За основу формування моделі та використання математичного апарату проведених розрахунків було використано та адаптовано «Методичні рекомендації щодо розрахунку рівня економічної безпеки України», затверджені Наказом Міністерства економічного розвитку і торгівлі України № 1277 від 29.10.2013 р. [236].

Із зазначених методичних рекомендацій адаптовано алгоритм проведення та формули розрахунків інтегральних субіндексів економічної безпеки.

Проте, на відміну від зазначеної методики проектом дослідження та оцінювання в зазначеній моделі виступає мікрорівень підприємства, а саме впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства. Таким чином, замість низки складових та субіндексів макrorівня оцінювання економічної безпеки в зазначеній моделі дослідують мікрорівень підприємства з аналізом та оцінюванням ідентифікованих і визначених автором в підрозділі 2.1. та 2.2. показників-індикаторів економічної безпеки підприємства за трьома головними субіндексами оцінювання: цифровізації загальних процесів функціонування підприємства; використання цифрових технологій для управління бізнес-процесами діяльності; використання цифрових технологій в забезпеченні економічної безпеки.

Таким чином, особистим внеском автора в обґрунтованій розробленій моделі є ідентифікація та відбір показників оцінювання рівня економічної безпеки впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства; обґрунтування трьох головних

субіндексів, за якими буде здійснюватися оцінювання, адаптація формул та алгоритму оцінювання інтегральних субіндексів та загального інтегрального індексу відповідно до мети моделі – здійснення оцінювання та впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки на мікрорівні кожного конкретного підприємства незалежно від сфер та напрямів економічної діяльності, що разом забезпечує нові можливості для проведення аналізу, оцінювання та отримання об'єктивних комплексних даних щодо стану та рівня впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, дасть можливість виявити слабкі місця, недоліки та спланувати і впровадити своєчасні заходи з метою зростання рівня цифрової безпеки та ефективності підприємства у протидії ризикам та загрозам і дасть можливість для подальшого впровадження моніторингу як системи безперервного контролю над станом та рівнем управління системою економічної безпеки підприємства в умовах сучасної цифрової трансформації та зростання цифрових, інформаційних, кіберзагроз зовнішнього економічного середовища.

Використання моделі та проведення комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства здійснюється з послідовним виконанням етапів алгоритму, дій та розрахунків.

Модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства представлена на рис. 2.17. Як вже зазначалося проведення комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства потребує визначення етапів та їх послідовного виконання.

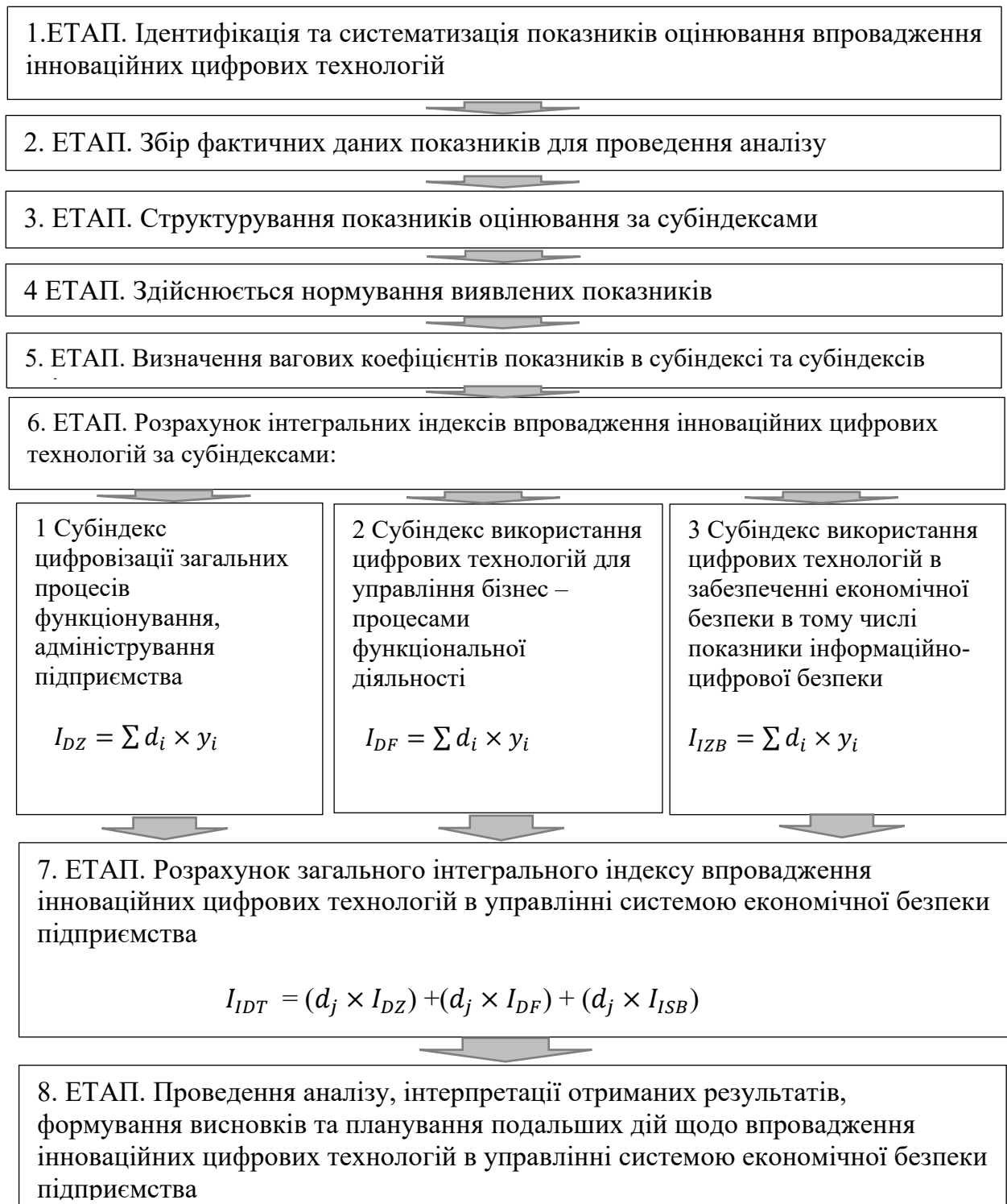


Рис. 2.17. Модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства

Джерело: сформовано автором

На першому етапі розробки моделі комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства здійснюється ідентифікація та відбір множини показників які характеризують впровадження тих чи інших цифрових технологій, програмного забезпечення, процесів що свідчитимуть про цифровізацію управління та різних аспектів функціонування підприємства. Такі показники ідентифіковано в підрозділі 2.1. дослідження. Всього відібрано для проведення аналізу 52 показники.

В таблиці. 2.11 представлено показники цифровізації загальних процесів функціонування підприємства.

Таблиця 2.11

Показники цифровізації загальних процесів функціонування

№	Найменування показника	Показник
1	1.1.Наявність доступу до мережі Інтернет та його використання в роботі підприємства	Y_{DZ1}
2	1.2.Кількість зайнятих працівників підприємства, які мають доступ до мережі Інтернет	Y_{DZ2}
3	1.3.Наявність мобільного додатку для просування і реалізації продукції та послуг	Y_{DZ3}
4	1.4. Наявність веб-сайту підприємства	Y_{DZ4}
5	1.5.Активність використання підприємством соціальних медіа	Y_{DZ5}
6	1.6.Активність використання блогів та мікроблогів	Y_{DZ6}
7	1.7.Активність використання веб сайтів чи веб-додатків	Y_{DZ7}
8	1.8.Активність використання інструментів обміну знаннями на основі Wiki	Y_{DZ8}
9	1.9. Оснащення комп'ютерною технікою робочих місць в обсягах достатніх для забезпечення роботи з ІКТ	Y_{DZ9}
10	1.10. Наявність серверу та формування внутрішньої інформаційної мережі підприємства	Y_{DZ10}
11	1.11. Наявність ліцензованого необхідного підприємству програмного забезпечення та його своєчасне оновлення	Y_{DZ11}
12	1.12. Частота та відповідність оновлення комп'ютерної техніки та ПЗ	Y_{DZ12}
13	1.13.Наявність штатних працівників чи договору з відповідними ІТ компаніями про технічний супровід, обслуговування	Y_{DZ13}
14	1.14. Впровадження навчання працівників підприємства роботі з ІКТ та ПЗ	Y_{DZ14}

Джерело: сформовано автором

В таблиці 2.12 представлено показники впровадження цифрових технологій для управління бізнес-процесами діяльності.

Таблиця 2.12.

Показники впровадження цифрових технологій для управління бізнес-процесами діяльності

№	Найменування показника	Показник
1	2.1. Впровадження та використання підприємством ERP-технології	Y_{DF1}
2	2.2. Впровадження та використання підприємством CRM-технологій	Y_{DF2}
3	2.3. Впровадження та використання підприємством BI технології	Y_{DF3}
4	2.4. Здійснення електронного обміну інформацією в ланцюгах постачання з партнерами, постачальниками чи покупцями	Y_{DF4}
5	2.5. Впровадження аналізу «Великих даних» з метою виконання різних завдань операційної, виробничої чи комерційної діяльності	Y_{DF5}
6	2.6. Використання підприємством послуг «хмарних обчислень»	Y_{DF6}
7	2.7. Використання в роботі підприємства технологій «штучного інтелекту»	Y_{DF7}
8	2.8. Реалізація продукції підприємства з застосуванням засобів електронної торгівлі	Y_{DF8}
9	2.9. Реалізація продукції послуг через власні веб-сайти веб-додатки підприємства	Y_{DF9}
10	2.10. Використання цифрових електронних платформ для просування та реалізації продукції на внутрішньому ринку	Y_{DF10}
11	2.11. Використання цифрових електронних платформ для просування та реалізації продукції на міжнародному ринку	Y_{DF11}
12	2.12. Реалізація продукції, послуг з використанням повідомлень типу EDI, з обміном стандартизованими електронними повідомленнями між підприємствами та автоматизацією бізнес-процесів.	Y_{DF12}

Джерело: сформовано автором

В таблиці 2.13 представлено показники впровадження цифрових технологій в забезпеченні економічної безпеки.

Таблиця 2.13

Показники впровадження цифрових технологій в забезпеченні економічної безпеки

№	Найменування показника	Показник
1	3.1.Наявність на підприємстві документації яка регламентує забезпечення безпеки ІКТ	Y_{IZB1}
2	3.2.Розробка та затвердження та підприємстві документів, які регламентують питання безпеки ІКТ для віддаленого доступу	Y_{IZB2}
3	3.3.Показник впровадження документації - регламентів які визначають безпеку ІКТ під час онлайн-заходів в режимі реального часу, с застосуванням інтернет	Y_{IZB3}
4	3.4.Наявність на підприємствах програмного забезпечення для захисту, безпеки віддаленого доступу	Y_{IZB4}
5	3.5. Впровадження, використання штучного інтелекту для забезпечення безпеки інформаційно- комунікаційних технологій	Y_{IZB5}
6	3.6.Частота появи проблем в діяльності підприємства через інциденти безпеки ІКТ	Y_{IZB6}
7	3.7.Частота виникнення проблем недоступності послуг ІКТ через відмови в роботі апаратного або ПЗ	Y_{IZB7}
8	3.8.Частота виникнення проблем недоступності послуг ІКТ через кібер атаки та відмови в обслуговуванні (DoS attack)	Y_{IZB8}
9	3.9.Впровадження заходів безпеки ІКТ в інформаційно- комунікаційних системах	Y_{IZB9}
10	3.9.1. Застосування автентифікація за допомогою надійного пароля	Y_{IZB10}
11	3.9.2. Застосування автентифікація за допомогою біометричних методів	Y_{IZB11}
12	3.9.3. Застосування автентифікації на основі комбінування принаймні двох та більше механізмів, засобів	Y_{IZB12}
13	3.9.4. Застосування шифрування даних, документів або пошти	Y_{IZB13}
14	3.9.5. Застосування резервного копіювання інформації в сховища	Y_{IZB14}
15	3.9.6. Застосування контролю доступу до мережі та VPN	Y_{IZB15}
16	3.9.7. Застосування системи моніторингу безпеки ІКТ	Y_{IZB16}
17	3.9.8. Застосування ведення журналів реєстрації подій (лог-файлів), які дають можливість здійснювати аналіз інцидентів безпеки ІКТ	Y_{IZB17}
18	3.9.9. Застосування на підприємстві оцінювання ризику ІКТ	Y_{IZB18}
19	3.9.10. Застосування на підприємстві тестування безпеки ІКТ	Y_{IZB19}
20	3.10.Частота виникнення проблем через знищення чи пошкодження інформації внаслідок збоїв у роботі апаратного або ПЗ	Y_{IZB20}
21	3.11.Застосування підприємством технологій «інтернету речей»	Y_{IZB21}
22	3.12. Застосування купівлі послуг «хмарних обчислень» з розміщенням програмного забезпечення для безпеки	Y_{IZB22}
23	3.13. Впровадження програмного забезпечення для безпеки (антивірусних програм, контролю доступу до мережі, тощо)	Y_{IZB23}
24	3.14. Впровадження на підприємстві страхування від інцидентів безпеки ІКТ	Y_{IZB24}
25	3.15. Впровадження нових технічних засобів сигналізації та забезпечення безпеки приміщень	Y_{IZB25}
26	3.16. Застосування датчиків та засобів аудіо та відео спостереження	Y_{IZB26}

Джерело: сформовано автором

На другому етапі розробки моделі розроблено листи опитування. Форми листів опитування підприємства приведені в Додатку В. цього дисертаційного дослідження.

На другому етапі здійснюється збір інформації діяльності групи провідних компаній в сфері інформаційних технологій та високих технологій з метою отримання фактичних значень показників. Подальший аналіз та обробка цих даних дасть можливість для проведення аналізу оцінки та проведення досліджень.

На третьому етапі застосування моделі проводять структурування показників оцінювання за субіндексами. Загалом субіндекс виступає показником який входить до структури загального інтегрального індексу, та є сумою відповідних показників-індикаторів впровадження для цифрових технологій із урахуванням того, що показники повинні бути нормалізованими та має бути враховано вагу кожного показника в загальній сукупності субіндексу.

Таким чином, кожний із визначених у даній моделі субіндексів виступає складовою та процесом більш вищого порядку, а саме складовою загального індексу впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

Загалом в моделі виявлено три головні субіндекси до яких відносять показники структуровані відповідно до приналежності до певної групи забезпечення процесів функціонування, а разом ці субіндекси та їх показники формують загальну сукупність необхідну для проведення аналізу та оцінювання.

Таким чином, виявлено та структуровано три субіндекси. Перший субіндекс до якого відносять показники цифровізації загальних процесів функціонування, адміністрування підприємства; другий субіндекс показники якого дають можливість оцінити використання цифрових технологій для управління бізнес-процесами функціональної діяльності; третій субіндекс який включає показники, що дають можливість оцінити та проаналізувати

використання цифрових технологій в забезпеченні економічної безпеки підприємства в тому числі показників інформаційно-цифрової безпеки.

Результати такого структурування представлені в таблицях 2.15, 2.16, 2.17.

На четвертому етапі здійснюється нормування виявлених показників. Воно здійснюється з урахуванням рекомендацій зазначених в Державній методиці [236] з адаптацією розрахункових даних до структури та алгоритму цієї моделі та даних, що використовуються для дослідження [236].

Для розрахування показників застосовують лінійну функцію враховуючи, що фактичні значення показників мають бути зіставними за величинами та знаходитися у визначених інтервалах від 0 до 1., або ж у відсотках і до 1-100%. За цих умов розраховано нормоване значення показника буде знаходитися в цих діапазонах та наближатися до свого найбільш оптимального значення -1.

Нормування показників-стимуляторів y_{ijj} розраховується за формулою 2.1.:

$$Y_{ij} = \frac{x_{ijj} - x_{\min}}{x_{\min} - x_{\max}} \quad (2.1.)$$

Де: x_{ijj} - фактичне значення і-го показника впровадження цифрових технологій;

$x_{\min}$ - мінімальне значення і-го показника впровадження цифрових технологій;

$x_{\max}$ - максимальне значення і-го показника впровадження цифрових технологій.

Або ж для нормування показників - стимуляторів та де-стимуляторів нормування розраховується та здійснюється за формулою:

$$Y_{ijj} = \begin{cases} x_{ij} / x_{\text{opt}} \text{ якщо показник є стимулятором, при цьому:} \\ Y_{ijj} = 1 \text{ при } x_{ij} = x_{\text{opt}} \\ x_{\text{opt}} / x_{ij} \text{ якщо показник є де-стимулятором, при цьому} \\ Y_{ijj} = 1 \text{ при } x_{ij} = x_{\text{opt}} \end{cases} \quad (2.1.1.)$$

Де: x_{opt} - максимальне значення і-го показника впровадження цифрових технологій.

На п'ятому етапі здійснюється визначення вагових коефіцієнтів показників в субіндексі та субіндексів оцінки яке дає можливість визначати вагу того чи іншого показника в загальній сукупності показників індикаторів за кожним із субіндексів, а також на наступному етапі здійснюється визначення ваги та значення кожного субіндексу в загальному значенні інтегрального індексу впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

Розрахунок інтегрального індексу за окремими субіндексами та загалом впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки розраховують з використанням вагових коефіцієнтів які визначають із застосуванням експертної оцінки.

Таким чином, розрахунок вагових коефіцієнтів для окремих показників та відповідно субіндексів розраховують за формулою 2.2.

$$d_i = \frac{a_i}{\sum_{i=1}^n a_i}, \quad (2.2.)$$

Де i , – індикатор який визначає значення агрегованого індикатора чи субіндексу в загальній сукупності окремих субіндексів та загальному значенні інтегрального індексу до $i = (1, 2, 3 \dots i \text{ т. д.})$.

Де a_i – оцінка яка визначає важливість i -го показника для субіндексів.

Де d_i – ваговий коефіцієнт який визначає вагу кожного i -го показника в сукупності в інтегральному індексі оцінювання.

Результати здійснених розрахунків ваги кожного з показників зазначається в таблицях нормалізованих показників ДОДАТКУ Д.

Результати розрахунків вагових коефіцієнтів окремих субіндексів в загальному інтегральному індексі оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства приведено в таблиці 2.14.

Таблиця 2.14.

**Вагові коефіцієнти окремих субіндексів в зальному інтегральному
індексі оцінювання**

№	Субіндекси	Формула	Ваговий коефіцієнт
1	Субіндекс цифровізації загальних процесів функціонування, адміністрування підприємства	I_{DZ}	0,334
2	Субіндекс використання цифрових технологій для управління бізнес-процесами функціональної діяльності	I_{DF}	0,333
3	Субіндекс використання цифрових технологій в забезпеченні економічної безпеки.	I_{IZB}	0,333

Джерело: сформовано автором

На шостому етапі здійснюється розрахунок інтегральних індексів впровадження інноваційних цифрових технологій за кожним із субіндексів.

Розрахунок інтегрального індексу за субіндексом цифровізації загальних процесів функціонування, адміністрування підприємства визначається за формулою 2.3.:

$$I_{DZ} = \sum d_i \times y_i, \quad (2.3)$$

Де: I_{DZ} – агрегований субіндекс цифровізації загальних процесів функціонування, адміністрування підприємства;

d_i – вагові коефіцієнти, що визначають ступінь внеску i -го показника в інтегральний індекс субіндексу цифровізації загальних процесів функціонування, адміністрування підприємства;

y_i – нормалізована оцінка i -го показника-індикатора.

Розрахунок інтегрального індексу за субіндексом використання цифрових технологій для управління бізнес-процесами функціональної діяльності підприємства визначається за формулою 2.4.:

$$I_{DF} = \sum d_i \times y_i, \quad (2.4)$$

Де: I_{DF} – агрегований субіндекс використання цифрових технологій для управління бізнес-процесами функціональної діяльності підприємства;

d_i – вагові коефіцієнти, що визначають ступінь внеску i -го показника в інтегральний індекс субіндексу використання цифрових технологій для управління бізнес-процесами функціональної діяльності підприємства;

y_i – нормалізована оцінка i -го показника-індикатора.

Розрахунок інтегрального індексу за субіндексом використання цифрових технологій в забезпеченні економічної безпеки в тому числі показників інформаційно-цифрової безпеки визначаються за формулою 2.5:

$$I_{IZB} = \sum d_i \times y_i, \quad (2.5)$$

де I_{IZB} – агрегований субіндекс використання цифрових технологій в забезпеченні економічної безпеки;

d_i – вагові коефіцієнти, що визначають ступінь внеску i -го показника в інтегральний індекс субіндексу використання цифрових технологій в забезпеченні економічної безпеки;

y_i – нормалізована оцінка i -го показника-індикатора.

На сьомому етапі здійснюється розрахунок Загального Інтегрального індексу впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства за формулою 2.6.:

$$I_{IDT} = (d_j \times I_{DZ}) + (d_j \times I_{DF}) + (d_j \times I_{ISB}) \quad (2.6.)$$

де, d_j – вагові коефіцієнти які визначають ступінь внеску субіндексів в інтегральний індекс впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства;

I_{IDT} – загальний інтегральний індекс впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

На восьмому етапі проводять аналіз та інтерпретацію отриманих результатів, формування висновків та планування подальших дій щодо впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

Відповідно до «Методичних рекомендації щодо розрахунку рівня економічної безпеки України» затверджених Наказом Міністерства економічного розвитку і торгівлі України № 1277 від 29.10.2013 р. оцінювання показників-індикаторів здійснюється в діапазоні від 0 до 1, при чому показник «1» дорівнює найкращому найбільш високому рівню економічної безпеки, а показник «0» найгіршому.

Формуючи умовну шкалу порівняння характерну для значення інтегрального індексу при розрахунку індексу економічної безпеки зазначимо, що значення індексу 1 відповідатиме високому рівню впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства; значення 0,6-0,8 стабільному рівню поступового впровадження; значення менше 0,5 означає відсутність системних процесів та низький рівень впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

З метою проведення емпіричних досліджень та апробації розробленої моделі на практиці в межах дисертаційного дослідження розроблено листи опитування та проведено опитування збір інформації щодо впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки групи провідних підприємств які працюють в сфері високих технологій, а саме: ТОВ «Леві9 Україна», ТОВ «ЄВРОУКРСІТІГРІН», ТОВ «ЕПАМ ДІДЖИТАЛ», ТОВ "ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНІХРОМ", ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ ІМ.Є.О. ПАТОНА" НАН УКРАЇНИ.

На основі зібраних даних проведено відповідні розрахунки представлені в ДОДАТКУ Д до дисертаційного дослідження. Результати проведених розрахунків моделі оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства представлено в таблиці 2.15. та на рис. 2.18

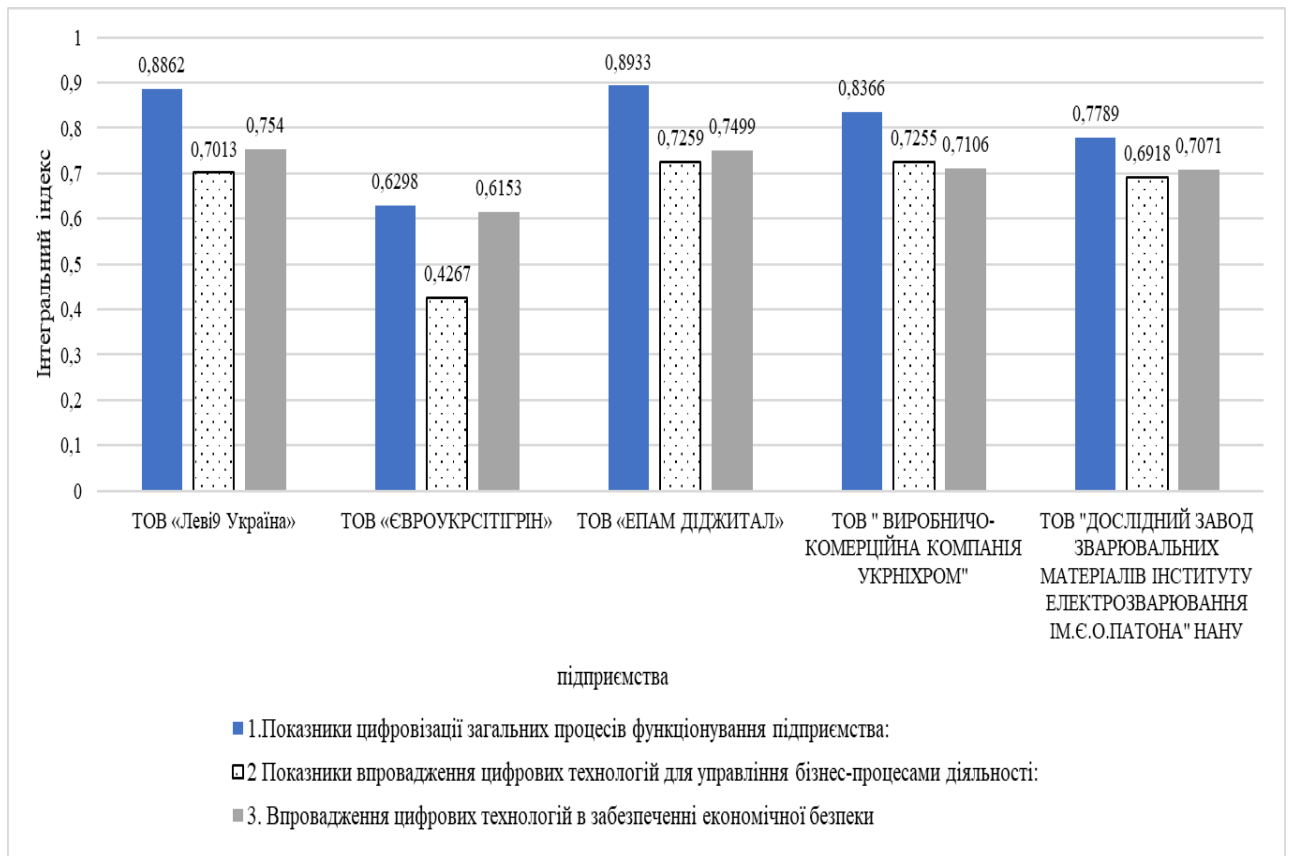


Рис. 2.18. Результат розрахунків інтегральних індексів за субіндексами впровадження інноваційних цифрових технологій

Джерело: розраховано автором

В результаті розрахунку інтегрального субіндексу цифровізації загальних процесів функціонування, адміністрування підприємства; інтегрального субіндексу оцінювання використання цифрових технологій для управління бізнес-процесами функціональної діяльності; та інтегрального субіндексу використання цифрових технологій в забезпеченні економічної безпеки підприємства в тому числі показників інформаційно-цифрової безпеки підприємств ТОВ «Леві9 Україна», ТОВ «ЄВРОУКРСІТІГРІН», ТОВ «ЕПАМ ДІДЖИТАЛ», ТОВ "ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНІХРОМ", ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ ІМ.Є.О. ПАТОНА" НАН УКРАЇНИ виявлено, що отримані результати за показниками цифровізації загальних процесів функціонування знаходяться в діапазоні від

0,6298 до 0,8933 що свідчить про поступове системне впровадження інноваційних цифрових технологій та середній рівень загальної цифровізації діяльності підприємств.

Таблиця 2.15.

Результати проведених розрахунків моделі оцінювання впровадження інноваційних цифрових технологій в управлінні СЕБП

Субіндекси	Вагові коеф	ТОВ «Леві9 Україна»	ТОВ «ЄВРО УКРСІПГРН»	ТОВ «ЕПАМ ДІДЖИТАЛ»	ТОВ " ВИРОБ НИЧО- КОМЕРЦІЙНА КОМПАНІЯ УКР НІХРОМ"	ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРО
Показники цифровізації загальних процесів функціонування підприємства:	0,334	0,8862	0,6298	0,8933	0,8366	0,7789
Показники впровадження цифрових технологій для управління бізнес-процесами діяльності:	0,333	0,7013	0,4267	0,7259	0,7255	0,6918
Впровадження цифрових технологій в забезпеченні економічної безпеки	0,333	0,754	0,6153	0,7499	0,7106	0,7071
Загальний інтегральний індекс		0,7806	0,5573	0,7898	0,7576	0,7259

Джерело: розраховано автором

Інтегральний субіндекс оцінювання використання цифрових технологій для управління бізнес-процесами функціональної діяльності знаходиться в діапазоні від 0,4267 до 0,7259, що свідчить про середній рівень активності використання підприємствами інноваційних цифрових технологій в управління бізнес-процесами функціональної та операційної діяльності підприємства, що передусім обумовлено самою специфікою діяльності підприємств та необхідністю впровадження таких технологій. Інтегральний субіндекс використання цифрових технологій в забезпеченні економічної безпеки підприємств знаходиться на різних рівнях від 0,6153 до 0,754 в діапазоні значень від 0,6 до 0,8, що є середнім рівнем та також свідчить про

системне поступове впровадження інноваційних цифрових технологій в управління системою економічної безпеки цих підприємств, що забезпечує більші можливості для забезпечення безпеки в здійсненні як стратегічної діяльності так і в оперативному управлінні системою економічної безпеки зазначених підприємств.

Результати розрахунків інтегральних індексів за субіндексами впровадження інноваційних цифрових технологій п'яти вітчизняних підприємств ТОВ «Леві9 Україна», ТОВ «ЄВРОУКРСІТІГРІН», ТОВ «ЕПАМ ДІДЖИТАЛ», ТОВ "ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНІХРОМ", ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ ІМ.Є.О. ПАТОНА" НАН УКРАЇНИ представлено на рис. 2.19.

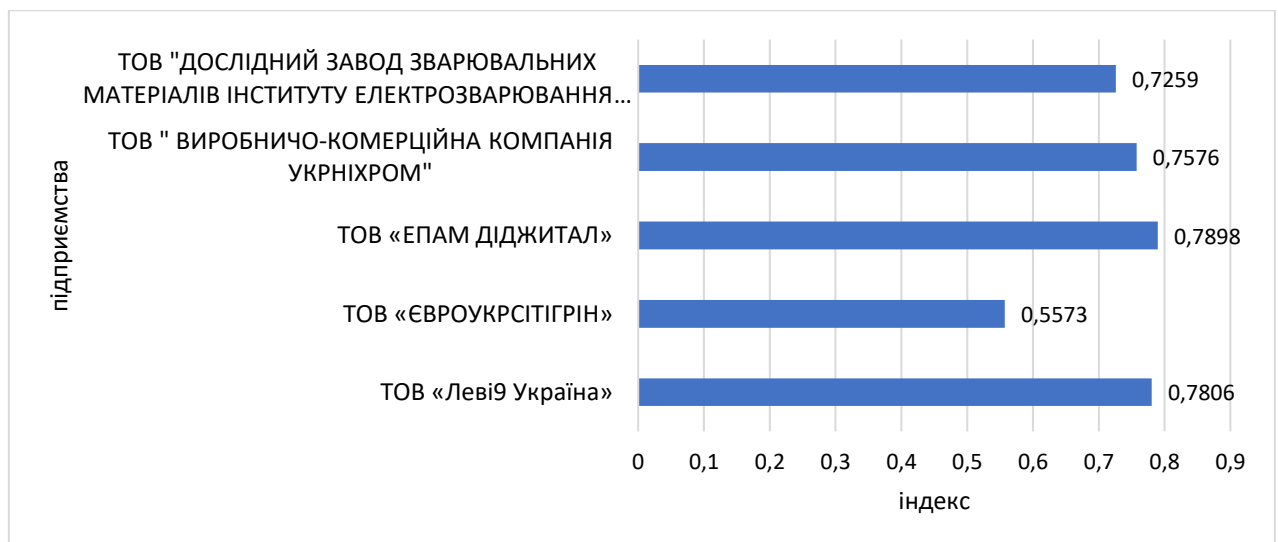


Рис. 2.19. Результат розрахунків Загального інтегрального індексу впровадження інноваційних цифрових технологій вітчизняних підприємств

Джерело: розраховано автором

В результаті застосування моделі комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та проведених розрахунків виявлено, що загальний інтегральний індекс впровадження інноваційних цифрових

технологій п'яти вітчизняних підприємств ТОВ «Леві9 Україна», ТОВ «ЄВРОУКРСІТІГРІН», ТОВ «ЕПАМ ДІДЖИТАЛ», ТОВ "ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНІХРОМ", ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ ІМ. Є.О. ПАТОНА" НАН УКРАЇНИ має різні значення, що знаходяться в діапазоні від 0,7 до 0,8 що свідчить про стабільний середній рівень впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та можливості для подальшого та більш широкого використання інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства з метою удосконалення процесів та системи управління економічною безпекою цих підприємств на відповідному сучасному високотехнологічному рівні.

Висновки до Розділу 2

Дослідження аспектів управління системою економічної безпеки підприємства з використанням інноваційних технологій потребує дефрагментації поділу на складові функціональної сфери всієї діяльності підприємств та детального розгляду показників застосування інноваційних цифрових технологій, які впливатимуть на результати виконання роботи та ефективності тих чи інших сфер діяльності підприємства, фінансової, операційної, інноваційно- інвестиційної діяльності, маркетингової діяльності з просуванням та реалізацією продукції та інших сферах, що прямо чи опосередковано здійснюють впливи на результати роботи, ефективність, стабільність функціонування підприємства і таким чином впливають на забезпечення рівня економічної безпеки підприємства.

Проведено аналіз та сформовано проекцію впливу застосування інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, яка дала можливість виявити та ідентифікувати вплив

використання цифрових технологій загального спрямування, інноваційних цифрових технологій управління і забезпечення функціональної діяльності та безпосередньо цифрових технологій, які використовуються в забезпеченні економічної безпеки підприємства, загальне та комплексне використання яких дають можливість здійснювати управління системою економічної безпеки підприємства на сучасному цифровому рівні та забезпечувати належний рівень економічної безпеки підприємства в умовах нових цифрових викликів та загроз.

В результаті проведеного дослідження ідентифіковано та систематизовано три групи показників (1) цифровізації загальних процесів функціонування підприємства, (2) показників впровадження цифрових технологій для управління бізнес-процесами діяльності та (3) показників впровадження цифрових технологій в забезпеченні економічної безпеки всього п'ятдесят два показника комплексний системний аналіз яких дасть можливість дослідити та проаналізувати процеси впровадження інноваційних цифрових технологій цифрового базису сучасного управління та на основі яких може бути здійснене подальше всебічне та системне оцінювання процесів управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Відповідно до проведеної ідентифікації та групування до першої групи показників віднесено показники цифровізації загальних процесів функціонування підприємства а саме: наявність доступу до мережі Інтернет та його використання в роботі підприємства; кількість зайнятих працівників підприємства, які мають доступ до мережі Інтернет; наявність мобільного додатку для просування і реалізації продукції та послуг; наявність веб-сайту підприємства; активність використання підприємством соціальних медіа; активність використання блогів та мікроблогів; активність використання веб-сайтів чи веб-додатків; активність використання інструментів обміну знаннями на основі Wiki; оснащення комп'ютерною технікою робочих місць в обсягах достатніх для забезпечення роботи з ІКТ на сучасному технологічному

рівні; наявність серверу та формування внутрішньої інформаційної мережі підприємства; наявність ліцензованого необхідного підприємству програмного забезпечення та його своєчасне оновлення; частота та відповідність оновлення комп'ютерної техніки та ПЗ підприємства; наявність штатних працівників чи договору з відповідними ІТ компаніями про технічний супровід, обслуговування інформаційно-комунікаційної мережі підприємства; впровадження навчання працівників підприємства роботі з ІКТ та ПЗ.

До другої групи віднесено показники використання цифрових технологій для управління бізнес-процесами діяльності в тому числі: впровадження та використання підприємством ERP-технології впровадження та використання підприємством CRM-технологій; впровадження та використання підприємством ВІ технологій; здійснення електронного обміну інформацією в ланцюгах постачання з партнерами, постачальниками чи покупцями; впровадження аналізу «Великих даних» з метою виконання різних завдань операційної, виробничої чи комерційної діяльності; використання підприємством послуг «хмарних обчислень»; використання в роботі підприємства технологій «штучного інтелекту»; реалізація продукції підприємства з застосуванням засобів електронної торгівлі; реалізація продукції послуг через власні веб-сайти веб-додатки підприємства; використання цифрових електронних платформ для просування та реалізації продукції на внутрішньому ринку; використання цифрових електронних платформ для просування та реалізації продукції на міжнародному ринку; реалізація продукції, послуг з використанням повідомлень типу EDI, з обміном стандартизованими електронними повідомленнями між підприємствами та автоматизацією бізнес-процесів.

Третя група об'єднує ідентифіковані показники використання цифрових технологій в забезпеченні економічної безпеки: наявність на підприємстві документації яка регламентує проведення заходів, дій чи процедур дотримання забезпечення безпеки ІКТ; розробка та затвердження та підприємстві документів, які регламентують питання безпеки ІКТ для

віддаленого доступу; показник впровадження документації - регламентів які визначають безпеку інформаційно-комунікаційних технологій під час онлайн-заходів в режимі реального часу, с застосуванням Інтернет; наявність на підприємствах програмного забезпечення для захисту, безпеки віддаленого доступу; впровадження, використання штучного інтелекту для забезпечення безпеки інформаційно-комунікаційних технологій; частота появи проблем в діяльності підприємства через інциденти безпеки ІКТ; частота виникнення проблем недоступності послуг ІКТ через відмови в роботі апаратного або ПЗ; частота виникнення проблем недоступності послуг ІКТ через кібер атаки та відмови в обслуговуванні (DoS attack); впровадження заходів безпеки ІКТ в інформаційно-комунікаційних системах; частота виникнення проблем через знищення чи пошкодження інформації внаслідок збоїв у роботі апаратного або ПЗ; застосування підприємством технологій «інтернету речей»; застосування купівлі послуг «хмарних обчислень» з розміщенням програмного забезпечення для безпеки (антивірусних програм, контролю доступу до мережі, тощо); впровадження програмного забезпечення для безпеки (антивірусних програм, контролю доступу до мережі, тощо); впровадження на підприємстві страхування від інцидентів безпеки ІКТ; впровадження нових технічних засобів сигналізації та забезпечення безпеки приміщень; застосування датчиків та засобів аудіо та відео спостереження.

Розроблено модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, що передбачає оцінювання на трьох рівнях: рівні загальних процесів функціонування, рівні окремих бізнес-процесів діяльності та в забезпеченні економічної безпеки підприємства. Крім того модель передбачає комплексне оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки, що забезпечує нові можливості для проведення аналізу, оцінювання та отримання об'єктивних комплексних даних щодо стану та рівня впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та

дозволяє впровадити моніторинг та виявити слабкі місця, недоліки, спланувати своєчасні заходи з метою зростання рівня цифрової безпеки та ефективності підприємства у протидії ризикам та загрозам в умовах сучасної цифрової трансформації, зростання рівня кіберзагроз зовнішнього середовища.

Алгоритм розрахунку моделі комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства передбачає виконання таких етапів: (1) ідентифікації та систематизації показників – індикаторів оцінювання впровадження інноваційних цифрових технологій; (2) збору фактичних даних показників для проведення аналізу; (3) структурування показників індикаторів оцінювання за субіндексами; (4) здійснення нормування виявлених показників; (5) визначення вагових коефіцієнтів показників в субіндексі та субіндексів; (6) розрахунку інтегральних індексів впровадження інноваційних цифрових технологій за субіндексами: цифровізації загальних процесів функціонування, адміністрування підприємства; субіндекс використання цифрових технологій для управління бізнес – процесами функціональної діяльності; субіндексу використання цифрових технологій в забезпеченні економічної безпеки в тому числі показники інформаційно-цифрової безпеки; (7) розрахунком загального інтегрального індексу впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства; (8) проведенням аналізу, інтерпретації отриманих результатів, формування висновків та планування подальших дій щодо впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

Результати проведених досліджень та розробок висвітлено у працях автора: [237, 238, 239].

РОЗДІЛ 3. УДОСКОНАЛЕННЯ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ ІННОВАЦІЙНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ

3.1. Розбудова системи економічної безпеки підприємства на основі інноваційних цифрових технологій

В сучасних умовах соціально-економічного розвитку, значних технологічних змін та трансформацій, пов'язаних із впровадженням нових інформаційних технологій, цифровізацією всіх сфер економіки та суспільного життя людства, ефективність функціонування та подальші можливості до розвитку кожного окремого підприємства, як суб'єкта господарювання залежать від його конкурентних позицій та можливостей своєчасно й адекватно відповідати на ризики та загрози, в тому числі нові, пов'язані із масовим впровадженням нових цифрових технологій.

В суспільно-економічному та ринковому середовищах відбуваються постійні зміни, які призводять до динаміки та значного рівня нестабільності, непередбачуваності майбутніх змін. Така нестабільність зовнішнього середовища породжує ризики та загрози, які відповідно впливають на внутрішнє середовище підприємства, дестабілізуючи діяльність чи навпаки надаючи нові можливості до розвитку. Ці процеси набувають ще більшого масштабу та динаміки під впливом глобалізаційних та інтеграційних змін, адже приєднуються фактори не лише внутрішньо ринкові, а й фактори впливу на міжнародних ринках. Ще більше ці процеси посилюються під впливом переходу до нових технологій Четвертої промислової революції та Індустрії 4.0., що радикально змінюють процеси операційної, управлінської, маркетингової та іншої діяльності, функціонування самих підприємств.

Забезпечення безпеки господарської діяльності є однією із важливих сфер застосування інноваційних цифрових технологій, адже забезпечує широкі можливості для адекватного реагування на нові ризики, загрози та

забезпечує захист підприємств на відповідному цифровому техніко-технологічному рівні.

Слід зазначити, що самі процеси цифровізації засновані на використанні інформації як основного ресурсу, який виступає змістом, наповненням всіх подальших процесів. Фінансова, кадрова, техніко-технологічна, управлінська, комерційна інформація підприємства опрацьовується у відповідному цифровому програмному забезпеченні, рухається у інформаційних системах як самого підприємства, так і в безпосередній взаємодії із контрагентами та партнерами зовнішнього середовища в мережах Інтернет, що виводить інформаційно-цифрову безпеку на перший план та водночас показує невід'ємний взаємозв'язок інформаційно-цифрової безпеки з кадровою, фінансовою, техніко-технологічною та іншими складовими економічної безпеки підприємства.

В нових цифрових умовах та реаліях забезпечення економічної безпеки підприємств потребує розбудови та налагодження ефективного функціонування системи економічної безпеки підприємства з широким активним впровадженням та використанням інноваційних цифрових технологій. Зазначимо, що масштаб такого впровадження цифрових технологій та їх використання можуть бути різним, це залежить передусім від масштабів, кількості напрямів та сфер діяльності самого підприємства та відповідно його потреб в забезпеченні економічної безпеки. Проте, сама система економічної безпеки підприємства повинна включати такі механізми і складові, які забезпечували б їй можливість адекватно реагувати на нові ризики та загрози, впроваджувати як превентивні, так і знешкоджуючі безпекові дії, активно протидіяти новим ризикам та загрозам.

В сучасному світі зростають обсяги інформації, даних, які використовуються в операційній, фінансовій, управлінській, обліковій та іншій діяльності підприємств. В умовах діджиталізації ефективного функціонування та забезпечення належного рівня економічної безпеки передусім пов'язано із можливостями використання сучасних цифрових

технологій для обробки значного обсягу інформації із забезпеченням належного рівня безпеки. Сьогодні інформація визначається як ключовий ресурс, необхідний для функціонування. Кожної миті в мережі Інтернет створюються та рухаються величезні обсяги інформації, що використовують в роботі в різних сферах та напрямках економічної діяльності. Підприємства створюють власні інформаційні системи з метою збору, отримання, опрацювання, збереження та передачі інформації, її структурування та аналізу, необхідного для здійснення діяльності. Проте, не менш важливого значення набуває забезпечення безпеки цієї інформації, інформаційних ресурсів підприємства загалом. Це актуалізує питання використання підприємствами нових цифрових технологій найпоширенішими з яких є технології великих даних (Big Data) та технології штучного інтелекту (Artificial Intelligence), що забезпечують обробку, структурування, аналіз та інші операції з інформацією. На підставі цієї обробленої інформації приймають виважені обґрунтовані управлінські рішення щодо розробки та впровадження як превентивних заходів та дій в сфері безпеки та і в усіх сферах функціонування підприємства. Використання інформації дає можливість оцінювати як поточний стан та діючі загрози, так і розробляти прогнози на майбутні періоди аналізуючи, оцінюючи потенційні ризики та загрози. Таким чином, цифрова трансформація створює нові можливості для забезпечення економічної безпеки підприємств із впровадженням цифрових технологій у бізнес-процесах функціонування підприємств. На нашу думку, така цифрова трансформація в системі економічної безпеки підприємства повинна передбачати не тільки встановлення нового обладнання, приладів, програмного забезпечення, вона має супроводжуватися фундаментальними змінами в наукових підходах, принципах управління, формуванні внутрішніх та зовнішніх комунікацій, обміну інформацією, орієнтації на інформацію та кадрові ресурси як ключові, розвитку внутрішнього корпоративного середовища. Це дасть можливість сформувати нове за якістю та змістом внутрішнє цифрове безпекове

середовище підприємства, основою та центром ядра якого є сама система економічної безпеки підприємства.

Впровадження процесів цифровізації у всіх функціональних сферах життєдіяльності підприємства, набуття працівниками нових цифрових знань та навичок, розбудова ефективних внутрішніх та зовнішніх комунікацій, реалізація бізнес-процесів перетікання, руху інформації дає можливість оптимізувати роботу, покращити результати та зменшити витрати всіх сфер функціонування: операційної, фінансової, управлінської, логістичної, збутової та безпекової діяльності та як наслідок це забезпечує зростання рівня економічної безпеки підприємства, як єдиної цілісності. На наш погляд, система економічної безпеки підприємства в нових цифрових умовах має бути повністю інтегрована в загальну систему управління, є її невід'ємною функціональною частиною, а сама безпека забезпечується завдяки забезпеченню та налагодженню ефективного функціонування всіх функціональних підсистем-складових.

Слід зазначити, що однією із умов забезпечення конкурентоспроможності та високого рівня безпеки є забезпечення відповідальності підприємства вимогам зовнішнього середовища, що швидко змінюється.

Розбудова сучасних систем економічної безпеки підприємств та їх подальше функціонування здійснюється з використанням сучасних пристроїв, ресурсів мережі Інтернет, спеціалізованого програмного забезпечення та широкого використання інших цифрових технологій. При цьому, в самій системі економічної безпеки відбувається зміщення ключової уваги із захисту матеріальних ресурсів на захист інформаційних ресурсів, оскільки через пошкодження, втрату інформаційних ресурсів можуть реалізуватися ризики матеріальних та фінансових втрат. Порушення конфіденційності, цілісності інформації як загроза здатна завдати значних збитків діяльності підприємства, завдати значних втрат репутації. Особливо це важливо для підприємств, що працюють в сфері високих технологій, здійснюють самостійні інноваційні

розробки, впроваджують інноваційні продукти, реалізують інноваційно-інвестиційні проекти та значною мірою залежать від випереджувального розвитку, фактору новизни, оскільки для них втрата, порушення, витік інформації може призвести до втрати ефективності та загальних результатів діяльності загалом.

Розбудова системи економічної безпеки підприємства розпочинається з визначення мети функціонування такої системи.

Метою розбудови системи економічної безпеки підприємства є забезпечення стабільного та ефективного функціонування підприємства, його захист від внутрішніх та зовнішніх небезпек, загроз, створення передумов для майбутнього ефективного розвитку, конкурентоспроможності на засадах широкого впровадження та використання інноваційних цифрових технологій.

Змістом цифровізації безпекової діяльності є вибір, обґрунтування та впровадження в систему економічної безпеки підприємства нових інноваційних цифрових технологій, які дають можливість забезпечити зростання ефективності роботи суб'єктів безпеки у їх можливості реалізувати мету та цілі системи економічної безпеки під впливом нових цифрових небезпек та загроз.

Цілями розбудови системи економічної безпеки підприємства на основі інноваційних цифрових технологій є:

- забезпечення стабільного та ефективного функціонування підприємства із впровадженням превентивних антикризових заходів та уникнення фінансових майнових збитків;
- захист від загроз внутрішнього та зовнішнього середовищ підприємства;
- забезпечення ефективного використання та захист майна, матеріальних та фінансових ресурсів підприємства;
- захист кадрових, інтелектуальних ресурсів підприємства та примноження знань та компетентностей працівників;

- забезпечення безпеки інформаційних, цифрових ресурсів, інформації, і в тому числі конфіденційної від втрати, порушення, несанкціонованого доступу чи розголошення, кібер-злочинності;
- створення умов, що забезпечуватимуть зростання конкурентоспроможності підприємства та його ринкових позицій;
- формування засад для адаптації до зовнішніх змін та підґрунтя забезпечення майбутнього сталого розвитку підприємства.

Ключовими етапами впровадження інноваційних цифрових технологій в системі економічної безпеки підприємства є: 1) ідентифікація визначення проблем економічної безпеки, вирішення яких потребує застосування інноваційних цифрових технологій; 2) розробка та впровадження комплексу інноваційних змін в системі безпеки з використанням сучасних інноваційних цифрових технологій; 3) розробка та реалізація програм навчання персоналу підприємства та підрозділу економічної безпеки роботі з сучасними інноваційними цифровими технологіями в сфері безпеки.

Розбудова системи економічної безпеки підприємства з використанням нових цифрових технологій повинна здійснюватися на засадах базових принципів розбудови безпекових систем та з дотриманням принципів: комплексності, цілеспрямованості, своєчасності, гнучкості, масштабності, доцільності, неперервності, законності, мобільності, взаємодії та координації, централізації управління, плановості, поєднання гласності та конфіденційності, адаптованості, компетентності.

Зазначимо, що ключовими науковими підходами, на засадах яких відбувається розбудова та функціонування СЕБ є: системний, процесний, комплексний, технологічний, ризик-орієнтований підходи, підхід з позицій синергії.

Системний підхід є базовим основоположним підходом, за яким забезпечення економічної безпеки підприємства загалом розглядається як система, що має свою структуру та складається з елементів (об'єктів, суб'єктів, функцій, принципів, механізму та ін.), що взаємопов'язані та

взаємодіють між собою завдяки встановленому взаємозв'язку. Система економічної безпеки підприємства на основі інноваційних цифрових технологій передбачає, що такий взаємозв'язок визначається не лише проектуванням структури підприємства, його підсистем та впровадженими адміністративними, організаційними, адміністративно-розпорядчими методами та їх інструментами, а й технічними цифровими методами та засобами завдяки впровадженню інтегрованим системам управління, що призводить до автоматизації та оптимізації функціонування такої системи.

Необхідність технологізації процесів у функціонуванні системи призвело до актуалізації та необхідності обґрунтування нового наукового підходу до розбудови системи економічної безпеки підприємства обґрунтованого у першому розділі цього дослідження.

Технологічний підхід є новим підходом до управління СЕБ, який розглядає систему економічної безпеки як сукупність підсистем, складових та елементів, взаємодія яких реалізується із застосуванням сучасних цифрових технологічних засобів та технологій, використання яких забезпечує ефективне функціонування механізму системи безпеки, використання методів та інструментів управління.

Процесний підхід до управління розглядає систему економічної безпеки підприємства в широкому сенсі як певну сукупність процесів, які пов'язують та забезпечують взаємодію між окремими структурними підрозділами та виконання конкретних дій, заходів в забезпеченні економічної безпеки як процеси кожен з яких має конкретного виконавця, відповідального, час виконання та визначені ресурси, необхідні для цього. При цьому, по суті, сукупність таких процесів та їх проектування дає можливість дефрагментувати всі заходи та дії щодо забезпечення економічної безпеки підприємства, визначивши їх послідовність, виконавців, час, ресурси, що дає можливість для ефективного планування та впровадження безпекових заходів. У вузькому сенсі процесний підхід розглядається як процес управління, що передбачає послідовне виконання основних управлінських функцій:

планування, організації, мотивації, координації, контролю та є основою прийняття управлінських рішень в управлінні системою економічної безпеки підприємства, яке здійснює як сам перший керівник, власник підприємства, так і керівники підрозділу (служби) економічної безпеки підприємства.

Комплексний підхід до управління системою економічної безпеки підприємства заснований на тому, що всі методи, заходи та дії спрямовані на забезпечення економічної безпеки, кожна із складових економічної безпеки та всі складові разом мають плануватися та впроваджуватися комплексно, оскільки фрагментарне одиничне впровадження дій не поєднаних з іншими не дасть ефективних результатів та не забезпечить ефективного захисту від небезпек та загроз.

Застосування ризик-орієнтованого підходу в системі економічної безпеки має значне поширення та затвердження на законодавчому рівні, оскільки Бюро економічної безпеки в 2023 р. затвердило порядок його застосування в безпекових цілях [240]. Так, відповідно до цього порядку ризик-орієнтований підхід передбачає ідентифікацію, оцінку ризиків; впровадження дій з управління ризиками; фіксацію результатів, отриманих за певні періоди; та актуалізацію інформації з питань оцінювання ризиків. Водночас, відповідно до міжнародного стандарту ISO 9001 [241] ризик-орієнтований підхід виступає стратегією управління, що дає можливість ідентифікувати, оцінити та зменшити ризики на всіх етапах впровадження бізнес-процесів у всіх функціональних сферах діяльності підприємства. Застосування ризик-орієнтованого підходу до управління системами економічної безпеки підприємства на основі цифрових технологій відкриває можливості до управління ризиками та забезпечення безпеки в процесі планування та реалізації всіх бізнес-процесів діяльності, що дає можливості до зменшення та управління ризиками, пов'язаними із цифровізацією та діджиталізацією процесів функціонування самого підприємства і є невід'ємною складовою загальної системи управління.

Підхід з позицій синергії визначає, що найбільш значний результат ефективності управління системою економічної безпеки підприємства на основі впровадження цифрових технологій може бути досягненим завдяки плануванню та впровадженню комплексних дій, які охоплюватимуть всі функціональні сфери та підсистеми в діяльності підприємства, а не лише безпекову сферу та за умови залучення, участі всіх керівників та працівників підприємства в реалізації безпекових дій та заходів. Зростання рівня економічної безпеки підприємства не може бути досягнутим лише діями фахівців служби економічної безпеки. Зазначимо, що в умовах впровадження в системі безпеки інноваційних цифрових технологій, на наш погляд, важливого значення набуває дотримання низки специфічних принципів.

Серед таких специфічних принципів слід зазначити: технологічність, відповідність сучасному цифровому технологічному рівню, пріоритету превентивних заходів, компетентності, інтегрованості, своєчасності та оперативності, сумісності та надійності. Складові та структура управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій представлено на рис. 3.1. Результати проведених у першому розділі дослідження наукових засад розбудови системи економічної безпеки підприємства дають підстави визначити ключові елементи та складові системи економічної безпеки підприємства, а саме: суб'єкти управління, об'єкти управління, функції управління, нормативно-правове, техніко-технологічне, методичне, фінансове, програмно-цифрове, кадрове забезпечення; механізм управління, методи, інструменти, технології управління, функціональні складові (підсистеми) системи економічної безпеки підприємства.

Суб'єктами системи економічної безпеки підприємства виступають внутрішні та зовнішні суб'єкти. Внутрішніми суб'єктами є: керівник, власник підприємства; фахівці підрозділу, служби економічної безпеки підприємства; спеціалісти інших структурних підрозділів, задіяні в питаннях забезпечення економічної безпеки; фахівці сфери інформаційних технологій, програмісти, технічні фахівці з впровадження нових інноваційних цифрових технологій.

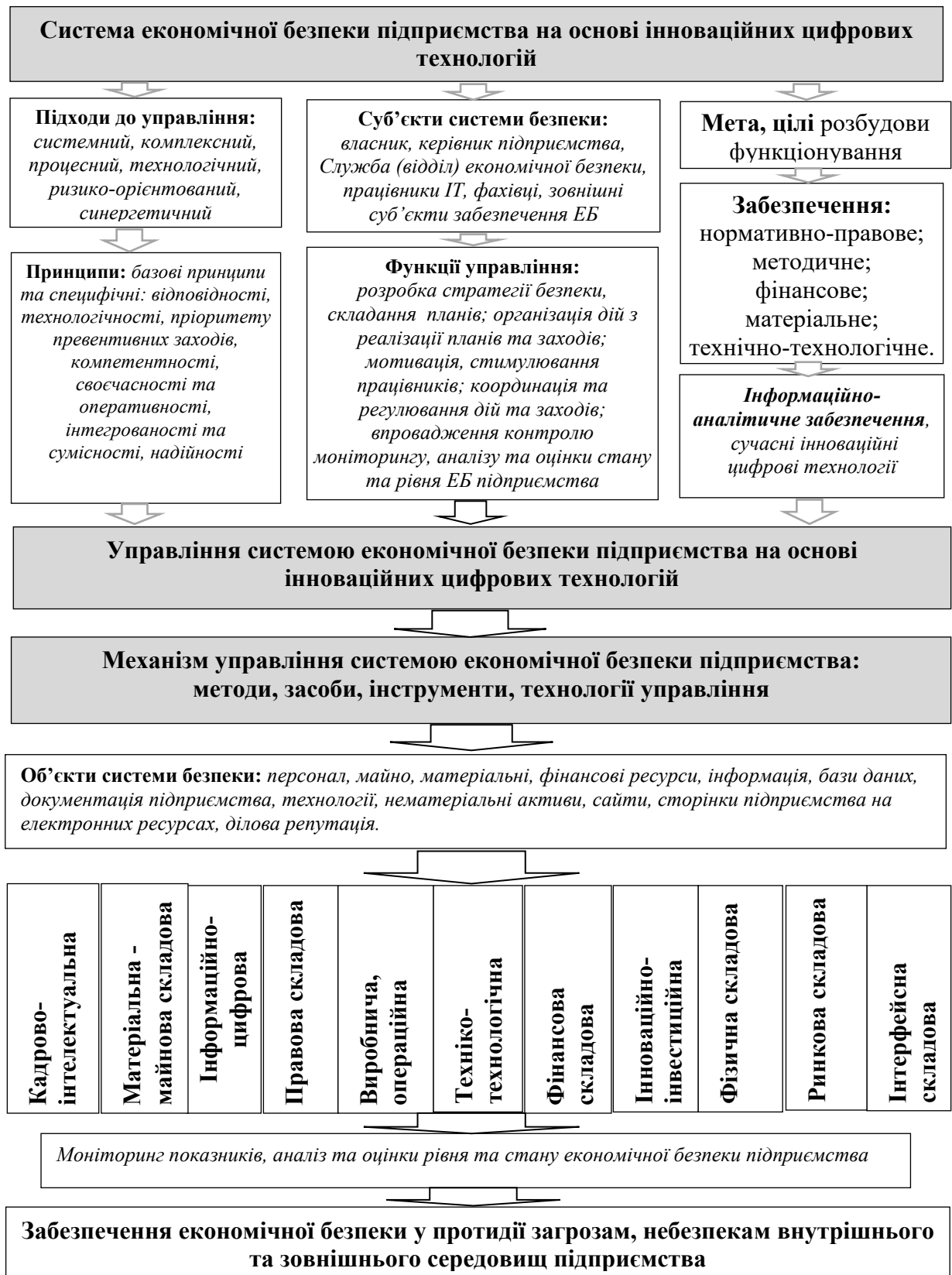


Рис. 3.1. Складові та структура управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій

Джерело: розроблено автором

Внутрішні суб'єкти входять до структури самого підприємства та безпосередньо задіяні у вирішенні питань забезпечення економічної безпеки підприємства.

До зовнішніх суб'єктів системи економічної безпеки підприємства відносяться організації, які знаходяться поза межами підприємства, проте можуть приймати участь та бути задіяними у вирішенні конкретних питань економічної безпеки, а також вирішувати проблеми та забезпечувати захист, коли забезпечення безпеки виходить за межі компетентності власних структур забезпечення економічної безпеки підприємства. До них відносять органи державної влади, законодавчі органи, що приймають закони та створюють нормативно-правове поле забезпечення безпеки на всіх її рівнях; державні, регуляторні та контролюючі органи, державний антимонопольний комітет, державну податкову службу, митні органи, прокуратуру, правоохоронні органи, органи правопорядку, суди, органи місцевого самоврядування; установи та організації, які здійснюють підготовку фахівців з економічної безпеки та науково-дослідні установи в сфері інноваційної діяльності; організації в сфері ІТ-технологій.

Об'єктами системи економічної безпеки підприємства виступають: персонал, працівники підприємства, інтелектуальні ресурси, знання та компетентності працівників; майно, матеріальні, фінансові ресурси підприємства; інформація, інформаційні ресурси, бази даних, документація підприємства, в тому числі конфіденційна інформація, що становить комерційну таємницю підприємства; нематеріальні активи, гудвіл, торгові марки, ліцензії, патенти, сайти, сторінки підприємства на електронних ресурсах, ділова репутація; техніко-технологічні ресурси, технології, програмне забезпечення; стратегія та плани діяльності із забезпечення економічної безпеки підприємства.

Безпосередніми об'єктами захисту в системі економічної безпеки підприємств із впровадженням інноваційних цифрових технологій виступають: фінансові ресурси, в тому числі капітал, фінансові ресурси

господарської діяльності, інвестиції, витрати; технології виробництва, операційної діяльності, управління, просування та збуту, забезпечення безпеки; майно та матеріальні активи, цінності підприємства; працівники підприємства; правовстановлююча документація підприємства; інформація, документи, бази даних; нематеріальні активи підприємства; екологічний стан підприємства.

Розбудова системи економічної безпеки підприємства передбачає застосування сучасних цифрових технологій, програмного забезпечення, інформації, розбудови комунікацій, спрямованих на захист кадрової, майнової, виробничої, фінансової, інформаційної та інших складових.

Загалом, впровадження інноваційних цифрових технологій в функціональних сферах безпеки дає можливість підвищити оперативність прийняття безпекових заходів та дій, ефективність в забезпеченні безпеки, впровадити автоматизований моніторинг безпекових показників, аналізувати та оцінювати отримані дані, своєчасно виявляти загрози та оперативно на них реагувати, розробляючи та впроваджуючи комплекс невідкладних заходів, планувати та впроваджувати превентивні заходи, дії.

Складовими (підсистемами) системи економічної безпеки підприємства на основі впровадження інноваційних цифрових технологій виступають: фінансова, правова, кадрова, інтелектуальна, виробничо-операційна, матеріально-майнова, техніко-технологічна, інноваційно-інвестиційна, інформаційно-цифрова, інтерфейсна, ринкова, фізична складові системи економічної безпеки.

Фінансова складова економічної безпеки підприємства визначає фінансовий стан підприємства, захищеність його фінансових активів, впровадження контролю над проведенням фінансових операцій, оптимізацію руху фінансових потоків, впровадження оцінювання фінансових результатів діяльності та здійснення фінансового обліку та управління фінансовими ризиками підприємства. Впровадження цифрових технологій, в першу чергу спеціалізованих програм в забезпеченні фінансової безпеки дає можливість

удосконалити, автоматизувати здійснення фінансового обліку та звітності, проводити фінансовий аналіз та працювати з великими масивами даних, в автоматичному режимі здійснювати операції фінансового контролю, управляти кредиторською та дебіторською заборгованістю, використовувати сучасні методи аналізу та оцінювання в управлінні фінансовими ризиками, впроваджувати автоматизований моніторинг витрат та руху фінансових потоків.

Виробнича (операційна) складова системи безпеки підприємства визначає стан виробничих баз, їх техніко-технологічне оснащення, потужності, модернізацію, ефективність виробничих процесів, їх технологічність, активність у впровадженні інновацій та можливості до відтворення вкладеного капіталу, їх безпеку, ефективність виробничої діяльності, собівартість виробництва продукції чи надання послуг, їх конкурентоспроможність в сучасних ринкових умовах та можливості до розширення операційної виробничої діяльності.

Матеріальна (майнова) складова системи економічної безпеки підприємства забезпечує захист майна та матеріальних активів, в тому числі приміщень, обладнання, сировини та матеріалів, готової продукції та інших активів, що знаходяться на балансі чи належать підприємству. Впровадження цифрових технологій в забезпеченні майнової безпеки дає можливість удосконалити, оптимізувати та автоматизувати облік та контроль за рухом матеріальних ресурсів, впровадити превентивні заходи для запобігання крадіжкам, зловживанням, псуванню майна матеріальних ресурсів, забезпечити їх збереження та ефективність використання.

Правова складова системи економічної безпеки підприємства забезпечує діяльність підприємства та прийняття управлінських рішень в межах діючого в країні нормативно-правового поля, а також передбачає юридичну, правову підтримку та безпеку в процесі розв'язання господарчих суперечок та судових розглядів, ризиків юридичної діяльності. Впровадження цифрових технологій у функціонуванні цієї складової системи економічної безпеки забезпечує

ведення електронного обігу документації та договірної діяльності, автоматизованого контролю за дотриманням термінів виконання договірних зобов'язань, налагодження систем електронного обміну документами з контрагентами та ін.

Інформаційно-цифрова складова економічної безпеки підприємства поєднує дві складові – інформаційну безпеку, що забезпечує безпеку роботи з інформацією, включає інформаційно-аналітичні методи, інструменти та цифрову безпеку впровадження та використання цифрових технологій, технічних цифрових засобів, ПЗ в роботі з інформацією. Інформаційно-цифрова безпека спрямована на захист інформації, баз даних, збереження комерційної таємниці та конфіденційної інформації. Цифрові технології, які при цьому використовують – це загальне та спеціалізоване програмне забезпечення, антивірусні програми, криптографічний захист, впровадження систем контролю доступу до інформації та інші технології і засоби, що забезпечують збереження і можливість безпечного, ефективного використання інформаційних та всіх інших ресурсів підприємства в інформаційних системах.

Інвестиційно-інноваційна складова системи економічної безпеки підприємства визначає стан впровадження, активність та безпеку інноваційних процесів в діяльності підприємства та їх інвестиційного забезпечення. Відповідно, ця складова визначає інноваційну новизну продукції, послуг підприємства, частоту та ефективність впровадження інновацій та фінансову ефективність інвестиційних проектів, реалізованих підприємством. Впровадження цифрових технологій пов'язано передусім із самим впровадженням нових інноваційних технологій в операційній виробничій діяльності підприємства, що безпосередньо і визначає інноваційну активність, здатність до відтворення та інноваційного розвитку, а також використання спеціалізованого програмного забезпечення для розробки та супроводу реалізації інноваційно-інвестиційних проектів, моніторингу показників ефективності, управління ресурсами та процесами.

Кадрова інтелектуальна складова системи економічної безпеки підприємства забезпечує збереження та примноження кадрових ресурсів, їх кількості, якості, відповідності, дотримання норм та вимог щодо безпеки роботи з інформацією та фаховості виконання своїх професійних обов'язків на підприємстві, водночас інтелектуальна складова може бути визначеною як комплекс знань, вмінь, компетентностей працівників підприємства, які вони використовують у виконанні своїх професійних обов'язків та які дають можливість забезпечувати високу якість отриманих результатів, що разом здатне забезпечити дотримання безпеки професійної діяльності та загалом сприяти зростанню рівня економічної безпеки підприємства. В сучасних умовах технологічні та кадрові інтелектуальні ресурси є одним з ключових ресурсів, які забезпечують ефективність та безпеку функціонування.

Техніко-технологічна складова системи економічної безпеки підприємства визначається рівнем технічного та технологічного забезпечення, яке має підприємство для здійснення своєї виробничої чи операційної діяльності. Це наявність та стан обладнання, технічних засобів та впровадження технологій, які використовуються підприємством у здійсненні виробничої (операційної), управлінської, логістичної, маркетингової діяльності, впровадження обліку та забезпечення економічної безпеки. Рівень техніко-технологічної безпеки передусім визначається рівнем прогресивності техніки та технологій, що використовуються та їх відповідності сучасним світовим стандартам, загальному техніко-технологічному рівню, який на даний час домінує в ринковому середовищі певної галузі, сфери економічної діяльності відповідно до найбільш нових інноваційних здобутків науково-технічного прогресу. Впровадження інноваційних цифрових технологій дає можливість автоматизувати процеси та операції, які виконуються у виробничій операційній діяльності, а їх застосування охоплює переважну більшість сучасних цифрових технологій, таких як АТМ-технології, формування кібер-фізичних систем, впровадження АСУ, «розумного виробництва», 3-D друку, робототехніки, методів та засобів автоматизованого

контролю якості та ін. Забезпечення економічної безпеки за техніко-технологічною складовою спрямоване на оптимізацію процесів та операцій в діяльності, зменшення витрат, зростання ефективності процесів виробництва (операційної діяльності), зростання конкурентоспроможності підприємства та його продукції.

Інтерфейсна складова – це складова, яка визначає безпеку формування взаємозв'язків та взаємодії між внутрішніми підрозділами, працівниками в середині підприємства та передбачає формування каналів обміну інформацією, контролю дотримання встановлених протоколів, правил та вимог безпеки в роботі з документацією, фінансовими, матеріальними та іншими ресурсами; навчання працівників та набуття ними необхідних безпекових навичок, компетентностей та взаємодію, яка відбувається між внутрішніми та зовнішніми суб'єктами, в тому числі у взаємодії з державними, податковими, правоохоронними органами, у взаємодії із контрагентами щодо перевірки їх надійності та ділової репутації, взаємодії із споживачами, ринковим середовищем щодо формування ефективних комунікацій, та взаємодії із суспільством, громадськістю з формуванням та зміцненням позитивного іміджу підприємства, поширенням позитивної інформації про підприємство та його продукцію. Впровадження цифрових технологій в управлінні цією складовою дає можливість оптимізувати, автоматизувати, забезпечити сучасний цифровий рівень обміну інформацією, дає можливість забезпечити контроль та захист-безпеку ресурсів підприємства, його конкурентоспроможності та ділової репутації.

Фізична складова СЕБП спрямована на забезпечення особистого захисту, фізичну безпеку власника, керівника та топ-менеджерів підприємства, забезпечення безпеки для працівників підприємства від протиправних дій третіх осіб та фізичних загроз, охорону та безпеку об'єктів, в тому числі з організацією охорони та пропускну режиму на територію підприємства з метою забезпечення фізичного захисту його майна, фінансових та матеріальних ресурсів, впровадження та дотримання систем контролю

доступу, навчання працівників щодо дій у випадку небезпечних, надзвичайних ситуацій; захисту майна, матеріальних цінностей та активів підприємства; захисту персоналу та дотримання безпеки охорони праці на робочих місцях; забезпечення безпеки процесів виробництва та обладнання, впровадження захисту від пожеж, аварійних та надзвичайних ситуацій; забезпечення роботи аварійно-рятувальних служб; протидії саботажам, тероризму, крадіжкам, псуванню матеріальних ресурсів, майна підприємства. Впровадження цифрових технологій в забезпеченні фізичної складової СЕБ передусім пов'язують із впровадженням систем автоматизованого відео- та аудіо-спостереження, автоматизованих систем протипожежної безпеки та охоронної сигналізації, використання сканерів, засобів автоматичного зчитування та ідентифікації об'єктів, товарів, використання штучного інтелекту, спеціалізованого програмного забезпечення для обробки інформації, розпізнавання обличч, інших технічних засобів та інше.

Ринкова складова СЕБП – це складова, орієнтована на формування та підтримання на високому рівні конкурентоспроможності підприємства та його ефективної роботи на ринку з просуванням та реалізацією продукції. Охоплює такі аспекти функціонування, як: визначення, розробка стратегії підприємства; формування ефективної конкурентоспроможної продуктової політики та політики ціноутворення; розробку та впровадження ефективної політики з просування та збуту продукції (послуг), спрямованої на зростання розширення ринків збуту та залучення і утримання нових споживачів; формування нових ефективних комунікацій з ринком, споживачами, конкурентами та партнерами; зростання конкурентоспроможності підприємства та його продукції; забезпечення формування та дотримання позитивного іміджу та ділової репутації підприємства на ринку. Забезпечення ринкової складової має важливе значення у досягненні стратегії підприємства та забезпеченні його довгострокового розвитку. Інноваційними цифровими технологіями, які впроваджують в забезпечення ринкової безпеки є створення сайтів, веб-додатків підприємства, активне використання мережі Інтернет та соціальних

мереж, використання технологій «блокчейн», технологій «хмарних обчислень», впровадження технологій електронної торгівлі з реалізацією продукції та послуг з використанням цифрових електронних платформ та інші.

Розбудова та функціонування системи економічної безпеки підприємства потребує необхідного для цього нормативно-правового, методичного, фінансового, матеріального, техніко-технологічного та інформаційно-аналітичного забезпечення.

Так, сама розбудова системи економічної безпеки здійснюється з дотриманням норм чинного законодавства, а всі рішення щодо управління приймаються в межах діючого нормативно-правового поля. Таким чином, нормативно-правове забезпечення, згідно з яким здійснюється безпекова діяльність включає прийняття державних законів, Податковий, Митний, Господарчий, Процесуальний та інші кодекси, державні нормативно-правові акти, що визначають та регулюють різні аспекти функціонування підприємства та внутрішні управлінські документи, які формують, визначають норми та встановлюють регламенти в діяльності кожного окремого підприємства.

Такими внутрішніми нормативними документами в сфері безпеки виступають розроблена та прийнята на підприємстві концепція та стратегія економічної безпеки, положення про службу економічної безпеки, плани заходів із забезпечення безпеки, накази, розпорядження, інструкції та інші документи, що визначають та регламентують діяльність підрозділу (служби) економічної безпеки підприємства. Формування цих документів відбувається поступово, проте від їх повноти та узгодженості залежить можливість визначення встановлення та регулювання внутрішніх процесів діяльності в сфері безпеки.

Методичне забезпечення системи економічної безпеки передбачає використання сучасних наукових методів, підходів, в тому числі методичні розрахунки рівня економічної безпеки держави, методики щодо роботи з інформацією та цифровими технологіями, міжнародні норми та норми і

стандарти, що регламентують питання управління та впровадження безпекових заходів, в тому числі в сфері безпеки інформаційних цифрових технологій. Також на підприємстві можуть бути прийнято власні методичні рекомендації та вимоги для працівників з питань безпеки.

Іншим видом забезпечення системи економічної безпеки є необхідне для її розбудови та функціонування фінансове забезпечення, оскільки фінансові ресурси забезпечують можливості для придбання та отримання всіх інших необхідних для функціонування ресурсів, таких як кадрові, матеріальні чи технологічні. Фінансове забезпечення має бути системним та достатнім. Система економічної безпеки підприємства, її функціонування та забезпечення в сучасних умовах цифровізації є пріоритетним напрямком в управлінні підприємством, а тому її фінансування не повинно здійснюватися за залишковим принципом. Навпаки, фінансування системи безпеки має бути передбачено як одна із основних постійних статей витрат бюджету підприємства, а кошти мають плануватися та виділятися за бюджетом на кожний наступний рік.

Матеріальне забезпечення системи економічної безпеки підприємства включає наявність, залучення та використання всіх видів матеріальних ресурсів, необхідних для її функціонування, в тому числі приміщень, обладнання, приладів, меблів, комп'ютерної й офісної техніки та інших матеріальних активів, які використовуються як загалом для функціонування підприємства, так і конкретно підрозділів економічної безпеки підприємства і забезпечують оснащення робочих місць працівників.

Кадрове забезпечення системи економічної безпеки підприємств є однією із фундаментальних задач, які підлягають вирішенню, оскільки від наявності кадрів, їх достатності, профільної освіти в сфері безпеки та в інших сферах, в тому числі в сфері інформаційних технологій, відповідності, досвіду, компетентності залежить здатність до керівництва системою економічної безпеки та її напрямками, організацією та впровадженням конкретних дій. Кадрове забезпечення системи економічної безпеки підприємства полягає не

лише в наявності необхідної кількості фахівців підрозділу економічної безпеки, а й в достатності та рівні кадрового складу інших структурних підрозділів підприємства, і в тому числі технічних працівників, фахівців інформаційних цифрових технологій, фахівців-аналітиків здатних здійснювати роботу з інформацією, цифровими ресурсами на високому професійному рівні.

Техніко-технологічне забезпечення полягає в наявності необхідного для розбудови та функціонування системи економічної безпеки технічного забезпечення, обладнання, приладів, програмного забезпечення та відповідних технологій, які необхідні для забезпечення безпеки за всіма складовими економічної безпеки та дають можливість забезпечувати її на належному сучасному високо технологічному рівні.

Інформаційно-аналітичне забезпечення загалом є невід'ємною складовою, а в умовах цифрових сучасних змін – основою для планування та забезпечення економічної безпеки підприємства за всіма складовими та напрямками діяльності. Ефективна налагоджена система інформаційно-аналітичного забезпечення в системі безпеки дає можливість збирати, опрацьовувати, вивчати, аналізувати та оцінювати великі обсяги різноманітної інформації. Використання при цьому сучасної техніки, технологій, великих масивів даних та штучного інтелекту дозволяє автоматизувати та оптимізувати роботу з інформацією та забезпечити зростання її точності та відповідності. Водночас, інформаційно-цифрове забезпечення є змістом інформаційно-цифрової складової системи економічної безпеки підприємства.

В процесі управління системою економічної безпеки підприємства керівники як суб'єкти управління застосовують загальні функції управління, такі як: функція планування, що включає розробку концепції, стратегії економічної безпеки, складання планів та безпекових заходів; функцію організації дій з реалізації розроблених планів та заходів; функції мотивації та стимулювання працівників, їх мотивування та зацікавленість в зростанні рівня безпеки діяльності підприємства та дотримання встановлених норм, порядків

та регламентів; функції координації та регулювання дій та заходів зі своєчасним та актуальним управлінням змінами в діяльності з забезпечення безпеки відповідно до змін зовнішнього та внутрішнього середовищ, виникнення та реалізації нових небезпек і загроз; функції контролю з впровадженням моніторингу, аналізу, оцінки стану та рівня ЕБ підприємства та реалізацією всіх доцільних та ефективних для конкретного підприємства форм та видів контролю за діяльністю організації та змінами, впливами зовнішніх та внутрішніх загроз та ризиків.

Управління системою економічної безпеки підприємства здійснюється завдяки механізму управління, який забезпечує фактичну реалізацію прийнятих затверджених стратегій та планів і прийнятих управлінських рішень. Таким чином, механізм управління системою економічної безпеки дає можливість реалізувати цілі та завдання безпеки завдяки застосуванню методів управління, інших ресурсів та засобів, завдяки яким реалізуються прийняті управлінські рішення.

На нашу думку, управління системою економічної безпеки на основі використання інноваційних цифрових технологій повинно здійснюватися з дотриманням групи специфічних спеціальних принципів: відповідності, технологічності, пріоритету превентивних заходів, компетентності, своєчасності та оперативності, інтегрованості та сумісності, надійності.

Принцип відповідності заснований на тому, що планування та впровадження дій заходів із забезпечення безпеки повинно відповідати реальним потребам того чи іншого підприємства відповідно до виявлених фактичних та потенційних небезпек і загроз зовнішнього та внутрішнього середовищ, які можуть негативно впливати на його функціонування. Таким чином, незважаючи на сукупність алгоритмів, дій та складових самої системи кожне підприємство має свій унікальний набір дій та заходів із забезпечення безпеки, найбільш спрямований на вирішення саме його проблем та убезпечення від загроз, характерних саме для діяльності такого конкретного підприємства в залежності від його масштабів, технологічності, видів та

напрямів економічної діяльності, етапів життєвого циклу на йому знаходиться те чи інше підприємство, агресивності та конкурентоспроможності зовнішнього ринкового середовища та інших факторів.

Принцип технологічності характерний для забезпечення безпеки підприємств на основі впровадження інноваційних цифрових технологій та здатний відповідати на вимоги сучасності, розвитку науково-технічного прогресу у всіх сферах функціонування та того впливу, що цей науково-технічний прогрес здійснює на саме функціонування підприємства, виступаючи джерелом впливу та дії нових цифрових кібер-загроз інформаційно-цифрового середовища. Як і сам технологічний підхід принцип технологічності полягає в необхідності обрати та застосувати саме ті технічні засоби та технології, які найкращим чином відповідають потребам підприємства та здатні протидіяти загрозам та ризикам, характерним саме для конкретного підприємства, згідно з рівнем як його власної технологічності, так і залежності від технологічності галузі, сфери економічної діяльності, до якої приналежне підприємство та вимогам технологічності, які висуваються до його продукції, послуг.

Принцип пріоритету превентивних заходів полягає у доцільності проведення аналізу та оцінювання небезпек та загроз та формування, планування комплексу заходів, спрямованих на попередження настання реалізації загроз та завдання підприємству шкоди та збитків. Превентивність та попередження здатні дати значно кращі результати, ніж констатація фактів реалізації загроз та боротьба з їх негативними наслідками, а тому превентивність має бути основою дій системи економічної безпеки підприємства, яка активно використовує інноваційні цифрові технології, оскільки саме ці технології дають нові можливості для своєчасного виявлення загроз та впровадження превентивних заходів.

Принцип компетентності визначає важливість знань та вмінь, сформованих загальних та спеціальних компетентностей працівників підрозділу з економічної безпеки та всіх його структурних складових,

секторів, в тому числі компетентностей юристів, фахівців інформаційно-аналітичного забезпечення та ІТ технологій, компетентностей фахівців, які безпосередньо працюють із впровадженням та використанням на підприємстві інформаційно-цифрових технологій та фахівців, що забезпечують інформаційно-цифрову безпеку в діяльності підприємства як одну із ключових в системі безпеки сучасного підприємства. Водночас, компетентність фахівців в сучасних цифрових технологіях потрібно постійно удосконалювати, розвивати з проходженням фахівцями необхідних курсів, тренінгів підвищення кваліфікації, впровадження групового, індивідуального та самонавчання. Також, основою продуктивної ефективної роботи та належного забезпечення безпеки всього підприємства є досягнення та підтримка необхідного рівня цифрової грамотності, загальних цифрових компетентностей всього персоналу підприємства.

Принцип своєчасності та оперативності, полягає у необхідності своєчасного виявлення потенційних, фактичних небезпек та загроз, розробки та впровадження попереджувальних превентивних заходів на їх усунення, уникнення. При цьому, важливим є саме своєчасність виявлення небезпек, загроз та ризиків до того, як вони почнуть реалізуватися та здійснювати негативний вплив на діяльність підприємства. Водночас, загрози можуть з'являтися та впливати раптово та швидко і від підприємства очікується така ж швидкість, оперативність у вирішенні задач протидії небезпекам та загрозам.

Принцип інтегрованості та сумісності полягає у необхідності впровадження та дотримання протоколів відповідності технічних засобів, програмного забезпечення, технологій які використовуються підприємством загалом та системою економічної безпеки підприємства зокрема, тим стандартам та вимогам, які висуваються до інформації, документації, комунікацій в сучасних інформаційних системах. Це даватиме можливість для ефективного інтегрування підприємства, його безпекової системи та інформаційних систем, присутніх на відповідних ринках та дасть можливість

ефективно і безпечно комунікувати, здійснювати безпечний контрольований обмін інформацією та даними з партнерами стейкхолдерами, державними органами та структурами на належному сучасному техніко-технологічному рівні.

Дотримання принципу надійності означає, що розбудова та функціонування системи економічної безпеки підприємства, її складових, планування та впровадження безпекових заходів повинні забезпечувати належний рівень захисту підприємства, надійність його інформаційної та безпекової підсистем, здатність відбивати небезпеки та загрози зовнішнього середовища. Таким чином, забезпечуватиметься надійність всієї системи, її можливість забезпечувати ефективне функціонування, стабільність у протидії впливу кризових явищ.

Узагальнюючи, зазначимо необхідність розбудови та управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій, метою та цілями функціонування якої є забезпечення стабільного та ефективного функціонування підприємства, його захист від внутрішніх і зовнішніх небезпек та загроз, створення передумов для майбутнього ефективного розвитку та конкурентоспроможності, яка будується на основі застосування системного, комплексного, процесного, технологічного, ризик-орієнтованого, синергетичного, наукових підходів, з дотриманням загальних та специфічних принципів, та необхідного для розвитку і функціонування системи нормативно-правового, методичного, фінансового, матеріального, технічно-технологічного, інформаційно-аналітичного забезпечення, сучасних інформаційно-цифрових технологій, наявність та застосування яких дають можливість здійснювати вплив суб'єктів управління СЕБ та об'єкти управління, використовуючи функції управління та передбачені механізмом управління СЕБ методи, засоби та технології управління. Все це разом дає можливість здійснювати системний, ефективний вплив на об'єкти управління, в тому числі персонал, майно, матеріальні, фінансові ресурси, інформацію, бази даних, документацію підприємства,

технології, нематеріальні активи, сайти, сторінки підприємства на електронних ресурсах, ділову репутацію, що формують зміст складових підсистем системи економічної безпеки підприємства, таких як кадрова, інтелектуальна, майнова, матеріальна, правова, інформаційно-цифрова, фінансова, інноваційно-інвестиційна, техніко-технологічна, інтерфейсна, фізична, ринкова, що дає можливість забезпечувати стабільність, належний рівень економічної безпеки підприємства та забезпечувати його захист від внутрішніх та зовнішніх небезпек та загроз на належному сучасному техніко-технологічному рівні.

3.2. Розробка стратегії управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій

Управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій передбачає розробку та затвердження на підприємстві стратегії впровадження інноваційних цифрових технологій, інструментів, методів, програмного забезпечення з метою захисту підприємства, всіх його ресурсів, персоналу, майна, інформації, активів від небезпек та загроз внутрішнього та зовнішнього середовищ, що змінюються. Розробка та прийняття такої стратегії, по суті, визначає цифровізацію безпекової діяльності підприємства, яка здійснюється у взаємозв'язку та взаємозалежності з цифровізацією загалом, управлінської, операційної, збутової та іншої діяльності підприємства, всіх процесів його функціонування. Реалізація стратегії та впровадження такої цифровізації забезпечує можливості до розвитку, зростання стійкості, конкурентоспроможності та можливості протидіяти ризикам та загрозам діяльності підприємства.

Метою розробки та реалізації стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є цифровізація всіх процесів безпекової діяльності

підприємства, забезпечення високого рівня його захисту від небезпек та загроз зовнішнього та внутрішнього середовищ, зростання його стійкості, ефективності, діяльності та забезпечення майбутнього розвитку.

Цілями стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є: цифровізація та удосконалення інформаційно-аналітичного забезпечення, комунікацій підприємства; автоматизація та цифровізація бізнес-процесів у всіх сферах діяльності; навчання та розвиток персоналу, здобуття цифрових компетентностей; забезпечення безпеки розробки та впровадження нових інноваційних технологій; впровадження цифрових технологій в забезпеченні фізичної безпеки, захисту об'єктів; впровадження систем контролю та моніторингу системи економічної безпеки, управління ризиками діяльності.

Розробка та впровадження стратегії передбачає визначення затвердження та подальшу реалізацію дій за ключовими напрямками забезпечення безпеки; визначення стратегічних цілей за кожним з напрямків та визначення в межах кожної стратегічної цілі – оперативних цілей. Стратегічні цілі спрямовані на забезпечення довгострокової діяльності та розвитку, оперативні цілі передбачають конкретні дії та задачі, які повинні бути виконаними задля досягнення кожної із визначених стратегічних цілей, конкретизують їх та є основою для здійснення подальшого тактичного планування.

Інформаційна цифрова діяльність підприємства, впровадження сучасних інноваційних технологій на підприємствах можливе за умови наявності відповідної комп'ютерної техніки, оснащення підприємства та робочих місць працівників. Така загальна комп'ютеризація формує технічне підґрунтя, основу, необхідні фізичні та технічні можливості для подальшого впровадження та використання будь-яких нових технологій. Іншою важливою основою подальшої цифровізації є наявність та підключення до мереж Інтернет належної потужності та безперебійний доступ до Інтернет мереж, як основного джерела отримання та передачі інформації та основного

комунікаційного каналу з зовнішніми інформаційними системами, інформаційним середовищем. Відповідно до цього, першим напрямом, який на наш погляд повинен бути реалізованим в розробленій стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є інформаційно-цифровий напрям, що включає стратегічні цілі, пов'язані із загальною цифровізацією та цілі за конкретними напрямками безпекової діяльності. Водночас, кожна із стратегічних цілей має оперативні цілі, що включають перелік дій, що мають бути виконаними для їх фактичної реалізації.

Першою стратегічною ціллю інформаційно-цифрового напрямку стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є загальна цифровізація робочих місць. Цифровізація робочих місць здійснюється з метою оснащення кожного робочого місця працівника необхідною для виконання його професійних обов'язків та функцій згідно із його посадою комп'ютерною технікою, необхідною для його роботи оргтехнікою, доступом до мереж Інтернет, загальним та спеціалізованим програмним забезпеченням, необхідним для виконання його функцій та задач. Відповідно, в результаті реалізації цієї цілі всі працівники функціональних підрозділів, в чій обов'язки входить робота з комп'ютерною технікою, на своїх робочих місцях будуть мати все необхідне обладнання та технології для виконання робіт на відповідному сучасному техніко-технологічному рівні. Оперативними цілями, які будуть реалізовуватися з метою виконання цієї стратегічної цілі є визначення обсягів відповідної техніки, обладнання є придбання, установка та виконання всіх інших конкретних заходів та робіт необхідних для реалізації цієї стратегічної цілі.

Другою ціллю інформаційно-цифрового напрямку є розбудова та забезпечення безпеки внутрішніх цифрових комунікацій. Реалізація цієї цілі передбачає виконання оперативних цілей, що включають розбудову внутрішньої інтегрованої інформаційної системи підприємства, впровадження

відповідного програмного забезпечення, антивірусних програм, встановлення фільтрів та інших технічних засобів, здатних убезпечити внутрішні інформаційні ресурси підприємства, внутрішні бази даних, інформацію від несанкціонованого доступу, вилучення, зміни, знищення та інших впливів, здатних завдати шкоду та збитки інформаційним ресурсам та операційним управлінським системам підприємства, інформації. Реалізація цих оперативних цілей дасть можливість реалізувати стратегічну ціль та розбудувати внутрішню інформаційну систему підприємства, налагодити та забезпечити внутрішнє, безпечне використання інформаційних, цифрових ресурсів.

Третьою стратегічною ціллю інформаційно-цифрового напрямку є цифровізація процесів прийняття управлінських рішень, спрямована на впровадження цифрових технологій, оптимізацію зростання ефективності управлінських рішень які приймаються керівниками підприємства на всіх рівнях та значною мірою впливають на стан та рівень економічної безпеки підприємства. Оперативними цілями, які визначають та мають бути реалізованими задля досягнень цієї стратегічної цілі, є: впровадження та застосування технологій аналізу великих даних з метою виявлення потенційних та фактичних небезпек і загроз та прийняття виважених, обґрунтованих управлінських рішень на всіх рівнях управління та за всіма напрямками діяльності; впровадження автоматизованих інформаційних систем для збору та аналізу інформації, проведення фінансово-економічного аналізу та отримання його результатів з метою виявлення та контролю фактичного фінансово-економічного стану підприємства, що виступає основою для розуміння наявного потенціалу підприємства, його стану та його фактичних можливостей; управління ризиками діяльності підприємства та прийняття відповідних управлінських рішень із врахуванням виявлених потенційних та діючих ризиків.

Четвертою стратегічною ціллю інформаційно-цифрового напрямку є удосконалення інформаційно-аналітичного забезпечення. За сучасних умов

інформаційно-аналітичне забезпечення загалом виступає основою функціонування як самої системи економічної безпеки, так і підрозділу служби економічної безпеки та виконання її працівниками своїх обов'язків на високому, ефективному рівні. Оперативними цілями, які пропонуються для реалізації зазначеної стратегічної цілі, є: впровадження нових технологій для збору та аналізу інформації з метою виявлення тенденцій, закономірностей, потенційних ризиків, загроз; впровадження роботи з великими даними з метою збору, обробки, аналізу, оцінювання інформації; застосування сучасних методів, інструментів для аналізу та оцінювання інформації, що забезпечує можливості для впровадження моніторингу, стану та рівня економічної безпеки підприємства та виступає основою для планування подальших дій та заходів із забезпечення економічної безпеки, дає можливості своєчасно та адекватно виявити загрози, небезпеки, ризики та впроваджувати превентивні дії, впливаючи на подальший розвиток подій, що дає можливість мінімізувати негативний вплив ризикових явищ, небезпек, загроз, забезпечити зростання рівня економічної безпеки та захисту підприємства.

П'ятою стратегічною ціллю стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є захист інформаційних цифрових ресурсів, оскільки зі зростанням рівня цифровізації зростає сам рівень небезпек та загроз цифрового середовища, пов'язаний із активністю та руйнівним впливом кібератак, поширенням вірусних програм, впливом який намагаються здійснювати зловмисники, використовуючи цифрові інформаційні мережі на діяльність підприємств, їх фінансові та матеріальні активи, інформаційні ресурси. Внаслідок цього, захист інформаційних ресурсів є однією із ключових стратегічних цілей, що забезпечує безпеку діяльності із впровадженням інформаційних цифрових технологій загалом. Оперативними цілями, які повинні бути передбаченими для реалізації цієї стратегічної цілі, є: впровадження систем захисту інформації, кібербезпеки; впровадження контролю доступу до інформації, баз даних для працівників підприємства та

зовнішнього доступу; визначення та персоналізація інтерфейсів користувачів, працівників підприємства з розмежуванням їх доступу до тієї чи іншої інформації та впровадженням індивідуальних персоніфікованих паролів доступу до інформаційних систем, що здатне забезпечувати контроль та безпеку роботи з інформацією; встановлення антивірусного програмного забезпечення, здатного надати захист інформації та баз даних підприємства від зловісних програм та вірусів; визначення переліку працівників, що мають право на доступ до тієї чи іншої комерційної конфіденційної інформації підприємства, обмеження та забезпечення її захисту від несанкціонованого впливу; застосування інших технічних програмних засобів захисту від несанкціонованого доступу, вилучення чи використання інформації.

Шостою стратегічною ціллю інформаційно-цифрового напрямку є цифровізація документообігу підприємства. Перехід з паперового формату на електронний документообіг підприємства є однією із важливих складових впровадження цифровізації діяльності, оскільки відповідає вимогам часу та дає можливість до відповідної електронної взаємодії з партнерами, покупцями, замовниками, постачальниками, державними органами та структурами, що здатне суттєво покращити процеси взаємодії, обміну інформацією, підготовки, отримання, передачі інформації та зменшити витрати, пов'язані із веденням документації, зменшити ризики, підвищити безпеку взаємодії із партнерами. Впровадження цієї стратегічної цілі включає реалізацію оперативних цілей, таких як: впровадження програмного забезпечення, необхідного для переходу на цифрові формати документації; оцифрування документації підприємства, розробку та встановлення шаблонів документації; навчання персоналу роботі з електронними документами та системами електронного обміну інформацією: впровадження захисту безпеки цифрової документації, її архівування, збереження конфіденційності. Реалізація цих вище зазначених оперативних цілей дасть можливість забезпечити зростання ефективності роботи з документами, їх надійність, безпеку, зменшити витрати ресурсів, необхідних для здійснення

документообігу, стандартизує та уніфікує документообіг, приведення документації у відповідність до єдиних норм та стандартів, підвищить рівень їх правової відповідності вимогам безпеки.

Сьомою стратегічною ціллю інформаційно-цифрового напрямку стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є цифровізація облікових функцій підприємства, які здійснюють працівники бухгалтерії чи фінансово-економічного відділів. Здійснення бухгалтерського обліку є вимогами норм чинного законодавства, норм податкового та митного кодексів, стандартів бухгалтерського обліку, оскільки в результаті такого обліку визначають обсяги податків та зборів, що мають бути сплаченими підприємством до відповідних фондів та державного і місцевих бюджетів. Відповідність ведення бухгалтерського обліку є процесом підзвітним та жорстко нормованим, порушення ведення такого обліку, відповідності нарахування податків та зборів чи несвоєчасного подання відповідних звітів є грубим порушенням нормативних норм та вимог і призводить до значних небезпеки та загроз в діяльності підприємства, перевірок, нарахування штрафних санкцій, завдання підприємствам значних фінансових та репутаційних збитків. Не менш важливого значення в діяльності та безпеці підприємства має впровадження складського обліку з використанням відповідно програмних продуктів, систем та його інтеграції з іншими системами, в тому числі із загальною програмою бухгалтерського обліку. Це пов'язано із тим, що на складах зберігають матеріальні ресурси, цінності підприємства, що підлягають обліку, контролю та захисту. Впровадження електронного обліку на складах забезпечує зростання рівня безпеки, збереження цих матеріальних ресурсів, їх точності та відповідності.

Реалізація цієї важливої стратегічної цілі забезпечується з виконанням операційних цілей: впровадження сучасного програмного забезпечення, здійснення бухгалтерського, управлінського обліку та інше; навчання персоналу роботі з цим програмним забезпеченням; перехід відповідних

підрозділів підприємства на ведення електронного обліку; перехід на подачу звітності використовують електронні формати та системи.

Наступним стратегічним напрямом стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є напрям автоматизації, оптимізації бізнес-процесів, який охоплює впровадження сучасних цифрових технологій, приладів, обладнання та програмного забезпечення з метою автоматичного і оптимального виконання процесів та операцій у всіх сферах функціональної діяльності підприємства, що дає можливість уніфікувати та стандартизувати всі процеси та операції, що виконуються, зменшити їх тривалість, збільшити кількість – продуктивність роботи і при цьому забезпечити уніфікованість, типовість виконання робіт та забезпечити зростання якості виконання робіт. Забезпечення отримання результатів за цим напрямом передбачає реалізацію низки стратегічних цілей.

Стратегічною ціллю напрямку автоматизації, оптимізації бізнес-процесів є безпосередньо автоматизація, оптимізація бізнес-процесів, безпекової діяльності. Оперативними цілями, завдяки яким реалізується ця стратегічна ціль, є: впровадження спеціалізованого програмного забезпечення, здатного забезпечити автоматизацію процесів безпекової діяльності підприємства, що дає можливості для мінімізації людського фактору у виконанні процесів та операцій, зменшує кількість помилок, що можуть допускатися в роботі; використання цифрових платформ та програмного забезпечення для аналізу та оцінювання ризиків, пов'язаних із шахрайськими діями, порушеннями, помилками в роботі.

Наступною стратегічною ціллю другого напрямку є автоматизація, оптимізація бізнес-процесів маркетингової, комерційної діяльності підприємства. Слід зазначити, що автоматизація, оптимізація бізнес-процесів маркетингової, комерційної діяльності підприємства має принципово важливе значення для результатів його роботи загалом, прибутковості, стійкості, конкурентоспроможності, дає можливість до ефективної роботи на ринку та

подальшого розвитку. Це пов'язано із появою та дією нових напрямів просування та збуту продукції, а саме широкого використання цифрових електронних платформ як на внутрішньому ринку країни, так і на міжнародних ринках, активним використанням споживачами електронних гаджетів та мереж Інтернет для замовлення, придбання продукції, послуг та активним використанням сучасних цифрових платформ для обміну інформації просування чи придбання продукції та послуг юридичними особами. Все це разом визначає по суті перехід ринків продукції та послуг в електронне цифрове середовище. Сьогодні, умовою ефективного збуту продукції та послуг підприємства є сама його присутність в мережі Інтернет, на платформах, порталах для просування та збуту продукції, соціальних мережах. Враховуючи обсяги та трудомісткість операцій, пов'язаних із опрацюванням запитів та наданням необхідної інформації клієнтам та споживачам, опрацювати такий обсяг робіт традиційним залученням та використанням кадрових ресурсів по суті неможливо. Саме тому, процеси автоматизації та оптимізації бізнес-процесів, комерційної діяльності невід'ємно пов'язані з необхідністю активного впровадження та використання штучного інтелекту, технології «блокчейн», спеціалізованого програмного забезпечення для роботи з великими базами даних, спеціалізованого програмного забезпечення для роботи з цифровими електронними платформами та іншими цифровими інноваціями. Оперативними цілями, які необхідно реалізувати для досягнення цієї стратегічної мети, слід визначити: впровадження техніко-технологічних засобів, обладнання, програмного забезпечення необхідного для автоматизації, оптимізації бізнес-процесів; створення та просування сайту підприємства; створення та просування мобільних додатків для роботи зі споживачами; навчання персоналу роботам з відповідними цифровими технологіями, інформаційними ресурсами; впровадження CRM (Customer Relationship Management) систем, які забезпечують автоматизоване ведення клієнтської бази управління маркетинговими операціями та обслуговуванням споживачів; проектування та впровадження автоматизації бізнес-процесів

маркетингової, комерційної діяльності; впровадження автоматизованих процесів контролю безпеки маркетингової, комерційної діяльності підприємства на цифрових електронних ресурсах.

Третьою стратегічною ціллю другого напрямку є автоматизація, оптимізація бізнес-процесів логістичної діяльності, управління операціями в ланцюгах поставок. Слід зазначити, що здійснення логістичної діяльності, визначення обсягів та графіків поставок, управління переміщенням товарів та матеріальних цінностей, управління запасами є тими задачами, які на сьогоднішній день успішно виконують завдяки впровадженню інноваційних цифрових технологій, які дають можливість оптимізувати, автоматизувати бізнес-процеси здійснення логістичної діяльності.

Оперативними цілями, які при цьому доцільно застосовувати для проведення такої оптимізації, є: впровадження ERP (Enterprise Resource Planning) систем, які забезпечуватимуть комплексне управління всіма видами ресурсів; впровадження цифрових електронних систем ідентифікації та обліку товарів на складах; застосування цифрових рішень програмного забезпечення, цифрових платформ для оптимізації процесів управління ланцюгами поставок, що забезпечує можливості до більш ефективного планування та управління матеріальними ресурсами та самими процесами логістичної діяльності як на внутрішньому, так і на міжнародному ринках.

Загалом, реалізація стратегічних цілей другого напрямку здатна зменшити витрати, збитки та ризики, пов'язані з людським фактором у виконанні процесів та операцій, забезпечити їх продуктивність, уніфікованість, якість, обсяги виконання та безпеку.

Третім напрямом стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є кадровий напрям, спрямований на навчання та розвиток персоналу. Стратегічною ціллю цього напрямку є впровадження навчання, здобуття цифрових компетентностей та подальший розвиток працівників. Необхідність впровадження цього напрямку обумовлена тим, що будь-яке впровадження

технічних засобів нових технологій, програмного забезпечення та інших інформаційних, цифрових чи технічних ресурсів потребує працівників, що мають знання та навички для використання цих передових технологій. Від наявності та відповідності цих знань та навичок значною мірою залежить результат використання цих нових технологій, а також безпека самих процесів використання, оскільки невміння чи незнання можуть привести до помилок під час використання та експлуатації. Саме тому важливими оперативними цілями, необхідними для реалізації цієї стратегічної цілі виступають: підбір на роботу працівників, що за своєю освітою, фахом, досвідом відповідають профілю професії та вимогам до кандидатів; впровадження програм навчання працівників щодо формування цифрових навичок та компетентностей; планування та реалізація програм професійного розвитку персоналу; управління знаннями, накопичення, розвиток знань працівників, необхідних для ефективної діяльності з забезпечення безпеки з використанням цифрових технологій; проведення навчальних тренінгів для використання цифрових інструментів, розпізнавання загроз та дій у цих випадках; проведення з працівниками інструктажів щодо дій та реагування у випадку надзвичайних ситуацій, реалізації загроз.

Четвертим напрямом стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є забезпечення безпеки інноваційної діяльності підприємства. Слід зазначити, що саме використання інноваційних цифрових технологій спрямоване на зростання ефективності функціонування системи економічної безпеки підприємства і передбачає, що підприємство буде здійснювати інноваційну діяльність, впроваджувати інноваційні продукти та процеси. Водночас, якщо підприємство високотехнологічне та працює в сфері ІТ чи інших високотехнологічних сферах, воно водночас може створювати інновації, нові розробки, технології. Відповідно, необхідно буде впроваджувати процеси забезпечення безпеки цих інноваційних розробок та технологій, що матиме ключове значення для ефективної діяльності

підприємства загалом. Відповідно, такі підприємства потребуватимуть захисту їх інноваційних розробок, інтелектуальних нематеріальних активів від дій кіберзлочинності, конкурентної розвідки чи несумлінних конкурентів. Стратегічною ціллю цього напрямку є розробка та впровадження нових інноваційних технологій. Оперативними цілями, що забезпечуватимуть можливість реалізації цієї стратегічної цілі, слід зазначити: захист комерційної таємниці інноваційних розробок підприємства від несанкціонованого доступу, витоку, розголошення; захист науково-технічної інноваційної інформації, розробок від дій конкурентної розвідки; захист патентів та ліцензій на розробки інших нематеріальних активів підприємств від нанесення збитків внаслідок порушення авторських прав, копіювання, підробок. Наступною стратегічною ціллю напряму безпеки інноваційної діяльності є управління ризиками інвестиційно-інноваційної діяльності та реалізації проектів підприємства. Це пов'язано із тим, що під час розробки та реалізації інноваційно-інвестиційних проектів зростають ризики та необхідним є їх прогнозування, виявлення та розробка заходів щодо управління ризиками. Відповідно, оперативними цілями реалізації цієї стратегічної цілі, є: прогнозування ризиків інноваційно-інвестиційних проектів; аналіз та оцінювання ризиків з використання сучасних методів та спеціалізованого програмного забезпечення; проведення експертизи відповідності розрахунків проектів та можливості їх реалізації; розробка комплексу заходів щодо управління ризиками проектів та інші. Реалізація цих стратегічних цілей спрямована на забезпечення інноваційно-інвестиційної складової системи економічної безпеки підприємства та передбачає, у тому числі, укладання з працівниками договорів про нерозголошення конфіденційної інформації про інноваційну діяльність підприємства, створення систем внутрішнього контролю та інших заходів.

П'ятим напрямом стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є впровадження цифрових технологій в забезпеченні безпеки об'єктів.

Стратегічною ціллю цього напрямку виступає впровадження цифрових технологій в забезпеченні фізичної безпеки, захисту об'єктів. Необхідність розробки дій та заходів за цим стратегічним напрямом обумовлена тим, що система економічної безпеки підприємства має значну кількість об'єктів, які підлягають захисту та забезпеченню безпеки – це працівники підприємства, його матеріальні та нематеріальні активи, власники підприємства, його інформація, розробки, ділова репутація та інші об'єкти, які потребують фізичного захисту та забезпечення безпеки. Впровадження інноваційних цифрових технологій здатне покращувати, удосконалити та оптимізувати процеси впровадження такого захисту, забезпечити зростання його надійності та ефективності. Водночас, цифровізація актуалізує появу нових об'єктів які потребують захисту, передусім інформації, самих технологій та інновацій, створених та набутих підприємством. Оперативними цілями для реалізації цього напрямку є: забезпечення безпеки на об'єктах виробництва, в операційній діяльності підприємства; технологічне забезпечення охорони та безпеки підприємства із впровадженням систем відео-нагляду, пожежної охорони та охорони сигналізаційних систем, впровадженням контролю доступу із застосуванням технічних засобів та сучасних технологій; розробка та затвердження планів та інструкцій, алгоритмів дій на випадок надзвичайних аварійних ситуацій; проведення інструктажів та навчання працівників щодо фізичного захисту та забезпечення безпеки об'єктів. Реалізація цих стратегічних та оперативних цілей спрямована на забезпечення фізичної складової системи економічної безпеки підприємства.

Шостим напрямом стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є впровадження контролю та моніторингу управління ризиками. Стратегування за цим напрямом передбачає реалізацію трьох стратегічних цілей.

На рисунку 3.2. представлено Стратегію управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

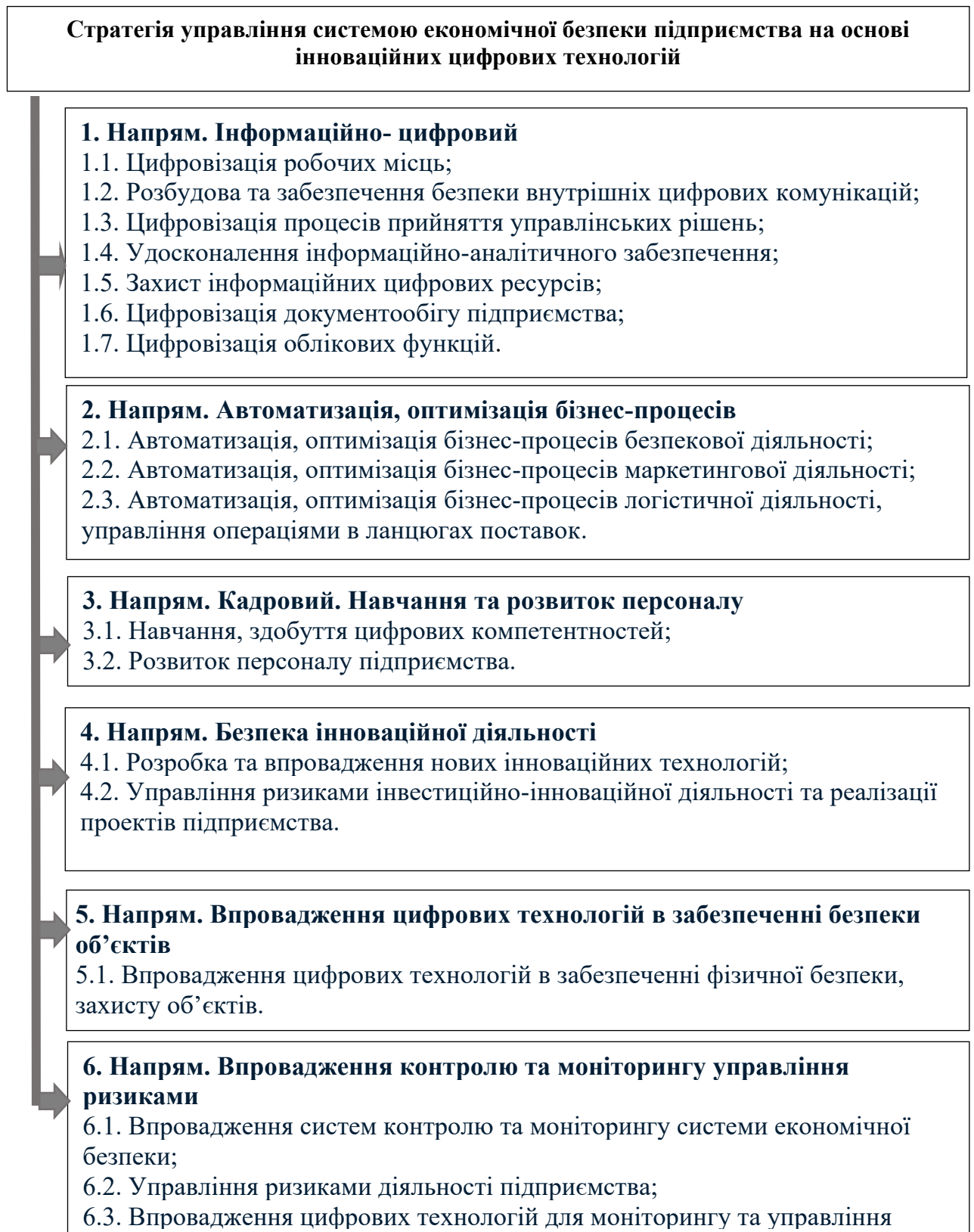


Рис. 3.2. Стратегія управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій

Джерело: сформовано автором

Впровадження систем контролю та моніторингу системи економічної безпеки є першою стратегічною ціллю цього напрямку, для реалізації якої передбачено розробку та реалізацію таких операційних цілей, як: визначення показників-індикаторів та методики, моделі для аналізу та оцінювання ризиків підприємства; впровадження системи моніторингу за станом та рівнем економічної безпеки підприємства; проведення аналізу та оцінки стану та рівня економічної безпеки, підготовка висновків; впровадження систем та комбінування різних видів контролю в управлінні системою економічної безпеки підприємства; застосування цифрових технологій для впровадження моніторингу небезпек у роботі з інформацією в цифровому середовищі, кібератак, витоку та втрати інформації.

Наступною стратегічною ціллю цього напрямку є загальне управління ризиками діяльності підприємства. Оперативними цілями що доцільно реалізувати з метою досягнення зазначеної стратегічної цілі, є: впровадження інформаційних цифрових технологій для моніторингу фінансових ризиків підприємства; впровадження технологій для управління ризиками операційної, виробничої діяльності, в тому числі відповідності обладнання, стану дотримання технологічного процесу та ін.; використання інноваційних технологій з метою управління ризиками безпеки матеріальних ресурсів та активів, в тому числі при їх збереженні на складах, переміщенні, реалізації та ін.; використання цифрових технологій в забезпеченні безпеки реалізації інноваційно-інвестиційних проектів, моніторингу інвестиційних ризиків.

Наступною стратегічною ціллю за напрямом впровадження контролю та моніторингу управління ризиками є впровадження цифрових технологій для моніторингу та управління репутацією підприємства. З метою досягнення цієї стратегічної цілі доцільним є реалізація таких оперативних цілей, як: застосування цифрових технологій для проведення моніторингу ЗМІ, соціальних мереж та інших інформаційних ресурсів з метою виявлення інформації, відгуків, коментарів, що можуть негативно вплинути на ділову репутацію підприємства; впровадження заходів спрямованих на нейтралізацію

негативного впливу цієї інформації на імідж та ділову репутацію підприємства; планування та впровадження заходів на поширення інформації, що може сприяти зростанню ділової репутації, відомості підприємства, довіри до нього та його продукції серед споживачів, партнерів, суспільства.

Реалізація стратегічних цілей за напрямом впровадження контролю та моніторингу управління ризиками має важливе значення для реалізації всієї стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій та ефективності функціонування системи та механізму управління економічною безпекою, оскільки забезпечує можливості для контролю стану та якості роботи всієї системи, результатів впровадження стратегічних цілей, планів, заходів і відповідно за результатами проведеного аналізу та оцінювання дає можливість внести своєчасні адекватні зміни, адаптуватися до зміни впливу зовнішнього та внутрішнього середовищ та ефективно протидіяти новим ризикам та загрозам, що виникають в діяльності підприємства в умовах цифрових технологій та високого рівня невизначеності.

Ключові інноваційні цифрові технології, що використовуються в розбудові та функціонуванні системи управління економічною безпекою підприємства, включають: Системи управління інформаційною безпекою (ISMS); Штучний інтелект (ШІ); Інтернет речей (IoT) та цифрові платформи; системи аналізу великих даних (Big Data Analytics); системи роботизованої автоматизації процесів (RPA); технології Блокчейн; системи виявлення вторгнень (IDS/IPS) та інші передові інноваційні цифрові технології.

Розробка та реалізація Стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є процесом комплексним, який передбачає виконання певного алгоритму дій, етапів планування та реалізації відповідних дій та заходів за основними етапами впровадження стратегії (рис. 3.3).

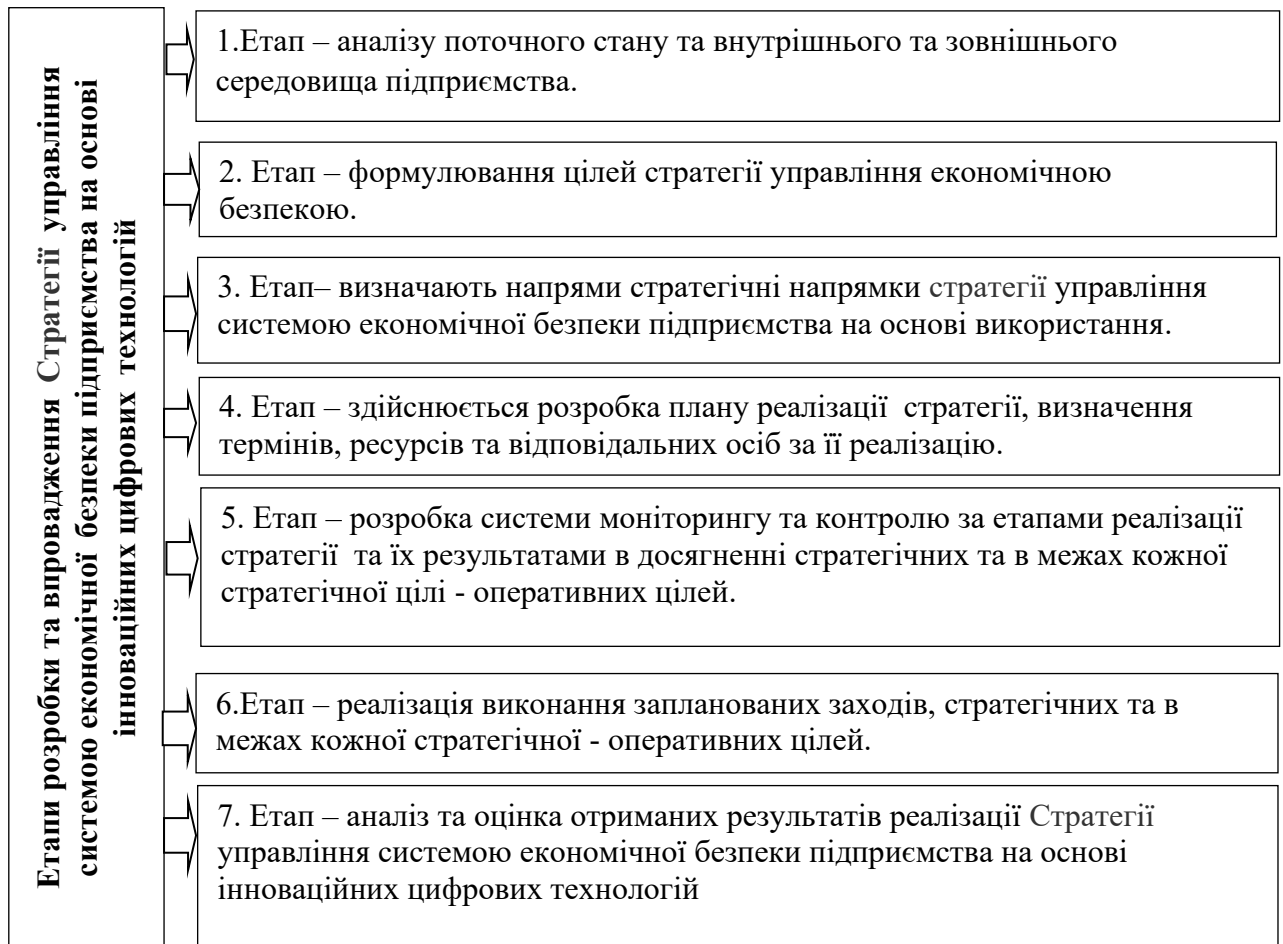


Рис. 3.3. Етапи розробки та впровадження стратегії управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій

Джерело: розроблено автором

Першим етапом розробки та реалізації стратегії є аналіз поточного стану внутрішнього і зовнішнього середовищ підприємства. На цьому етапі проводять аналіз та оцінку стану діяльності підприємства, його фінансових, матеріальних, кадрових, техніко-технологічних та фінансових ресурсів, визначають його потенціал, можливості та основні проблеми в діяльності, а також проводять аналіз небезпек та загроз зовнішнього середовища та вплив економічних, політичних, правових та інших факторів на його діяльність та стан безпеки. Таким чином, визначають, аналізують оцінюють поточний стан підприємства, проводять аналіз фінансової стійкості, техніко-технологічного

потенціалу, інформаційного цифрового забезпечення, визначають сильні та слабкі сторони, можливості та загрози в діяльності підприємства, визначають головні пріоритети діяльності підприємства.

Другим етапом формулюють цілі стратегії управління економічною безпекою, визначають загальні цілі, в тому числі такі як захист майна та ресурсів, активів підприємства, його персоналу, інформації, інноваційні та інші об'єкти забезпечення безпеки та оперативні цілі, спрямовані на конкретизацію загальних цілей та забезпечення можливості для їх практичної реалізації.

На третьому етапі визначаються напрями стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій та планують відповідні заходи до її впровадження за основними складовими системи економічної безпеки підприємства: фінансової, інформаційної, кадрової, правової, техніко-технологічної складових системи економічної безпеки.

На четвертому етапі здійснюється розробка плану реалізації стратегії та визначають і встановлюються терміни виконання тих чи інших стратегічних заходів та особи, працівники та підрозділи, відповідальні та виконавці запланованих заходів. На цьому ж етапі визначаються ресурси та необхідні кроки для розробки та реалізації стратегії, включаючи кадрові, техніко-технологічні, фінансові та матеріальні ресурси.

На п'ятому етапі здійснюються розробка системи моніторингу показників економічної безпеки та контролю за етапами реалізації стратегії та їх результатами в досягненні оперативних та стратегічних цілей. Проводиться проміжний контроль за етапами реалізації, за виконанням плану, виявленням відхилень та прийняттям необхідних заходів та дій на їх усунення.

На шостому етапі здійснюється реалізація виконання запланованих заходів в досягненні оперативних та стратегічних цілей.

На сьомому етапі проводять аналіз та оцінку отриманих результатів реалізації Стратегії управління системою економічної безпеки підприємства

на основі використання інноваційних цифрових технологій, виявляють фактичні значення показників-індикаторів та порівнюють їх із запланованими, аналізують причини відхилень та готують рекомендації щодо врахування змін в наступних етапах формування та реалізації стратегій.

Таким чином, визначено комплекс стратегічних напрямів та цілей стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій, до складу яких входить (1) інформаційно-цифровий напрям; (2) напрям автоматизації, оптимізації бізнес-процесів; (3) кадровий напрям, що реалізується завдяки навчанню та розвитку персоналу, здобуттям цифрових компетентностей; (4) напрям безпеки інноваційної діяльності з реалізацією стратегічних цілей розробки та впровадження нових інноваційних технологій; (5) напрям впровадження цифрових технологій в забезпеченні безпеки об'єктів; (6) напрям впровадження контролю та моніторингу управління ризиками та виявлено, що комплексна реалізація діяльності за визначеними напрямками, стратегічними та операційними цілями забезпечує можливість підприємству до стійкого та ефективного розвитку, протидії негативним впливам зовнішнього та внутрішнього середовищ, та надає можливості для забезпечення економічної безпеки підприємства в довготривалій стратегічній перспективі завдяки впровадженню та використанню в управлінні системою економічної безпеки підприємства інноваційних цифрових технологій.

3.3. Формування механізму управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій

Механізм управління системою економічної безпеки підприємства є одним із невід'ємних, найважливіших елементів системи економічної безпеки підприємства, оскільки саме він забезпечує управління всієї системою та виступає сукупністю нормативно-правової документації, методів,

інструментів, засобів, технологій, які забезпечують вплив суб'єктів управління на об'єкт управління в процесі здійснення управлінських дій, чим забезпечується сам процес управління системою економічної безпеки. По суті, механізм управління приводить в дію всі інші складові елементи системи, забезпечує фактичне виконання дій, реалізацію заходів, забезпечує мотивацію працівників у вирішенні завдань безпекової діяльності. При цьому, розбудова механізму управління економічною безпекою в умовах цифровізації потребує широкого застосування інноваційних цифрових технологій, використання сучасних технічних засобів програмного забезпечення, що здатне ефективно впливати на рівень якості, відповідності забезпечення безпеки, оптимізацію процесів та зменшення витрат на забезпечення економічної безпеки. Слід зазначити, що найбільш широко застосування цифрових технологій в розбудові механізму управління може бути використано у формуванні та впровадженні моніторингу стану безпеки, аналізу та управління ризиками діяльності, забезпечення кібер-безпеки, автоматизації бізнес-процесів, забезпечення безпеки, захисту інформації, баз даних інформаційної системи підприємства та за іншими напрямками.

Методи є однією із головних складових механізму управління системою економічної безпеки підприємства, що формують зміст та визначають управлінський інструментарій, із застосуванням якого здійснюється саме управління як вплив суб'єктів управління на об'єкти управління з метою отримання бажаного запланованого результату та виконання конкретних дій та заходів.

Першою групою методів, які на наш погляд необхідно застосовувати у функціонуванні механізму управління СЕБП є адміністративно-організаційні методи управління, оскільки вони є сукупністю інструментів, які застосовуються для здійснення прямого впливу на об'єкти управління задля досягнення мети та цілей забезпечення економічної безпеки підприємства. Слід зазначити, що всі інструменти адміністративно-організаційних методів засновані на дотриманні принципів єдиноначальності, делегування

повноважень та відповідальності, формуванні ієрархії та підпорядкування. Характеризуючи адміністративно-організаційні методи та їх інструментарій слід зазначити, що: (1) вони здійснюють безпосередній прямий вплив на об'єкти управління, в першу чергу на працівників, делегуючи та призначаючи їм виконання певних дій чи надаючи їм відповідні повноваження; (2) закріплені у вигляді внутрішньої нормативно-правової документації управлінські рішення є обов'язковими до виконання та передбачають надання ресурсів, необхідних для цього; (3) визначають та встановлюють внутрішні норми і регламенти, системи забезпечення економічної безпеки – обов'язкові до виконання відповідними працівниками, яких вони стосуються безпосередньо та дотримання всіма працівниками підприємства; (4) забезпечують впровадження контролю та закріплення особистої відповідальності працівників за результати виконання дій; (5) забезпечують організацію робіт, розподіл завдань, робіт та координацію дій між працівниками в межах підрозділу з економічної безпеки та між іншими структурними підрозділами в питаннях забезпечення та дотримання відповідних безпекових правил та норм.

Ключовими інструментами адміністративно-організаційних методів є сама стратегія економічної безпеки, накази, розпорядження, положення про службу економічної безпеки, посадові інструкції, інструкції, що формалізують правила та порядок виконання певних дій чи впровадження регламентів в питаннях забезпечення економічної безпеки підприємства та інші документи, що мають письмову форму прийнятих управлінських рішень. До інструментів адміністративно-організаційних методів належать також норми, правила та стандарти, які встановлюють внутрішній порядок, регламенти діяльності із забезпечення економічної безпеки, затвердження та дотримання працівниками відповідних інструкцій, інструктаж працівників, впровадження контролю над діяльністю та застосування санкцій за порушення встановлених правил чи порушення норм фінансової, матеріальної та іншої відповідальності.

Слід зазначити, що адміністративно-організаційні методи забезпечують нормування із встановленням та визначенням норм, правил, порядку, в тому числі у визначенні норм часу, витрат, норм в питаннях економічної безпеки, дотримання яких дає можливість забезпечувати безпеку роботи підрозділів, працівників та загалом функціонування.

Регламентування діяльності дає можливість впроваджувати внутрішні норми та правила з питань економічної безпеки, роботи з фінансовими, інформаційними, матеріальними, техніко-технологічними ресурсами, регламентувати роботу структурних підрозділів та окремих працівників.

Інструктаж передбачає проведення інструктажів працівників з питань охорони праці, техніки безпеки, роботи з матеріальними, фінансовими ресурсами, дій в тих чи інших безпекових ситуаціях та інших питань, що можуть впливати на забезпечення безпеки.

Загалом, впровадження адміністративно-організаційних методів засновано на наданні, затвердженні письмових розпоряджень, що визначають та встановлюють норми, засади діяльності із забезпечення безпеки та є обов'язковими для виконання всіма керівниками та працівниками підприємства всіх рівнів. Слід зазначити, що застосування адміністративно-організаційних методів механізму управління економічною безпекою дає можливість досягнути мету та цілі забезпечення безпеки завдяки ефективній організації робіт та забезпеченню належного всебічного контролю; забезпечити кращу організацію виконання робіт та дотримання встановлених норм трудової дисципліни; здійснювати стратегічне управління, планування; приймати та реалізувати управлінські рішення, реалізувати заходи з забезпечення економічної безпеки; активно реагувати на зміни та своєчасно впроваджувати оперативні управлінські рішення.

Наступною групою адміністративних методів, застосування яких є необхідним у функціонуванні механізму управління системи економічної безпеки підприємства є адміністративно-розпорядчі методи. Адміністративно-розпорядчі методи є засобами, які здійснюють вплив на діяльність працівників

та засновані на нормах та делегованих службових повноваженнях. Інструментами адміністративно-розпорядчих методів виступають засоби оперативного впливу, такі як складання планів, проведення нарад, надання вказівок та зауважень працівникам, а також інструменти розпорядчого впливу, такі як прийняття директив, постанов, рішень та наказів для вирішення питань тактичної діяльності із забезпечення економічної безпеки підприємства. Розпорядчі методи забезпечують можливості до здійснення оперативного управління із застосуванням, прийняттям наказів, розпоряджень та наданням безпосередніх усних вказівок працівникам щодо їх виконання. Важливого значення у застосуванні організаційно-розпорядчих методів має контроль впровадження та ефективність дій щодо забезпечення економічної безпеки та дотримання працівниками норм, вимог економічної безпеки та оперативний контроль з перевіркою виконання поставлених задач.

Змістом адміністративно-розпорядчих методів є організація виконання визначених задач завдяки узгодженому визначенню та розподілу робіт, обов'язків, надання працівникам чітких та конкретних вказівок щодо виконання робіт та здійснення контролю їх результатів.

Слід зазначити, що застосування адміністративно-організаційних та адміністративно-розпорядчих методів невід'ємно пов'язано із застосуванням економічних та соціально-психологічних та технологічних методів та разом вони формують комплекс засобів, необхідних для здійснення управління економічною безпекою підприємства.

В окремих випадках застосовують так звані дисциплінарні методи, які включають зауваження, догани, переміщення працівників чи посадових осіб та звільнення, застосовують для впровадження управлінських заходів у випадку грубого порушення працівниками вимог безпеки та своїх професійних обов'язків, а тому для дотримання загального порядку та дотримання працівниками встановлених адміністрацією правил та вимог потребують адміністративного покарання працівників із застосуванням відповідних інструментів.

Економічні методи управління механізму забезпечення економічної безпеки виступають комплексом економічних інструментів та засобів, спрямованих на захист матеріальних активів, майна, матеріальних та фінансових ресурсів підприємства та здійснюють забезпечення економічної безпеки підприємства завдяки фінансово-економічному впливу.

Інструментарій економічних методів в управлінні економічною безпекою включає проведення фінансово-економічного аналізу, бюджетування, розрахунок собівартості, політику та методи ціноутворення, фінансового та інвестиційного розвитку підприємства, впровадження контролінгу, аудиту, моніторингу, внутрішнього контролю та інше.

Так, інструменти фінансово-економічного аналізу здатні забезпечити регулярне системне проведення дослідження фінансово-економічного стану підприємства, його основних фінансово-економічних показників, таких як рентабельність, фінансова стійкість, ліквідність, автономність, прибутковість, платоспроможність та інші. На основі цих показників доцільним є впровадження моніторингу як безперервного стеження за фінансово-економічним станом та станом фінансово-економічної безпеки підприємства.

Проведення фінансово-економічного аналізу та його результати мають передувати плануванню, розробці та прийняттю важливих стратегічних рішень як в сфері економічної безпеки, так і загалом в діяльності підприємства. Це дасть можливість більш ефективно і виважено приймати управлінські рішення та зменшити ризики управлінської діяльності.

Наступним інструментом, який застосовується в межах економічних методів є управління ризиками, що передбачає виявлення, ідентифікацію та оцінювання ризиків обґрунтування стратегії, спрямованої на зменшення ризиків застосовуючи відповідні інструменти управління ризиками, такі як: страхування ризиків, розподіл ризиків, диверсифікацію, а також розробку, підготовку планів безпеки на випадок настання ризикових подій.

Бюджетування є однією із сучасних інструментів, технологій управління, яка може ефективно застосовуватися в управлінні системою

економічної безпеки підприємства та полягає у розробці планування та затвердження на підприємстві бюджету доходів та витрат, що дає можливість планувати витрати підприємства та більш ефективно і раціонально управляти фінансовими ресурсами за рахунок зменшення витрат.

Наступним інструментом є фінансова та інвестиційна політика, яка полягає у впровадженні контролю над фінансовими потоками та ретельний відбір інвестиційно-інноваційних проектів, які реалізує підприємство з метою уникнення фінансових втрат капіталу, залучених інвестиційних чи кредитних ресурсів на реалізацію економічно недоцільних, збиткових та високо-ризикових проектів. Ретельний розгляд, експертиза проектів дає можливість виявити потенційно збиткові та неефективні проекти та запобігти загрозам втрати значних фінансових коштів.

Вибір та застосування тих чи інших методів ціноутворення є наступним важливим інструментом економічних методів управління в системі економічної безпеки. Це пов'язано із тим, що завдяки обраному методу ціноутворення визначається рентабельність, прибутковість діяльності та конкурентоспроможність самих товарів чи послуг на ринку. Тому, вибір та визначення методу ціноутворення для конкретних товарів в конкретних ринкових умовах здатне забезпечити підприємству необхідний рівень конкурентоспроможності та прибутковості операційної діяльності, що формує основу фінансової стабільності підприємства загалом.

Впровадження внутрішнього фінансового контролю є наступним інструментом, який встановлює норми процедури фінансової відповідальності посадових осіб підприємства та спрямований на запобігання фінансовим зловживанням, шахрайству, привласненню фінансових коштів підприємства та інших зловживань посадових осіб підприємства чи матеріально-відповідальних працівників.

Управління оборотним капіталом, запасами підприємства його кредиторською та дебіторською заборгованістю є фінансовим інструментом, спрямованим на попередження проявів та поширення економічної кризи, що

може негативно вплинути на стан безпеки підприємства. Впровадження такого управління оборотним капіталом дає можливість оптимізувати, зменшити витрати ресурсів, оборотних активів підприємства та забезпечити зростання фінансової стійкості. Слід зазначити, що в межах економічних методів застосовується багато інструментів, спрямованих на забезпечення контролю.

Так, одним із ефективних сучасних економічних інструментів в управлінні економічною безпекою підприємства є контролінг. Контролінг забезпечує цілеспрямований збір, обробку, опрацювання інформації необхідної для прийняття управлінських рішень з метою найбільш ефективного розподілу витрат та управління прибутком підприємства. Таким чином, контролінг дає можливість зменшити, оптимізувати витрати та акумулювати і розподілити прибуток для забезпечення подальшого розвитку. В свою чергу контролінг здатен забезпечувати керівників інформацією, необхідною для прийняття виважених управлінських рішень.

Наступним інструментом економічних методів є моніторинг, який широко застосовується в управлінні системою економічної безпеки підприємства, оскільки саме впровадження моніторингу як безперервного стеження за станом показників-індикаторів дає можливість досліджувати, визначати стан та рівень економічної безпеки та ефективно реагувати на їх зміни, своєчасно планувати та впроваджувати комплекси необхідних превентивних дій, заходів.

Іншим важливим інструментом економічних методів, що може застосовуватися в управлінні системою економічної безпеки є аудит. Аудит дає можливість провести періодичну незалежну зовнішню перевірку, обстеження документації підприємства з метою, в тому числі, визначення стану безпеки. Особливо важливого значення застосування аудиту має для правової складової економічної безпеки, оскільки дає можливість виявити відповідність складених документів підприємства нормам та вимогам чинного законодавства, вимогам податкового кодексу та нормам ведення бухгалтерського обліку та звітності. Таким чином, застосування інструменту

аудиту в управлінні системою економічної безпеки підприємства потрібно використовувати періодично, як один із дієвих інструментів перевірки юридичного супроводу та відповідності ведення документації підприємства.

Наступним напрямом інструментів економічних методів в управлінні економічної безпеки підприємства є інструменти економічного стимулювання, мотивування працівників, персоналу підприємства для ефективного виконання їх професійних обов'язків. Економічні інструменти мотивації загалом мають широке застосування, оскільки мова йде не лише про мотивування працівників служби економічної безпеки. Одним із ключових аспектів успіху в забезпеченні економічної безпеки підприємства загалом є залучення до безпекових процесів всіх працівників підприємства, всіх його структурних підрозділів з метою широкого впровадження безпекових заходів та розуміння кожним працівником необхідності в дотриманні безпекових вимог та норм, що здатне забезпечити високу ефективність захисту підприємства від внутрішніх небезпек, загроз та підвищити стійкість підприємства в протидії зовнішнім ризикам та загрозам.

Інструментами економічних методів мотивації виступають інструменти преміювання працівників, впровадження тарифної системи оплати праці, впровадження диференційованої оплати праці, що напряду залежатиме від обсягів чи результатів зробленої роботи, відпрацьованого робочого часу, надання працівникам соціальних пакетів, а також, впровадження економічних заходів покарання за грубі порушення фінансової, матеріальної, корпоративної дисципліни, встановлених норм, вимог та виконання ними своїх обов'язків у вигляді штрафів та вирахування із заробітної плати працівників.

Загалом, економічні методи в управлінні системою економічної безпеки підприємства діють як прямо, так і опосередковано, формуючи матеріальну зацікавленість працівників та стимулюючи прояви ініціативи, активності та спрямовані на забезпечення зростання відповідальності працівників за результати прийнятих управлінських рішень та дій.

Наступною групою методів, що мають застосування в механізмі управління системою економічної безпеки підприємства виступають соціально-психологічні методи.

Соціально-психологічні методи виступають сукупністю дій, спрямованих на особистість працівників та психологію, поведінку та соціальні зв'язки між працівниками, персоналом підприємства, а також на соціальні процеси, які відбуваються в колективі підприємства загалом. На наш погляд, інструментами соціально-психологічних методів, які доцільно застосовувати в управлінні економічної безпеки в першу чергу є інструменти розбудови та розвитку корпоративної культури та позитивного внутрішнього соціально-психологічного клімату в колективі. Важливим є встановлення певних внутрішніх етичних норм в колективі, які будуть діяти як певні «запобіжники» проти порушення працівниками трудової, фінансової, матеріальної відповідальності, проявів корупції адже в колективі де такі прояви є не типовими та загально не прийнятними їх легше та швидше виявити й протидіяти їм. Отже, здорова внутрішня атмосфера колектив дотримання норм моралі, професіоналізму підвищує рівень відповідальності працівників та уважності до своїх обов'язків, дотримання безпекових вимог, що стають не виключенням, а нормою щоденної праці для персоналу та загально прийнятними.

Не менш важливим є планування соціального розвитку з покращенням умов праці персоналу, побутових умов та можливостей для відпочинку працівників. Іншою важливою групою соціально-психологічних методів є зростання трудової та соціальної активності працівників, що досягається з використанням таких інструментів, як обмін досвідом, направленням працівників на стажування, соціальні заохочення розвитку їх інтересів. Не менш важливого значення в соціально-психологічному стимулюванні має стимулювання професійної активності, проявів ініціативи, що досягається із застосуванням таких інструментів, як: публічне визнання заслуг, досягнення працівників з публічним виголошенням подяк, врученням грамот; занесенням

відповідних записів до трудової книжки працівників; наданням їм повноважень представляти підприємство на зовнішніх заходах, конференціях, презентаціях, виступах; включення працівників до складу комітетів, комісій, долучення до процесів управління підприємством та ухвалення управлінських рішень.

Загалом, інструментами соціально-психологічних методів в управлінні системою економічної безпеки підприємства виступають: формування позитивного клімату та розвиток корпоративної культури підприємства; управління конфліктами; впровадження соціально-психологічної адаптації новоприбулих працівників підприємства; впровадження широкого кола заходів щодо соціально-психологічної мотивації, стимулювання персоналу в питаннях дотримання норм та вимог економічної безпеки підприємства.

Іншими важливими інструментами, які доцільно застосовувати для управління є інструменти формування та розвитку персоналу, спрямовані на знаходження та підтримку оптимальної чисельності співробітників підприємства, враховуючи психологічну сумісність працівників; інструменти, спрямовані на гуманізацію відносин між працівниками на підприємстві, до яких слід віднести формування відповідного стилю управління; впровадження культури управління, встановлення та дотримання певної етики управління; а також інструменти стимулювання та мотивування працівників з використанням нематеріальних соціально-психологічних методів та засобів.

Слід зазначити, що на управління системою економічної безпеки підприємства також впливають ідеологічні методи, які полягають в тому, що на підприємстві потрібно сформувати, встановити та дотримуватися певної внутрішньої ідеології забезпечення безпеки. Зазначимо, що на наш погляд, ідеологічні методи враховують нематеріальний соціально-психологічний вплив на колектив і їх слід застосувати, проте вони відносяться до соціально-психологічних методів та визначають окремі інструменти управління, такі як впровадження корпоративної ідеології, певної мети, духу, що є основою формування корпоративної культури загалом, тому безперечно ідеологічні

інструменти також повинні використовуватись як інструменти, спрямовані на забезпечення безпеки в довготривалій та майбутній перспективі.

Іще однією групою соціально-психологічних методів є інструменти професійного відбору та навчання працівників, адже це дає можливість відібрати працівників та виявити їх професійну придатність на етапі прийняття працівника на роботу, на підприємство, та не приймати працівників, що не відповідають вимогам чи можуть становити нові додаткові загрози та ризики в діяльності, ставши джерелом появи цих ризиків. Саме тому, однією із важливих співбесід при прийманні працівників на роботу на підприємство має бути співбесіда з керівником служби економічної безпеки підприємства. Окрім цього, важливе значення має відповідність призначення працівника на посаду та визначення його обов'язків, які відповідають його психологічному типу з метою найкращого, найбільш оптимального використання його знань, навичок та трудових ресурсів. Також важливими є інструменти подальшого навчання та підвищення кваліфікації працівників, в тому числі й надання психологічних установок, заряджання працівників на ефективну роботу, дотримання безпекових заходів, в тому числі в умовах підвищеного рівня небезпек та загроз, чи за виконання небезпечних робіт.

Забезпечення економічної безпеки підприємства на основі використання сучасних інноваційних цифрових технологій, на нашу думку, потребує застосування відповідних засобів технічного забезпечення, технологій та відповідних методів управління. Відповідно до цього, наступною групою методів управління системою економічної безпеки підприємства виступають техніко-технологічні методи та їх інструменти.

Слід зазначити, що вони також визначаються науковцями як спеціальні технічні засоби.

Технічними технологічними засобами застосування техніко-технологічних методів виступають використання «поліграфу», систем відеоспостереження, аудіо-обладнання з фіксацією процесів, застосовування засобів технічної перевірки приміщень, забезпечення інформаційно-

аналітичного підрозділу служби економічної безпеки підприємства всім необхідним спеціальним обладнанням, приладами, програмним забезпеченням, впровадженням перевірки претендентів на керівні посади та працівників підприємства за обліком у МВС.

Слід зазначити, що техніко-технологічні методи забезпечення економічної безпеки підприємства узагальнюючи можна представити як певний комплекс заходів, що дають можливість технічними, технологічними засобами забезпечити захист інформації, обладнання, технологій, що використовуються від дії небезпек та загроз.

До основних техніко-технологічних методів механізму забезпечення економічної безпеки можна віднести впровадження інноваційних, цифрових технологій: програмного забезпечення; систем захисту комерційної таємниці; контроль доступу до інформаційних систем; автоматизацію та роботизацію процесів операційної, виробничої діяльності; забезпечення безпеки на об'єктах.

Так, одним із потужних сучасних інструментів техніко-технологічних методів, як в управлінні загалом, так і в забезпеченні економічної безпеки підприємства є автоматизація та впровадження робототехніки в управлінні процесами операційної та виробничої діяльності. Втім, на нашу думку, така автоматизація процесів з використанням сучасних цифрових технологій, в тому числі, успішно застосовується в управлінні будь-якими процесами операційної діяльності, в тому числі в управлінні процесами просування та реалізації продукції, роботи з покупцями, консультування, ведення операцій обліку, роботи з документацією, веденням логістичних процесів. При цьому, впровадження інноваційних цифрових технологій з метою забезпечення безпеки здатне інтегрувати безпекові завдання в основні процеси функціонування та поєднати їх. В цьому полягає важливе значення, роль та сутність впровадження інноваційних цифрових технологій в забезпеченні економічної безпеки підприємства, саме в можливості їх інтеграції у цифрові системи в функціональній діяльності підприємства. Відповідно, автоматизація

та роботизація процесів здатна уніфікувати, стандартизувати, забезпечити зростання якості та обсягів виконання процесів, забезпечити зростання їх точності, відповідності, зменшити ризики та помилки у функціонуванні за рахунок зменшення впливу людського фактору, зростання точності та продуктивності виконання процесів. Іще однією значною перевагою, на наш погляд, є зменшення витрат на виконання одиниці процесів чи операцій виробництва. Впровадження систем управління процесами та виробництвом, таких як (MES, ERP), здатне оптимізувати витрати всіх видів ресурсів, забезпечити ефективний контроль та підвищити ефективність на всіх етапах здійснення діяльності.

Наступним інструментом техніко-технологічних методів є захист інформаційних систем з широким застосуванням цифрових інноваційних засобів захисту інформації, в тому числі сучасного ефективного антивірусного програмного забезпечення, брандмауерів, шифрування, кодування інформації та впровадження на підприємствах контролю доступу до інформаційних систем, мереж загалом та до інформації, а особливо інформації, що становить комерційну таємницю зокрема.

Іншими важливими інструментами техніко-технологічної безпеки є забезпечення безпеки на виробничих об'єктах, об'єктах операційної діяльності із застосуванням відео-спостереження та аудіо-фіксації, систем охоронної, протипожежної сигналізації, а також впровадження контролю доступу на об'єкти.

Не менш важливими інструментами техніко-технологічних методів виступають інструменти, спрямовані на захист конфіденційної інформації та комерційної таємниці підприємства, а саме: укладання з працівниками договорів про нерозголошення комерційної таємниці, впровадження ключів доступу та обмеження працівникам доступу до конфіденційної інформації; впровадження систем контролю доступу.

Інструменти техніко-технологічних методів успішно застосовуються для проведення спостережень, моніторингу та аналізу інформації, даних

спостережень з метою виявлення відхилень, аномалій, потенційних загроз, які можуть впливати на безпеку виконання процесів. Відповідно, такий інструментарій є ефективним превентивним засобом в забезпеченні економічної безпеки.

Застосування техніко-технологічних методів та їх інструментів захисту здатне забезпечити безпеку в роботі обладнання та убезпечити від перевантажень, виходу з ладу, настання аварійних ситуацій, що може завдати збитку та зашкодити роботі підприємства.

Забезпечення технічного захисту інформації виступає ще одним напрямком застосування інструментів техніко-технологічних методів, оскільки запобігає ризикам несанкціонованого зчитування, копіювання чи знищення інформації, баз даних, розміщених на електронних ресурсах чи під час їх передачі мережами Інтернет чи іншими засобами зв'язку.

Позитивною практикою підприємств у впровадженні безпекових заходів механізму забезпечення безпеки є розробка та затвердження аварійних планів, що визначають дії працівників у випадку настання надзвичайних ситуацій: пожежі, аварії, терактів, інших нештатних ситуацій, що також є засобами превентивних дій що дає можливість зменшити ризики та збитки від настання таких високо-ризикових подій.

Впровадження всіх вищезазначених технічних дій та заходів у забезпеченні економічної безпеки підприємства актуалізує питання підготовки, навчання персоналу до роботи з відповідним обладнанням, програмним забезпеченням, приладами, а також дотримання знань щодо дій у випадку настання аварій, високо-ризикових ситуацій. Таким чином, одним із важливих інструментів виступає проведення навчальних курсів, тренінгів та проведення інструктажів для працівників з техніки безпеки, протипожежної безпеки, дій в аварійних ситуаціях, а також вимог, правил роботи з інформацією, технікою та технологіями.

Впровадження техніко-технологічних інструментів дає можливість зменшити ризики, забезпечує захист матеріальних та нематеріальних активів,

майна, конфіденційної інформації, інформаційних ресурсів підприємства, його працівників та забезпечує належний рівень безпеки функціонування підприємства.

Основною метою розбудови та функціонування механізму управління економічною безпекою підприємства є забезпечення надійної, стабільної роботи підприємства в теперішній час та в стратегічній перспективі. Цілями механізму управління є: захист від небезпек та загроз, збереження та зростання конкурентоспроможності, ефективності діяльності та забезпечення подальшого майбутнього розвитку.

Механізм управління системою економічної безпеки підприємства має свої типові елементи, до яких слід віднести: стратегію забезпечення безпеки; проведення аналізу, оцінювання небезпек та загроз; функціонування відповідних організаційних структур – підрозділів із забезпечення економічної безпеки; планування дій та заходів із забезпечення безпеки; застосування відповідних методів, засобів, інструментів, технологій управління забезпеченням безпеки; впровадження процесів та процедур забезпечення безпеки; навчання та підготовку персоналу; розбудову комунікацій та організацію взаємодії в забезпеченні економічної безпеки; застосування інструментів контролю та моніторингу. Важливою складовою розбудови системи економічної безпеки підприємства та умовою ефективної діяльності функціонування механізму забезпечення економічної безпеки підприємства є наявність стратегії та визначення стратегічних цілей діяльності із забезпечення економічної безпеки підприємства на майбутню перспективу. Функціонування механізму управління системою економічної безпеки передбачає планування дій та заходів, спрямованих на недопущення та мінімізацію небезпек, загроз і відповідно подальше впровадження та реалізацію прийнятих планів

Механізм управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій представлено на рис. 3.4.



Рис. 3.4. Механізм управління СЕБП на основі інноваційних цифрових технологій

Джерело: розроблено автором

Основні функції щодо виконання дій та заходів механізму управління економічною безпекою здійснюють працівники структурного підрозділу, відділу чи департаменту економічної безпеки, проте в забезпеченні економічної безпеки на тих чи інших етапах та заходах приймають участь та можуть бути задіяними інші керівники та працівники структурних підрозділів підприємства, відповідні фахівці.

Дія механізму управління економічною безпекою та реалізація прийнятих планів передбачає встановлення та впровадження зрозумілих процесів та процедур, як організації робіт, так і контролю за їх виконанням та результатами. Навчання працівників з питань безпеки виступає однією із важливих умов ефективного забезпечення економічної безпеки, особливо роль навчання та отримання відповідних знань та навичок зростає в умовах застосування процесів впровадження безпекових заходів сучасних інноваційних цифрових технологій, які потребують специфічних знань та навичок, набуття працівниками відповідних компетентностей. Внаслідок цього вважаємо, що впровадження навчання та підвищення кваліфікації працівників підрозділу безпеки та інших структурних підрозділів з питань безпеки може розглядатися як невід'ємний елемент в комплексі дій механізму управління СЕБ.

Впровадження контролю та моніторингу застосування методів, реалізації запланованих заходів, здійснення аналізу та оцінки їх виконання і результатів є невід'ємною важливою складовою механізму управління, оскільки дає можливість оцінити ефективність його функціонування та своєчасно запровадити, внести необхідні зміни в його функціонуванні та реалізації запланованих заходів, що є особливо важливим в умовах постійних динамічних змін зовнішнього та внутрішнього середовищ, появи і впливу нових небезпек та загроз.

Узагальнюючи зазначимо, що механізм управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій являє собою сукупність елементів, методів, інструментів, засобів

та технологій управління, які забезпечують вплив на об'єкти управління з метою здійснення реалізації запланованих дій та отримання результатів забезпечення економічної безпеки підприємства. Безпосередні дії щодо управління та планування діяльності механізму здійснює перший керівник, власник підприємства, керівник та працівники служби структурного підрозділу із забезпечення економічної безпеки. Вони виступають центральними суб'єктами управління, виконують всі відповідні управлінські функції та приймають і забезпечують реалізацію управлінських рішень та контроль за їх виконанням. При цьому, у виконанні безпекових та управлінських функцій служба, підрозділ з економічної безпеки взаємодіє із зовнішніми суб'єктами забезпечення економічної безпеки, в першу чергу структурами МВС України, іншими безпековими структурами та внутрішніми суб'єктами безпеки, до яких відносять всі структурні підрозділи та працівників підприємства, задіяних в заходах та діях з забезпечення та дотримання економічної безпеки. Безпосередньо управління включає низку дій, а саме: розробку та затвердження стратегії СЕБ; розробку завдань із забезпечення безпеки; планування заходів та складання поточних планів; організацію контролю за їх виконанням; впровадження стандартів виконання робіт та розбудову системи мотивації працівників, їх стимулювання для дотримання вимог та норм економічної безпеки.

Розбудова механізму управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій потребує формування самого механізму взаємодії між службою економічної безпеки, керівником підприємства, між структурними підрозділами, зовнішніми та внутрішніми суб'єктами забезпечення економічної безпеки, а також наявності правових засад функціонування цього механізму, як з позицій наявності та дотримання відповідних норм чинного законодавства та з позицій формування відповідного внутрішнього нормативного правового поля формування системи та механізму управління економічною безпекою та регулювання внутрішніх процесів забезпечення економічної безпеки. Важливе

значення при цьому має надання суб'єктам забезпечення безпеки, відповідних повноважень, делегування та закріплення за ними відповідних прав та обов'язків. Це дає можливість чітко визначити та закріпити зони відповідальності працівників та персоналізувати цю відповідальність.

Методи, інструменти та технології механізму управління включають адміністративні, організаційні методи, адміністративні оперативно-розпорядчі методи, економічні, соціально-психологічні та техніко-технологічні методи та їх інструменти, використання яких дає можливість здійснювати весь комплекс управлінських дій та впливів на об'єкти управління за всіма функціональними складовими напрямками діяльності підприємства і таким чином забезпечувати економічну безпеку підприємства на належному сучасному рівні.

Механізм управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій діє завдяки розбудові сучасних цифрових комунікацій, що забезпечують можливість планувати та впроваджувати ефективні заходи протидії внутрішнім та зовнішнім небезпекам, загрозам, ризикам та аналізувати результати впроваджених управлінських дій.

Завершальним етапом механізму управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій є впровадження моніторингу показників-індикаторів та на їх основі проведення аналізу, оцінки результативності, функціонування системи економічної безпеки підприємства та досягнення прийнятих, визначених цілей стратегії забезпечення економічної безпеки.

Ефективне функціонування механізму управління економічною безпекою підприємства потребує розбудови сучасних цифрових комунікацій та налагодження взаємодії між структурними підрозділами підприємства, між його працівниками у внутрішньому середовищі підприємства та формування і впровадження якісних ефективних комунікацій з партнерами, покупцями, постачальниками, стейкхолдерами зовнішнього середовища підприємства.

Узагальнюючи зазначимо, що розбудова та впровадження механізму управління системи економічної безпеки підприємства має важливу роль, значення та забезпечує фактичну реалізацію розробленої стратегії безпеки та впровадження запланованих заходів і таким чином приводить в дію всі складові та елементи системи управління економічною безпекою підприємства і дає можливість отримати відповідні результати.

Розбудова та впровадження механізму системи управління економічною безпекою на основі використання інноваційних цифрових технологій дає можливість: до забезпечення стабільного функціонування підприємства, забезпечуючи його захист від ризиків, небезпек та загроз; забезпечення зростання ефективності за рахунок оптимізації використання, зменшення витрат, забезпечення зростання продуктивності діяльності, що загалом дає можливість покращити фінансово-економічні результати його роботи, прибутковість, економічну ефективність; підвищує стійкість та формує умови для подальшого ефективного розвитку підприємства завдяки впровадженню інновацій, передових інноваційних цифрових технологій у всіх сферах діяльності та в системі економічної безпеки; забезпечує захист економічних інтересів у фінансовій, інформаційній, технологічній, правовій та інших сферах функціонування; забезпечує утримання ринкових позицій та зростання конкурентоспроможності підприємства.

Висновки до розділу 3.

Обґрунтовано структуру та елементи системи економічної безпеки підприємства, розбудованої на основі системного, процесного, комплексного, технологічного, наукових підходів та нормативно-правового, методичного, матеріального, фінансового, кадрового та інформаційно-аналітичного забезпечення та використання цифрових технологій, на засадах дотримання загальних та спеціальних принципів, до складу якої входять суб'єкти-

керівники, служба безпеки, що завдяки застосуванню функцій та механізму управління дасть можливість здійснювати системний цілеспрямований вплив на об'єкти управління: працівників, фінансові, матеріальні ресурси, майно підприємства, техніко-технологічні ресурси, засоби; його нематеріальні та матеріальні активи; інформаційні ресурси та ділову репутацію з широким застосуванням сучасних цифрових технологій та засобів з метою забезпечення їх захисту, збереження, примноження - зростання та забезпечення високого рівня економічної безпеки загалом в поточній діяльності підприємства та в майбутньому задля зростання його конкурентоспроможності та подальшого розвитку.

Визначено основні складові системи економічної безпеки підприємства, розбудованої із застосуванням цифрових технологій, до складу яких входить: правова, фінансова, кадрова, інтелектуальна, виробничо-операційна, матеріально-майнова техніко-технологічна, інноваційно-інвестиційна, інформаційно-цифрова, інтерфейсна, ринкова, фізична складові системи економічної безпеки, цифровізація якої дає можливість автоматизувати, оптимізувати процеси управління, зменшити витрати, забезпечити зростання ефективності та результативності у всіх функціональних сферах діяльності підприємства, як єдиної цілісної системи і таким чином досягнути зростання рівня їх стабільності, надійності, економічної безпеки.

Розроблено стратегію управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій, яка включає реалізацію стратегічних та оперативних цілей дії за напрямками реалізації та передбачає цифровізацію процесів здійснення управлінської, операційної, безпекової діяльності підприємства завдяки впровадженню та використанню нових інноваційних цифрових технологій та дає можливість удосконалити процеси управління та здійснювати безпекову діяльність, розбудову та функціонування системи управління та механізму управління економічною безпекою підприємства на сучасному техніко-технологічному рівні відповідно до ринкових, техніко-технологічних вимог та викликів цифрового техніко-

технологічного, ринкового середовищ та забезпечує можливості протидіяти ризикам та загрозам, забезпечувати безпеку, конкурентоспроможність, стійкість та ефективний розвиток підприємства.

Визначено комплекс стратегічних напрямів та цілей стратегії управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій, до складу яких входить (1) інформаційно-цифровий напрям з обґрунтуванням цілей цифровізації робочих місць; розбудови та забезпечення безпеки внутрішніх цифрових комунікацій; цифровізації процесів прийняття управлінських рішень; удосконаленням інформаційно-аналітичного забезпечення; захистом інформаційних цифрових ресурсів; цифровізацією документообігу підприємства; цифровізацією облікових функцій; (2) напрям автоматизації, оптимізації бізнес-процесів, що передбачає реалізацію таких цілей, як: автоматизація, оптимізація бізнес-процесів безпекової діяльності; автоматизація, оптимізація бізнес-процесів маркетингової комерційної діяльності; автоматизація, оптимізація бізнес-процесів логістичної діяльності, управління операціями в ланцюгах поставок; (3) кадровий напрям, що реалізується завдяки навчанню та розвитку персоналу, здобуттям цифрових компетентностей; (4) напрям безпеки інноваційної діяльності з реалізацією стратегічних цілей розробки та впровадження нових інноваційних технологій; управління ризиками інвестиційно-інноваційної діяльності та реалізації проектів підприємства; (5) напрям впровадження цифрових технологій в забезпеченні безпеки об'єктів, що реалізується завдяки впровадженню цифрових технологій в забезпеченні фізичної безпеки, захисту об'єктів; (6) напрям впровадження контролю та моніторингу управління ризиками, реалізація якого передбачає досягнення стратегічних цілей впровадження систем контролю та моніторингу системи економічної безпеки; управління ризиками діяльності підприємства; впровадження цифрових технологій для моніторингу та управління репутацією підприємства. Комплексна реалізація діяльності за визначеними напрямками, стратегічними та операційними цілями забезпечує можливість підприємству до стійкого та ефективного розвитку,

протидії негативним впливам зовнішнього та внутрішнього середовищ та надає можливості для забезпечення економічної безпеки підприємства в довготривалій стратегічній перспективі завдяки впровадженню та використанню в управлінні системою економічної безпеки підприємства інноваційних цифрових технологій.

В роботі сформовано механізм управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій, який виступає сукупністю елементів та забезпечує комплекс дій з розробки та реалізації планів і заходів відповідно до прийнятої стратегії забезпечення економічної безпеки та організації контролю за їх виконанням відповідно до прийнятих стандартів, норм виконання робіт з застосуванням адміністративно-організаційних, оперативно-розпорядчих, економічних, соціально-психологічних, техніко-технологічних методів та їх інструментів. Це дає можливість забезпечувати стійкість та формує умови для подальшого ефективного розвитку підприємства завдяки впровадженню інновацій, передових інноваційних цифрових технологій у всіх сферах діяльності та в системі економічної безпеки; забезпечує захист підприємства від внутрішніх та зовнішніх небезпек та загроз, забезпечує утримання ринкових позицій, зростання конкурентоспроможності та подальший розвиток підприємства.

Виявлено та узагальнено інструменти: адміністративно-організаційні методи, до яких відноситься: стратегія, накази, розпорядження, положення про службу ЕБ, інструкції, нормування та регламентування, впровадження правил, норм, стандартів, інструктажі, контроль, застосування санкцій та інше; адміністративно-оперативно-розпорядчі методи: оперативні (план, нарада, вказівки, зауваження); розпорядчі (директиви, постанови, рішення, накази), організаційне інформування; інструменти економічних методів: фінансово-економічний аналіз, аудит, бюджетування, контролінг, методи ціноутворення, впровадження фінансової інвестиційної політики, матеріальна мотивація працівників, управління витратами; інструменти техніко-технологічних методів та засобів: впровадження інноваційних, цифрових технологій MES,

ERP, захист комерційної таємниці, контроль доступу до інформаційних систем, автоматизацію процесів, забезпечення безпеки на об'єктах, перевірка співробітників за обліком МВС та ін.; інструменти соціально-психологічних методів, а саме: планування соціального розвитку, стимулювання ініціативи, розвиток трудової і соціальної активності, розвиток корпоративної культури, створення позитивного клімату, соціальна адаптація, мотивація, управління конфліктами; системне впровадження, застосування яких дасть можливість здійснювати весь комплекс дій в управлінні економічною безпекою підприємства на сучасному відповідному техніко-технологічному рівні.

Результати проведених досліджень та розробок висвітлено у працях автора: [244, 245, 246, 247, 248].

ВИСНОВКИ

Основні наукові результати дослідження дали можливість розв'язати важливе наукове завдання обґрунтування теоретико-методичних засад та розробки науково-практичних рекомендацій управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Отримані науково-теоретичні, методичні і практичні результати дають підстави для таких висновків:

1. Досліджено концептуально-методичні засади управління системою економічної безпеки підприємства та виявлено дію наукових підходів трьох рівнів: (1) підходів до розуміння поняття економічної безпеки; (2) підходів до розуміння системи економічної безпеки; (3) підходів до управління системою економічної безпеки підприємства, та на відміну від існуючих, обґрунтовано новий технологічний підхід до розуміння управління системою економічної безпеки підприємства як сукупності підсистем, складових та елементів, взаємодія яких реалізується із застосуванням сучасних цифрових технологічних засобів, що забезпечує ефективне функціонування механізму системи безпеки та застосування методів, інструментів, технологій управління; найбільш оптимальне раціональне використання її кадрових, фінансових, матеріальних ресурсів; зростання рівня безпеки підприємства завдяки широкому використанню технологічних можливостей і зростанню ролі та значення інформаційно-аналітичного забезпечення в прийнятті управлінських рішень.

2. Систематизовано наукові концепти, узагальнено функції застосування цифрових технологій в управлінні з виявленням дії облікової, логістичної, безпекової, інформаційно-аналітичної, комунікаційної, операційної, маркетингової функцій, використання яких забезпечує можливість впровадження цифровізації, цифрової трансформації бізнес-процесів у всіх функціональних сферах діяльності підприємства та формування якісно нових

комунікацій співпраці і взаємодії з партнерами, стейкхолдерами зовнішнього, глобального середовища, що дасть можливість оптимізувати та зменшити витрати, забезпечити зростання економічної та ринкової ефективності діяльності підприємства.

3. Досліджено теоретичні основи застосування інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та визначено сутність інформаційно-цифрової складової системи економічної безпеки підприємства, яка поєднує в собі ознаки та функції інформаційної та цифрової складових, що разом надають технології, інструменти та засоби, мають значно ширші можливості для впровадження ефективного інформаційно-аналітичного забезпечення та формують комплексний дієвий захист підприємства адаптований до протидії реалізації небезпек і загроз зовнішнього ринкового і внутрішнього середовищ в умовах впровадження технологій Четвертої промислової революції, Індустрії 4.0. та нових технологічних викликів і змін.

4. Проведено аналіз та сформовано проекцію впливу впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, яка дає можливість виявити та ідентифікувати вплив використання цифрових технологій загального спрямування, інноваційних цифрових технологій управління забезпеченням функціональної діяльності та безпосередньо цифрових технологій, які використовуються в забезпеченні економічної безпеки підприємства, загальне та комплексне використання яких дає можливість здійснювати управління системою економічної безпеки на сучасному цифровому рівні та забезпечувати належний рівень економічної безпеки підприємства в умовах нових цифрових викликів та загроз.

5. Ідентифіковано та систематизовано три групи показників: цифровізації загальних процесів функціонування підприємства; показників впровадження цифрових технологій для управління бізнес-процесами діяльності; показників впровадження цифрових технологій в забезпеченні економічної безпеки до складу яких віднесено п'ятдесят два показника

системний аналіз яких забезпечує можливості для комплексного дослідження процесів впровадження інноваційних цифрових технологій та на основі отриманих даних дає можливість здійснювати моніторинг та подальше всебічне системне оцінювання процесів управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

6. Розроблено модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, що передбачає оцінювання на трьох рівнях: рівні загальних процесів функціонування, рівні окремих бізнес-процесів діяльності та в забезпеченні економічної безпеки підприємства. Крім того модель передбачає комплексне оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки, що забезпечує нові можливості для проведення аналізу, оцінювання та отримання об'єктивних комплексних даних щодо стану та рівня впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства та дозволяє впровадити моніторинг та виявити слабкі місця, недоліки, спланувати своєчасні заходи з метою зростання рівня цифрової безпеки та ефективності підприємства у протидії ризикам та загрозам в умовах сучасної цифрової трансформації, зростання рівня кіберзагроз зовнішнього середовища.

7. Обґрунтовано структуру і елементи системи економічної безпеки підприємства розбудованої із впровадженням цифрових технологій та визначено правову, фінансову, кадрову, інтелектуальну, виробничо-операційну, матеріально-майнову, техніко-технологічну, інноваційно-інвестиційну, інформаційно-цифрову, інтерфейсну, ринкову, фізичну складові системи економічної безпеки, цифровізація якої, на відміну від існуючих, дає можливість автоматизувати, оптимізувати процеси управління, зменшити витрати, забезпечити зростання ефективності та результативності у всіх функціональних сферах діяльності підприємства, як єдиної цілісної системи і

таким чином досягнути зростання рівня стабільності, надійності економічної безпеки підприємства.

8. Розроблено стратегію управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій, яка включає реалізацію стратегічних та оперативних цілей за ключовими напрямками та передбачає цифровізацію процесів здійснення управлінської, операційної, безпекової діяльності підприємства завдяки впровадженню і використанню інноваційних цифрових технологій і дає можливість удосконалити процеси управління, розбудову і функціонування системи та механізму управління економічною безпекою підприємства на сучасному техніко-технологічному рівні, відповідно до вимог та викликів цифрового, техніко-технологічного, ринкового середовищ і забезпечує можливості протидіяти ризикам, загрозам, забезпечувати безпеку, конкурентоспроможність, стійкість і ефективний розвиток підприємства.

9. Сформовано механізм управління системою економічної безпеки підприємства на основі впровадження інноваційних цифрових технологій, який виступає сукупністю елементів, і на відміну від існуючих, забезпечує комплекс дій з розробки та реалізації планів і заходів відповідно до прийнятої стратегії забезпечення економічної безпеки та організації контролю за їх виконанням відповідно до прийнятих стандартів, норм виконання робіт з застосуванням адміністративно-організаційних, оперативно-розпорядчих, економічних, соціально-психологічних, техніко-технологічних методів та їх інструментів, що дає можливість забезпечувати стійкість та формує умови для подальшого ефективного розвитку підприємства завдяки впровадженню інновацій, передових інноваційних цифрових технологій у всіх сферах діяльності та в системі економічної безпеки; забезпечує захист підприємства від внутрішніх та зовнішніх небезпек, загроз; забезпечує утримання ринкових позицій, зростання конкурентоспроможності та подальший розвиток підприємства.

Список використаних джерел:

1. Омелянвич Л. О., Долматова Г. Є. Економічна безпека торговельного підприємства: монографія. Донецьк : ДонДУЕТ, 2005. 195 с.
2. Хома І. Б. Формування та використання систем діагностики економічної захищеності промислового підприємства: монографія. Львів: Вид-во НУ Львівська політехніка, 2012. 504 с.
3. Реверчук Н. Й. Управління економічною безпекою підприємницьких структур : монографія. Львів: ЛБІ НБУ, 2004. 195 с.
4. Алькема В.Г., Літвін Н.М., Кириченко О.С. Економічна безпека інноваційного підприємства: навчальний посібник. Київ: ВНЗ «Університет економіки та права «КРОК», 2015. 320 с.
<https://dspace.krok.edu.ua/handle/krok/79>
5. Дикань В. Л., Назаренко І. Л. Комплексна методика визначення рівня економічної безпеки підприємства: монографія. Харків : УкрДАЗТ, 2011. 142 с.
6. Копитко М. І. Комплексне забезпечення економічної безпеки підприємств (на матеріалах підприємств транспортного машинобудування): дис. ... д-ра екон. наук : 21.04.02. Київ, 2015. 478 с.
7. Шемаєва Л. Г. Забезпечення економічної безпеки підприємства на основі управління стратегічною взаємодією з суб'єктами зовнішнього середовища : монографія. Київ : НІПМБ, 2009. 357 с.
8. Юдіна С., Галаганов В., Стребіж М. (2023). Методичний підхід до управління фінансовою стійкістю підприємства. *Економічний простір*. № 187. С. 178-183. <https://doi.org/10.32782/2224-6282/187-29>
9. Белоусова І. А. Управлінський облік – інформаційна складова системи економічної безпеки підприємства: монографія. Київ: Дорадо-Друк, 2010. 432 с.
10. Андрушків Б. М. Економічна та майнова безпека підприємства і підприємництва. Антирейдерство. Тернопіль: Терно-граф, 2008. 424 с.

11. Єрмошенко М. М., Горячева К. С. Фінансова складова економічної безпеки: держава і підприємство: монографія. Київ : НАУ, 2010. 232 с.
12. Кириленко В. І. Інвестиційна складова економічної безпеки: монографія. Київ: КНЕУ, 2005. 232 с.
13. Фоміна М. В. Проблеми економічно безпечного розвитку підприємств: теорія і практика: монографія. Донецьк: Дон ДУЕТ, 2005. 140 с.
14. Бровкіна Ю. О. Підходи до вивчення поняття економічної безпеки підприємства. 2015. № 1 (17). С. 122–128.
15. Єпіфанов А. О., Пластун О. Л., Домбровський В. С. Фінансова безпека підприємств і банківських установ: монографія. Суми: ДВНЗ УАБС НБУ, 2009. 295 с.
16. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: монографія. Львів : Арал, 2008. 384 с.
17. Козаченко Г. В., Пономарьов В. П., Лященко О. М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія. Київ: Лібра, 2003. 280 с.
18. Корчевська Л. О., Деменська А. М. Концептуальні підходи до визначення економічної безпеки підприємства. *Бізнес-навігатор*. 2011. № 24 (3). С. 40–47.
19. Зайцева І. Ю. Економіко-організаційні основи захисту підприємств автотранспорту від недружніх поглинань: монографія. Харків: УкрДАЗТ, 2011. 427 с.
20. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства: монографія. Луганськ : СНУ ім. В. Даля, 2011. 400 с.
21. Сосновська І. М. Поняття та значення економічної безпеки виробничо-господарської діяльності підприємств. *Ефективна економіка*. 2015. № 9. URL: <http://www.economy.nauka.com.ua>.
22. Донець Л. І., Ващенко Н. В. Економічна безпека підприємства. К.: Центр навчальної літератури, 2008. 240 с.

23. Шнипко О. С. Економічна безпека ієрархічних багаторівневих систем: регіональний аспект. Київ : Генеза, 2006. 288 с.
24. Слободяник Т. М. Запровадження комплексної системи економічної безпеки та оцінка її ефективності на сучасному підприємстві. *Економічний простір*. 2008. № 12/2. С. 22–27.
25. Камлик М.І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект. К.: Атіка, 2005. 432 с.
26. Шульга І. П., Васенко В. К., Пуш Л. А., Зачосова Н. В., Герасименко О.М. Економічна безпека держави, суб'єктів господарювання та тіньова економіка: колективна монографія. Черкаси: Маклаут. Черкаси, 2010. 367 с.
27. Шемаєва Л.Г. Забезпечення економічної безпеки підприємства на основі управління стратегічною взаємодією з суб'єктами зовнішнього середовища : монографія. К. : НШМБ, 2009. 357 с.
28. Живко З. Б., Черевко О. В., Копитко М. І., Зачосова Н. В., Живко М. О., Середа В. В., Занора В.О., Бівець А.В. Економічна безпека держави: навчально-методичний посібник. Черкаси: Чабаненко Ю.А. 2019. 240 с.
29. Іванюта Т. М. Заїчковський А. О. Економічна безпека підприємства. навч. Київ : Центр навч. л-ри, 2009. 256 с.
30. Прохорова В.В., Прохорова Ю.В., Кучеренко О. О. Управління економічною безпекою підприємств: монографія. Харків: УкрДАЗТ, 2010. 282 с.
31. Захаров О. І. Теоретичні основи забезпечення економічної безпеки підприємств. *Вчені записки університету КРОК*. 2012. № 32. С. 80-86.
32. Коробчинський О.Л. Методика формування системи економічної безпеки підприємства. *Актуальні проблеми економіки*. 2009. №. 4 (94). С. 41-45.
33. Андрієнко В.М. Сучасні підходи до забезпечення економічної безпеки будівельних підприємств. *Будівельне виробництво*. 2013. № 55. С. 14-22.

34. Ілляшенко О. В., Погорелов Ю. С. Передумови формування механізму управління системою економічної безпеки підприємства. *Вісник Хмельницького національного університету*. 2015. №4 (2). С. 151-156.
35. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства: монографія. К. : НІСД, 2015. 348с.
36. Ілляшенко С. М. Складники економічної безпеки підприємства і підходи до їх оцінки. *Актуальні проблеми економіки*. 2003. № 3. С. 12-19.
37. Корецький Б. Діагностика економічної безпеки суб'єктів господарювання в транзитивній економіці. *Наукові записки Тернопільського Національного економічного університету*. 2006. №15. С.74-77.
38. Молодід О. О. Характеристика загроз економічної безпеки будівельного підприємства. *Теорія і практика будівництва*. 2009. № 5. С. 54-58.
39. Тулуб О. М. Особливості формування та функціонування системи економічної безпеки інституцій бізнесу та підприємництва за видами економічної діяльності. *Глобальна та національні проблеми економіки*. 2017. № 16. С. 496-498 <http://global-national.in.ua/issue-16-2017/24-vipusk-16-kviten-2017-r/2967>
40. Живко З. Б., Черевко О.В., Зачосова Н.В., Живко М. О., Баворовська О.Б., Занора В.О. Організація та управління системою економічної безпеки підприємства. Черкаси : Чабаненко Ю.А., 2019. 120 с.
41. Зачосова Н. В. Шостак А. В. Концептуальні засади формування комплексної системи забезпечення фінансово-економічної безпеки підприємств та фінансових установ України. *Економіка та держава*. 2016. № 7. С. 80-83.
42. Богдан Н. М. Теоретичні аспекти забезпечення економічної безпеки підприємств будівельного комплексу в процесі взаємодії із зовнішнім середовищем. *Ефективна економіка*. 2012. № 10. С. 18-26.
43. Гнилицька Л. В. Обліково-аналітичне забезпечення функціонування системи економічної безпеки суб'єктів господарювання як

об'єкт наукових досліджень. *Управління проектами та розвиток виробництва*. 2011. № 1(37). С. 142-150.

44. Камлик М. І. Економічна безпека підприємницької діяльності. *Економіко-правовий аспект*. К.: Атіка, 2005. 432 с.

45. Худолій М. Л. Складові економічної безпеки суб'єктів господарської діяльності *Ефективна економіка*. Режим доступу: <http://www.economy.nayka.com.ua/?op=1&z=455>.

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

47. Донець Л. І. Ващенко Н. В. Економічна безпека підприємства. К.: Центр навчальної літератури. 2008. 240 с.

48. Ячменьова В. М. Ідентифікація стійкості діяльності промислових підприємств: монографія. Сімферополь: Доля, 2007. 523 с.

49. Комарницький І.Ф. Бойда С. В., Банар В. Ф. Економічна теорія. Чернівці. 2012. 137 с.

50. Варналій З. С. Економічна безпека. К.: Знання. 2009. 647 с.

51. Єпіфанов А. О., Пластун О. Л., Домбровський В. С. Фінансова безпека підприємств і банківських установ: монографія. Суми : ДВНЗ УАБС НБУ. 2009. 295 с.

52. Васильєв О. В. Формування системи управління економічною безпекою промислових підприємств. *Економічний аналіз*. 2013. Т. 14. № 2. С. 138–145.

53. Зачосова Н. В., Шостак А. В. Концептуальні засади формування комплексної системи забезпечення фінансово-економічної безпеки підприємств та фінансових установ України. *Економіка та держава*. 2016. № 7. С. 80–83.

54. Хіміч О. В. Система управління економічною безпекою підприємства. *Вісник ОНУ імені І. І. Мечнікова*. 2020. Т. 25. №6(85). С. 176-180.

55. Момот Т.О., Філатова І.О., Тофанюк О.В. Економічна безпека корпоративних підприємств будівельної галузі. *Економіка та управління підприємствами машинобудівної галузі: проблеми теорії та практики*. 2011. № 2(14). С. 14-26.
56. Ареф'єва О. В. Конкурентоспроможність підприємств у міжнародному цифровому просторі: монографія. К.: ФОП Маслаков. 2019. 342 с.
57. Тульчинська С. О. Солосіч О.С. Актуальні проблеми підвищення прибутковості комунальних підприємств як фактору економічної безпеки. *Агросвіт*. 2019. № 22. С. 54-59.
58. Тульчинська С. О. Чорній Б. П., Салоїд С. В. Механізм оцінювання залучення інвестиційних ресурсів як засіб забезпечення економічної безпеки промислових підприємств: монографія. К.: Центр навчальної літератури. 2018. 170 с.
59. Рудніченко Є. М. Оцінювання та моделювання впливу суб'єктів митного регулювання на систему економічної безпеки підприємства: монографія Луганськ: Промдрук. 2014. 389 с.
60. Доценко І. О. Сутнісна характеристика функціональних складових економічної безпеки підприємства Режим доступу: <http://elar.khnu.km.ua/jspui/bitstream/123456789/4106/1/Dotsenko.pdf>
61. Шемаєва Л.Г. Забезпечення економічної безпеки підприємства на основі управління стратегічною взаємодією з суб'єктами зовнішнього середовища : монографія. К.: НІШМБ, 2009. 357 с.
62. Чорна М.В. Концептуальна модель економічної безпеки будівельного підприємства. *Ефективна економіка*. 2012. № 10. С. 15-21.
63. Васильєв О. В. Мейта В. І. Формування системи управління економічною безпекою промислових підприємств. *Економічний аналіз*. 2013. Т.14. № 2. С. 138-145.
64. Фоміченко І.П. Формування системи управління економічної безпеки на підприємствах України. *Економіка та управління підприємствами*

машинобудівної галузі: проблеми теорії та практики. 2013. № 3 (23). С. 57-66.

65. Дуб Б. С. Система економічної безпеки підприємства: поняття та структура. *Управління проектами та розвиток виробництва.* 2016. № 4 (60). С. 5-18.

66. Тульчинська С. Чорній В., Солосіч О. Вплив діджиталізації управлінських процесів на систему забезпечення економічної безпеки підприємства. *Інвестиції: практика та досвід.* 2021. № 9. С. 54-58.

67. Шульга І. П., Васенко В. К., Пуш Л. А., Зачосова Н. В., Герасименко О. М. Економічна безпека держави, суб'єктів господарювання та тіньова економіка: колективна монографія. Черкаси: Маклаут. 2010. 367 с.

68. Занора В. О. Недотопа І. Ю. Ризики, загрози, небезпеки, можливості: взаємоузгодження категорій. Економічна безпека України: Тези доповідей учасників Всеукраїнської наук.-практ. конф., 22 квітня 2016 р. Львів: ЛьвДУВС, 2016. С. 105-108.

69. Хринюк О. С. Корчовна М. Р. Система забезпечення економічної безпеки підприємства: основні елементи. *Ефективна економіка.* 2015. № 3. Режим доступу: <http://www.economy.nayka.com.ua/?op=1&z=3927>.

70. Кузенко Т.Б. Планування економічної безпеки підприємства в умовах ринкової економіки: автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 08.06.01. Європейський ун-т фінансів, інформаційних систем, менеджменту і бізнесу. К. 2004. 18 с.

71. Малик О.В. Формування механізму управління фінансовою безпекою підприємства: дисертація канд. екон. наук . 08.00.04 економіка та упр. підприємствами. Хмельницький: ХНУ. 2016. 262 с.

72. Донець Л. І., Ващенко Н. В. Економічна безпека підприємства: навч. посіб. Київ : ЦУЛ. 2008. 240 с.

73. Пригунов П.Я. Особливості використання сучасних концепцій управління в системі забезпечення економічної безпеки підприємств. *Європейські перспективи.* 2013. № 11. С. 103–108.

74. Козаченко Г.В., Ляшенко О. М. Система економічної безпеки: держава, регіон, підприємство: монографія Луганськ: Елтон-2. 2010. 282 с.
75. Франчук В. І. Особливості організації системи економічної безпеки вітчизняних акціонерних товариств в умовах трансформаційної економіки: монографія. Львів: Львівський державний університет внутрішніх справ, 2010. 440 с.
76. Фролов С.М. Управління фінансовою безпекою економічних суб'єктів. Суми : ДВНЗ УАБС НБУ. 2015. 333 с.
77. Овчаренко Є. І. Система економічної безпеки підприємства: формування та цілепокладання: монографія. Лисичанськ: ПромЕнерго, 2015. 483 с.
78. Поляков П. А. Структура системи управління економічною безпекою машинобудівного підприємства. *Вісник Хмельницького національного університету*. 2019. № 2. С. 207-211.
79. Вовк О. М. Управління розвитком системи економічної безпеки підприємства: теоретичне забезпечення. *Приазовський економічний вісник*. 2018. № 6(11). С. 120-124.
80. Рудніченко Є. М. Аналіз нормативного забезпечення системи економічної безпеки підприємств. *Вісник Хмельницького національного університету*. 2013. № 5. т. 1. С. 133-140.
81. Алькема В.Г. Аналіз системи економічної безпеки суб'єктів господарської діяльності. *Фінансова система України*. 2012. № 16. С. 99-107.
82. Данченко О. Б., Поскрипко Ю.А. Стратегічне управління у сфері фінансово-економічної безпеки підприємства: методичні положення щодо забезпечення. *Економіка та суспільство*. 2016. № 6. С. 111-116.
83. Гнилицька Л. В. Обліково-аналітичне забезпечення функціонування системи економічної безпеки суб'єктів господарювання як об'єкт наукових досліджень. *Управління проектами та розвиток виробництва*. 2011. № 1(37). С. 142–150.

84. Ортинський В. Л., Керницький І. С. Економічна безпека підприємств, організацій та установ. К.: Правова єдність. 2009. 544 с.
85. Подра О. П., Лавків Г. Я., Копитко М. І. Теоретичні засади формування системи економічної безпеки підприємства. *Вісник Хмельницького національного університету*. 2019. № 3. С. 136-140
86. Ткаченко В. В., Климчук М. М. Імперативи цифрової економіки в розвитку методології управління підприємством. *Шляхи підвищення ефективності будівництва в умовах формування ринкових відносин*. 2019. Вип. 42. С. 3-18.
87. Струтинська І. В. Малий та середній бізнес у реалізації концепції розвитку цифрової економіки України. *Сталий розвиток економіки*. 2019. № 4[45]. С. 57-63.
88. Тертичний Я. С. Детермінанти впливу цифрового бізнесу на глобальний економічний розвиток. *Економіка і організація управління*. 2016. №4 (24). С. 363– 368.
89. Коляденко С. В. Використання ланцюгів постачання в умовах діджиталізації економіки. *Соціально-економічні проблеми і держава*. 2021. № 25 (2). С. 41– 52.
90. Чиков І. А. Цифрова трансформація економіки: сутність, проблеми, особливості. *Підприємництво та інновації*. 2022. № 25. С. 97 –102.
91. Юрчук Н. П., Кіпоренко С. С. Особливості використання цифрових технологій в агробізнесі. *Східна Європа: економіка, бізнес та управління*. 2022. № 3 (36). С. 109 –116.
92. Солоня О. В. Застосування цифрових технологій в аграрному виробництві. *Техніка, енергетика, транспорт АПК*. 2022. № 3 (118). С. 19 –25.
93. Бурдяк М. І., Томашук І. В. Загальні аспекти застосування цифрових технологій у діяльності аграрних підприємств. *Управління змінами та інноваціями*. 2023. № 7. С.12

94. Лебідь О. Цифрові та інформаційні технології в управлінні підприємством, реальність та погляд у майбутнє. *Економіка та суспільство*. 2023. № 55. <https://doi.org/10.32782/2524-0072/2023-55-19>
95. Програма Європейського Союзу «Цифрова Європа 2021-2027» <https://eufordigital.eu/uk/discover-eu/the-digital-europe-programme/>
96. Цифрова трансформація бізнесу: зміна стратегій і моделей розвитку. Віртуалізація як каталізатор суспільних трансформацій. URL: [https://ndipzir.org.ua/wp-content/uploads/2020/02/Strizhkova19Mono/Strizhkova19Mono%20\(4\).pdf](https://ndipzir.org.ua/wp-content/uploads/2020/02/Strizhkova19Mono/Strizhkova19Mono%20(4).pdf) (дата звернення: 10.10.2024).
97. Лебідь О. В. Цифрова трансформація галузей економіки в Україні у воєнний час. *Економіка, фінанси, менеджмент: актуальні питання науки і практики*. 2022. № 2 (60). С. 141-156.
98. Гбур З. В. Державне управління економічною безпекою України: теорія та практика: монографія. Кам'янець-Подільський: Друкарня Рута. 2018. 408 с.
99. Варналій З. С. Фінансова безпека. Львів : Ліга-Прес. 2018. 300 с.
100. Матвєєва Н. М., Килимник І. І., Коюда О. П. Розвиток суб'єктів економічної діяльності в умовах цифрової економіки: матеріали всеукр. наук.-практ. конф., Харків, 25–27 листопада 2020 року. Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова та ін. Харків : ХНУМГ ім. О. М. Бекетова, 2020. 121 с.
101. Гуржій Н., Гавран В., Сапотницька Н. Цифрові технології та їхній вплив на управління логістичними процесами підприємств. *Економіка та суспільство*. 2023. № 55. <https://doi.org/10.32782/2524-0072/2023-55-20>
102. Маргасова В., Самойлович О. Роль цифрових технологій в організації ефективного функціонування маркетингової та логістичної систем промислового підприємства. *Проблеми і перспективи економіки та управління*. 2023. № 2 (34). С. 26–37.
103. Васильців Т. Г., Волошин В. І., Бойкевич О. Р., Каркавчук В. В. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія. Львів: Ліга-Прес 2012. 386 с.

104. Давиденко С.В., Єгорова О.О., Приходько В.П. Економіка та економічна безпека держави. Теорія і практика. Ужгород: РІК-У, 2017. 383 с.
105. Птащенко Л.О. Стратегічне та інноваційне забезпечення розвитку системи економічної безпеки підприємства. Київ: Центр учбової літератури. 2018. 320 с.
106. Соломіна Г.В., Забезпечення фінансово-економічної безпеки підприємництва. Дніпро : ДДУВС. 2018. 234 с
107. Олифіренко Ю., Повна С., Біланенко, О. Цифровий маркетинг і логістика в адаптивному управлінні інноваційним розвитком підприємства. Науковий вісник Полісся. 2022. № 2 (25). С. 240–250.
108. Дідик А.М. Економічна безпека підприємства : підручник. Львів : Львівська політехніка. 2019. 624 с
109. Васильців Т.Г., Лупак Р.Л., Зайченко В.В. Економічна безпека та фінансові розслідування: концепти, прагматика, інструментарій забезпечення. Тернопіль : ТНЕУ. 2019. 394 с.
110. Попело О. В., Ткаченко Т. П. Стратегія ефективного функціонування логістичної системи підприємства в контексті забезпечення економічної безпеки. *Economic Synergy*. 2023. № 2. С. 23–35.
111. Мігус І.П. Лаптев С.М. Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання. *Ефективна економіка*. 2011. № 12. Режим доступу: http://nbuv.gov.ua/UJRN/efek_2011_12_5
112. Погосова М.Ю. Структурно-логічний аналіз поняття фінансова безпека підприємства. *Наука й економіка*. 2008. № 3. С. 258–263.
113. Больботенко І.В. Методичні засади організації системи економічної безпеки суб'єктів аудиторської діяльності. *Вчені записки університету КРОК*. 2014. № 36. С. 204–211.
114. Коробчинський О.Л. Методика формування системи економічної безпеки підприємства *Актуальні проблеми економіки*. 2009. №. 4 (94). С. 41-45.

115. Мігус І.П. Методологічний підхід до оцінки стану системи економічної безпеки акціонерних товариств. *Ефективна економіка*. Режим доступу: <http://www.economy.nauka.com.ua/?op=1&z=2571>.
116. Васенко В. К., Пуш Л. А., Шульга І. П., Зачосова Н. В., Герасименко О. М. Економічна безпека держави, суб'єктів господарювання та тіньова економіка: колективна монографія. Черкаси : Маклаут. 2010. 367 с.
117. Веретенникова Г. Б. Економічна безпека підприємства: планування й організація : конспект лекцій. Х. : ХНЕУ. 2008. 83 с.
118. Герасименко О. М. Індикатори оцінки стану системи економічної безпеки торговців цінними паперами : монографія. Черкаси : Маклаут. 2011. 250 с.
119. Губарев О. О. Економічна безпека: конспект лекцій. Х. : ХНЕУ. 2007. 59 с.
120. Живко З.Б. Механізм управління системою економічної безпеки підприємства. *Науковий вісник Ужгородського університету*. 2014. № 3 (44). С. 37–42.
121. Захаров О.І. Теоретичні основи забезпечення економічної безпеки підприємств. *Вчені записки університету КРОК*. 2012. № 32. С. 80–86.
122. Ілляшенко О. В. Механізм системи економічної безпеки підприємства: монографія. Харків : Мачулін, 2016. 503 с.
123. Копитко М. І. Економічна безпека підприємств з виробництва транспортних засобів: монографія. К.: ВНЗ Університет економіки та права КРОК. 2015. 573 с.
124. Живко З. Б. Чернобай Л. І., Чернобай Д. А. Ідентифікування ризиків при мотивуванні персоналу підприємства. *Науковий вісник ЛьвДУВС*. 2017. №. 2. С. 179-189.
125. Іванілов О. С. Економіка підприємства: К.: Центр учбової літератури. 2009. 728 с.

126. Воронко Р. М., Редченко К. І., Бурдик О. Ю. Роль внутрішнього контролю в системі управління торговельним підприємством. *Підприємництво і торгівля*. 2023. № 35. С. 11–20.
127. Хаустова В. Є., Решетняк О. І., Хаустов М. М., Зінченко В. А. Аналіз розвитку ІКТ-сфери в Україні за міжнародними індексами та рейтингами. *Бізнес інформ*. № 5.2022. С. 40-56
128. Трушкіна Н. В., Джвігол Х., Сергеева О., Шкригун, Ю. Розвиток концепції Логістика 4.0 в умовах цифрової економіки. *Економічний вісник Донбасу*. 2021. № 4 (62). С. 85-96.
129. Zadorozhnyi Z.M. Innovative accounting methodology of ensuring the interaction of economic and cybersecurity of enterprises. *Marketing and Management of Innovations*. 2021. Vol. 5, no. 4. P. 36–46.
130. Manzhula V., Semanyuk V., Rozhelyuk V. Evaluation Method of Economic Benefit Taking Into Account Additional Data in Decision-Making Process. 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic. 5–7 June 2019. 2019. DOI: <https://doi.org/10.1109/acitt.2019.8779982>
131. Аналітика Big Data підвищує масштабованість логістичних послуг. BigDataLab. URL: <https://www.bigdatalab.com.ua/news-116/> (дата звернення: 12.10.2024).
132. Management of Domestic Marketing of Service Enterprises / S. Radev Koev et al. IBIMA Business Review. 2019. P. 1–13. DOI: <https://doi.org/10.5171/2019.681709> (date of access: 12.10.2024).
133. Живко З. Б. Забезпечення системи економічної безпеки підприємства як об'єкта управління. Актуальні проблеми забезпечення економічної безпеки в Україні : колективна монографія .Львів : Ліга-Прес, 2017. С. 292-307.
134. Бойда С. Інноваційні підходи до управління підприємствами в умовах діджиталізації економіки. *Економіка та управління підприємствами*. 2022 . №85. С. 72 –81.

135. Використання інформаційно-комунікаційних технологій на підприємствах. Офіційний сайт Державної служби статистики України. URL: <http://www.ukrstat.gov.ua> (дата звернення: 22.11.2024).

136. Діджиталізація: спосіб розвитку бізнесу. URL: <https://ua.scallium.pro/what-is-digital> (дата звернення: 21.11.2024).

137. Дубина М. В., Козлянченко О. М. Концептуальні аспекти дослідження сутності діджиталізації та її ролі в розвитку сучасного суспільства. *Проблеми і перспективи економіки та управління*. №3 (19). 2019. С. 21–31.

138. Жосан Г. Стан розвитку діджиталізації в Україні. *Економічний аналіз*. 2020. Том 30. № 1. Частина 2. С. 44–52.

139. Іляшенко С.М., Іляшенко Н.С. Цифровізація як перспективний напрямок інноваційного розвитку економіки України. III Міжнародна науково-практична конференція: Бізнес, інновації, менеджмент: проблеми та перспективи. Київ. 2022. С. 172–173.

140. Клименко К.В. Діджиталізація як інноваційний розвиток підприємств: досвід України. *Вісник Хмельницького національного університету*. 2020. № 4. Том 3. С. 13–18.

141. Іванов С. В., Ляшенко В. І., Шамілева Л. Л., Трушкіна Н. В. Тенденції розвитку транспортно-логістичної системи Придніпровського економічного району. *Вісник економічної науки України*. 2019. № 2 (37). С. 143–150.

142. Єфремова К. В., Шматков Д. І., Кохан В. П. Базові аспекти цифровізації та їх правове забезпечення: монографія. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. 180 с

143. Zaloznova Y., Trushkina N. Scientific and methodological support of improvement of the management system of logistic activities of the enterprise. *Economic innovations*. 2018. Vol. 20, no. 3(68). P. 57–67.

144. Тенденції використання Інтернету у світі. URL: <https://zhuk.ua/istoriyi-ta-fakty/tendentsii-vikoristann-ya-internetu-u-sviti/> (дата звернення: 11.10.2024)
145. Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу "Цифрова Європа" (2021–2027). URL: <https://ips.ligazakon.net/document/MU22050> (дата звернення: 11.10.2024).
146. Краус Н. М., Голобородько О. П., Краус К. М. Цифрова економіка: тренди та перспективи авангардного характеру розвитку. *Ефективна економіка*. 2018. № 1. URL: <http://www.economy.nayka.com.ua/?op=1&z=6047> (дата звернення: 03.01.2025).
147. Айзексон В. Інноватори: як група хакерів, геніїв та гіків здійснила цифрову революцію. Київ. Наш формат. 2017. 488 с.
148. Криворучко О. С. Краус Н. М., Краус К. М. Інноваційний портрет європейського економічного простору. *Інфраструктура ринку*. 2017. № 3. Режим доступу до ресурсу: <http://market-infr.od.ua/uk/3-2017>.
149. Криворучко О. С. Краус Н. М., Краус К. М. “Інноваційний ландшафт” у координатах світ-економіки. *Глобальні та національні проблеми економіки*. 2017. № 16. Режим доступу: <http://www.global-national.in.ua/issue-16-2017>.
150. Цифрова адженда України – 2020. “Цифровий порядок денний” 2020. Концептуальні засади (версія 1.0). Першочергові сфери, ініціативи, проекти “цифровізації” України до 2020 року. К.: NITECH office. 2016. 90 с. Режим доступу: <https://uccr.org.ua/uploads/files/58e78ee3c3922.pdf>.
151. Краус Н. М. Інституціоналізація інноваційної економіки: глобальні та національні тенденції : автореф. дис. на здобуття наук. ступеня докт. економ. наук : спец. 08.00.01 Економічна теорія та історія економічної думки. К. : Знання, 2017. 40 с.
152. Краус Н. М., Краус К. М. Інноваційне табло України. *Східна Європа: економіка, бізнес та управління*. 2017. № 6. <http://www.easterneurope-ebm.in.ua/62017-ukr>.

153. Negroponte, N. Being Digital. NY : Knopf, 1995. 256 p.
154. Голобородько А. Ю. Цифрова економіка: підходи та особливості розвитку. *Бізнес Інформ*. 2022. №9. С. 10–18. <https://doi.org/10.32983/2222-4459-2022-9-10-18>
155. Tapscott, D. The Digital Economy: Promise and Peril In The Age of Networked Intelligence. NY : McGraw-Hill, 1994. 368 p.
156. Войнаренко М. П., Скоробогата Л. В. Мережеві інструменти капіталізації інформаційно інтелектуального потенціалу та інновацій. *Вісник Хмельницького національного університету*. 2015. № 3. Т. 3. С. 18–24.
157. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. *Вісник Дніпропетровського університету*. 2015. №. 4. С. 9–18.
158. Lane, N. Advancing the digital economy into the 21st century. *Information Systems Frontiers*. 1999. Vol. 1. No. 3. P. 317–320.
159. Kane G. C. et al. Strategy, Not Technology, Drives Digital Transformation. *Becoming a Digitally Mature Enterprise*. Cambridge, MA: MIT Sloan Management School; Deloitte, 2015. 630 p.
160. Mesenbourg T. L. Measuring the Digital Economy // U.S. Bureau of the Census. URL: <https://www.census.gov/content/dam/Census/library/working-papers/2001/econ/digitalecon.pdf>
161. Коляденко С. В. Цифрова економіка: передумови та етапи становлення в Україні і у світі. *Економіка. Фінанси. Менеджмент: актуальні питання науки і практики*. 2016. № 6. С. 105–112.
162. Карчева Г. Т., Огородня Д. В., Опенько В. А. Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. *Фінансовий простір*. 2017. № 3. С. 13–21.
163. Dahlman, C., Mealy S., Wermelinger M. Harnessing the Digital Economy for Developing Countries: *Working Paper*. No. 334. Paris: OECD. 2016. OECD URL: <http://www.oecd-ilibrary.org/docserver/download/4adffb24-en.pdf>

164. Матвейчук Л. О. Цифрова економіка: теоретичні аспекти. *Вісник Запорізького національного університету*. 2018. № 4. С. 116–127.
165. Гриценко О. А. Цифрова економіка: сучасні виклики для економістів та правознавців. *Економічна теорія та право*. 2018. № 2. С. 77–90.
166. Малюта Л. Я., Дерманська Л. В. Інноваційно-цифрові перспективи розвитку економіки України. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. 2019. Т. 30. № 2. С. 55–60.
167. Кузнєцова А. Я., Чмерук Г. Г. Теоретичні підходи до визначення цифрової економіки. *Проблеми системного підходу в економіці*. 2019. №. 6. С. 34–41.
168. Фіщук В. Цифрова економіка – це реально. НВ. Бізнес. URL: <https://biz.nv.ua/ukr/experts/tsifrova-ekonomika-tse-realno-1001102.html>
169. Цифрова адженда України – 2020»: проект. Концептуальні засади (версія 1.0). 2016. URL: <https://uccr.org.ua/uploads/files/58e78ee3c3922.pdf>
170. Марченко О. Цифрова економіка в Україні: основні тенденції та перспективи розвитку. *Галицький економічний вісник*. 2020. Т. 65. № 4. С. 34–39.
171. Сірко А. В. Реалії цифрової економіки: нові можливості та виклики для суспільства і держави. *Ефективна економіка*. 2020. № 11. DOI: 10.32702/2307-2105-2020.11.15
172. Україна 2030 Е-країна з розвинутою цифровою економікою. Український інститут майбутнього. URL: <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html>
173. Василенко В. Ю., Буряк А. М. Безпека даних в епоху цифрової трансформації: проблеми та виклики. *Інформація та соціум*. 2024. №10. С. 103-106.
174. Чайковська І., Ткач Т., Чайковський М. Роль сучасних інформаційних систем та технологій у забезпеченні економічної безпеки

підприємства в умовах DIGITAL-економіки. *Вісник Хмельницького національного університету*. 2024. № 3. С. 424-430.

175. Рудніченко Є. М., Гавловська Н. І., Суходоля С. А., Лісовський І. В., Ядуча С. Й. Цифрова економіка та її вплив на розвиток організацій. *Вісник Хмельницького національного університету*. 2020. № 4. Т. 1. С.172-176.

176. Панченко О. А. Інформаційні технології в забезпеченні державної безпеки. *Science Review*. 2020. № 5(32). С. 30-35

177. Britchenko I., Voitovych S., Lošonczi P., Lorvi I., Kulyk I., Begun S. Modern information and communication technologies in the Digital economy in the system of economic security of the enterprises. Shmatkovska. *AD ALTA: Journal of Interdisciplinary Research*. 2022. P.153-156.

178. Kukhar O., Kravchyk Y., Brechko O. Digital transformation as a factor in ensuring economic security of enterprises. *Baltic Journal of Economic Studies*. 2023. Vol. 9. № 5. P. 143-152.

179. Чайковська І.І., Лук'янова В.В., Чайковський М.Ю. Розробка моделі інформаційної системи управління знаннями на проєктноорієнтованому підприємстві. *Modeling the development of the economic systems*. 2023. №2. С. 153-158.

180. Дикань В., Фролова Н., Пань Цзян. Забезпечення економічної безпеки малого та середнього бізнесу в умовах цифровізації. *Інфраструктура ринку*. 2021. №. 62. С.21-27.

181. Решетов С. Полусмяк Ю. Вплив цифрової трансформації економіки на економічну безпеку. *Management and entrepreneurship: trends of development*. 2020. № 4 (22). P. 8-16.

182. Gonchar V. Polupanova K. Development of economic security of enterprises in the conditions of transformations. *Public Security and Public Order*. 2022. № 29. P. 44-58.

183. Samoilenko Y., Britchenko I., Levchenko L., Lošonczi P., Bilichenko O., Bodnar O. Economic Security of the Enterprise Within the Conditions of Digital Transformation. *Economic affairs*. 2022. № 67(04). P. 619-629.

184. Мельничук Г., Мамалига В. Цифровізація економіки: можливості та загрози для ефективного функціонування підприємств. *Приазовський економічний вісник*. 2020. № 2 (19). С. 125–130.
185. Касьянова Н. В., Біличенко М. М., Севериненко А. О. Моделювання цифрової безпеки підприємства. *Modern Economics*. 2023. № 39. С. 54-61.
186. Саврук М. В. Актуальність проблеми забезпечення інформаційної безпеки України та шляхи її розв'язання системи обробки інформації. *Системи обробки інформації*. 2010. № 3 (84). С. 77-79.
187. Передерій Т. Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. *Вісник економічної науки України*. 2019. № 2 (37). С. 201–204.
188. Краус К., Краус Н., Штепа О. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. № 3. С. 26–37.
189. Чайковська І. І., Ткач Т. І., Поперечний Б. А. Трансформація ролі людського капіталу в умовах Digital-економіки. *Modeling the development of the economic systems*. 2024. №1. С. 189-194.
190. Проскура В., Черничко Т., Верецький Д. Сучасні підходи до визначення рівня економічної безпеки підприємства в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2024. №4 (13). С. 61-67.
191. Ткачук Г. О. «Цифрові» трансформації: взаємозв'язок із системою економічної безпеки підприємства. *Економіка харчової промисловості*. 2019. Том 11. № 4. С. 42–50.
192. Аванесова Н.Е., Мордовцев О.С., Колодяжна Т.В. Формування механізму комплексного забезпечення цифрової безпеки промислового підприємства України. *Вісник НТУ «ХПІ»*. 2020. № 3. С. 9-14.
193. Дуляба Н., Обрамич О. Теоретичні засади дослідження сутності цифрової безпеки. *Економіка та суспільство*. 2023. № 55. <https://doi.org/10.32782/2524-0072/2023-55-66>

194. UNCTAD: eCommerce Week 2019: From Digitalization to Development. 01-05 April 2019, Palais des Nations, Geneva, Switzerland. URL: <https://unctad.org/meeting/ecommerce-week-2019-digitalization-development>
195. Алькема В.Г., Сумець О. М. Інтегрована модель комунікативного управління персоналом ІТ-компаній в умовах кадрових ризиків. *Економіка та суспільство*. 2025. № 75. DOI <https://doi.org/10.32782/2524-0072/2025-75-16>
196. Онешко С. В., Вітер С. А., Вірмейчик А. М. Стратегія розвитку аудиту в умовах цифрової економіки. *Інвестиції: практика та досвід*. 2021. № 15. С. 64–69. DOI: 10.32702/2306-6814.2021.15.64
197. Онешко С., Башлай С., Короленко О. Особливості збереження та підтримання економічного потенціалу України в умовах війни. *Економіка та суспільство*. 2022. № 40. DOI: <https://doi.org/10.32782/2524-0072/2022-40-4>
198. Пищуліна О. Цифрова економіка: тренди, ризики та соціальні детермінанти : доповідь. 2020. Київ : Razumkov center. 274 с.
199. Шостак Л., Більо І., Микитюк Є. Потенціал цифровізації вітчизняного бізнес-середовища. *Економічний аналіз*. 2021. Том 31. № 1. С. 245–251.
200. Варіс І., Кравчук О., Парашук Ю. Цифровізація бізнес-процесів менеджменту персоналу: можливості HRM систем. *Галицький економічний вісник*. 2022. № 74(1). С. 90-102.
201. Кириченко О. Управління системою економічної безпеки підприємств, банківських установ та оцінювання їх ділової репутації із застосуванням інформаційно-аналітичного забезпечення, цифрових технологій. *Вчені записки Університету КРОК*. 2025. № 2(78). С. 185-192. DOI <https://doi.org/10.31732/2663-2209-2025-78-185-192>
202. Длугопольська Т., Гук Ю. Цифрова трансформація у сфері HR: напрями, проблеми та можливості. *Причорноморські економічні студії*. 2021. № 62. DOI: <https://doi.org/10.32843/bses.62-2>.

203. Добринін А. П. Цілісна модель трансформації в цифровій економіці – як стати цифровими лідерами. *International Journal of Open Information Technologies*. 2017. т. 5. № 1. С. 16-28.

204. Кириченко О. Інформаційно-аналітичні, репутаційні, цифрові, технологічні аспекти управління системою економічної безпеки підприємств, банківських установ, їх вплив та оцінювання. *Вчені записки Університету КРОК*. 2025. № 1(77). С. 203-210. DOI <https://doi.org/10.31732/2663-2209-2025-77-203-210>

205. Вишневський В.П. Смарт-промисловість в епоху цифрової економіки: перспективи, напрями і механізми розвитку: монографія. Київ: НАН України, Ін-т економіки пром-ті. 2018. 192 с.

206. Вишневський В.П., Князєв С.І. Як підвищити готовність промисловості України до смарт трансформацій. *Наука та інновації*. 2018. Т. 14. № 4. С. 55-69.

207. Куйбіда В.С., Петроє О.М., Федулова Л.І., Андрощук Г.О. Цифрові компетенції як умова формування якості людського капіталу. Київ : НАДУ, 2019. 28 с.

208. Алькема В. Діденко В. Цифровізація інформаційно-аналітичного забезпечення управління інноваційною діяльністю, інноваційним розвитком підприємств. *Вчені записки Університету КРОК*. 2024. № 3(75). С. 85-92. DOI <https://doi.org/10.31732/2663-2209-2024-75-85-92>

209. Про рішення Ради національної безпеки і оборони України від 14.09.2020 р. «Про Стратегію національної безпеки України», введено в дію Указом Президента України № 392/2020 від 14.09.2020 р. URL: <https://www.president.gov.ua/>

210. Алькема В.Г. Принципи управління інформаційно-аналітичним забезпеченням та цифровізацією системи економічної безпеки підприємств, банківських установ. *Бізнес-навігатор*. 2025. № 6 (83). С. 142-146.

211. Мехед А. М., Варналій З. С. Фінансова безпека підприємства в умовах цифрової економіки. *Socio-Economic Relations in the Digital Society*. 2021. № 3(42). С. 55-61.
212. Чайкіна А., Маслій О., Черв'як А. Сучасні драйвери підвищення економічної безпеки в умовах цифрової трансформації. *Сталий розвиток економіки*. 2024. №2(49). С. 307-313.
213. Брюховецька Н.Ю., Черних О.В. Індустрія 4.0 та цифровізація економіки: можливості використання зарубіжного досвіду на промислових підприємствах України. *Економіка промисловості*. 2020. № 2 (90). С. 116–132.
214. Industry 5.0, a transformative vision for Europe. URL: <https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/38a2fa08-728e-11ec-9136-01aa75ed71a1>
215. Храпкіна В.В., Устименко В.А. Детермінанти сталого розвитку економіки : монографія. Київ : Інтерсервіс. 2019. 264 с.
216. Пищуліна О. Цифрова економіка: тренди, ризики та соціальні детермінанти: доповідь. 2020. Київ: Razumkovcenter. 274 с.
217. Рекомендації ініціативи “Вирівнювання політики інтеграції до Єдиного цифрового ринку ЄС та гармонізації цифрових ринків СхП” Центр розвитку інновацій. <https://cid.center/wp-content/uploads/2022/01/https://lpnu.ua/sites/default/files/2022/3/27/paragraphs/39476/metodichka-skhp.pdf>
218. Dong Q. J. Moving a Mountain with a Teaspoon: Toward a Theory of Digital Entrepreneurship in the Regulatory Environment. *Technological Forecasting and Social Change*. 2019. Vol. 146. P. 923–930.
219. Galindo-Martin M.A., Castano-Martinez M.S., Mendez-Picazo M.T. Digital Transformation, Digital Dividends and Entrepreneurship: A Quantitative Analysis. *Journal of Business Research*. 2019. Vol. 101(C). no. 146. P. 522–527.
220. Wong, Chu. Digital Governance as Institutional Adaptation and Development: Social Media Strategies between Hong Kong and Shenzhen. *China Review*. 2020. Aug. Vol. 20, no. 3. P. 43-70.

221. Bretschneider S.I., Mergel I. Technology and Public Management Information Systems: Where we have been and where we are going. The state of public administration: issues, challenges, and opportunities. 1st ed. London: Routledge Taylor Francis Group. 2015. P. 187-203.

222. Mergel, Edelmann, Haug. Defining digital transformation: Results from expert interviews. *Government Information Quarterly*. 2019. Oct. Vol. 36, no. 4. P. 101-385

223. Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному? URL: http://eap-csf.org.ua/wp-content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf

224. Шило Ж.С. Методи оцінки рівня економічної безпеки підприємства: підходи до оцінювання та забезпечення економічної безпеки. *Вісник НУБГП*. 2022. № 2(98). С. 278-288. URL: <https://ep3.nuwm.edu.ua/24406/1/Ve9824%20%281%29.pdf9>.

225. Щодо вдосконалення методології інтегрального оцінювання рівня економічної безпеки України. Аналітична записка. Національний інститут стратегічних досліджень. 2013. URL: <https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/schodo-vdoskonalennya-metodologii-integralnogo-ocinyuvannya-rivnya>

226. Єфремова К.В. Новітні вимоги до розрахунку рівня економічної безпеки України під впливом цифровізації. 2023. URL: https://ndipzir.org.ua/wp-content/uploads/2023/04/conf_21.04.2023.pdf#page=25

227. Чайкіна А.О. Індустрія 4.0: особливості цифрової трансформації України. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. 2021. Т. 32 (71). С. 24–31.

228. Череп А., Череп О., Гельман В., Лосева Е. Європейські вектори цифровізації економіки задля забезпечення національної безпеки держави. *Молодий вчений*. 2023. № 11 (123). С. 163–167.

229. Onyshchenko V., Onyshchenko S., Maslii O., Maksymenko A. Systematization of Threats to Financial Security of Individual, Society, Business and the State in Terms of the Pandemic. In International Conference BUILDING INNOVATIONS. 2022. P. 749–760.

230. Бєлобородова М.В. Економічна безпека суб'єктів підприємництва в умовах переходу до цифрової економіки. *Актуальні аспекти розвитку суб'єктів підприємництва в умовах глобальної економіки*. 2021. №3. С. 349–358.

231. Ситнік Є. Концептуальні засади та наукові підходи до розуміння поняття сутності економічної безпеки підприємства. *Вчені записки Університету КРОК*. 2024. № 4 (76). С. 249–255.

232. Ситнік Є. Теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства. *Вчені записки Університету КРОК*. 2025. № 1(77). С. 371–378.

233. Ситнік Є.І. Сутність та наукові підходи до визначення поняття економічної безпеки підприємства. Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2024: тези доповідей науково-практичної конференції (квітень, 2024р). Київ: Університет "КРОК» 2024 <https://conf.krok.edu.ua/MMO/MMO-2024/paper/view/2127>

234. Ситнік Є.І. Наукові підходи до розбудови системи економічної безпеки підприємства. Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку- 2024: тези доповідей науково-практичної конференції (грудень, 2024р). Київ: Університет "КРОК", 2024 <https://conf.krok.edu.ua/SRE/SRE-2024/paper/view/2362>

235. Матеріали офіційного сайту Державної служби статистики України. [Електронний ресурс]. Режим доступу: <http://www.ukrstat.gov.ua>.

236. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України: наказ Міністерства економічного

розвитку і торгівлі України № 1277 від 29 жовтня 2013 року [Електронний ресурс]. http://cct.com.ua/2013/29.10.2013_1277.htm.

237. Ситнік Є. Аналіз та ідентифікація показників впровадження цифрових технологій в забезпеченні економічної безпеки підприємств. *Вчені записки Університету КРОК*. 2025. №3(79). С. 351–359. <https://doi.org/10.31732/2663-2209-2025-79-351-359>

238. Ситнік Є. І. Управління системою економічної безпеки підприємства. Тези доповідей міжнародної наукової конференції. Сілезька академія. Катовіце. (19-20 вересня 2023) Катовіце. 2023 https://scholar.google.com.ua/citations?view_op=view_citation&hl=uk&user=hveUsecAAAAJ&citation_for_view=hveUsecAAAAJ:u-x6o8ySG0sC

239. Ситнік Є. І. Поняття цифрової безпеки як складової економічної безпеки підприємства. Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2025: тези доповідей міжнародної науково-практичної конференції (квітень, 2025 р.). Київ: Університет "КРОК", 2025 <https://conf.krok.edu.ua/MMO/MMO-2025/paper/view/2851>

240. «Про затвердження порядку застосування ризик-орієнтованого підходу в Бюро економічної безпеки України» Бюро економічної безпеки Наказ № 36 від 01.02.2023 <https://zakon.rada.gov.ua/laws/show/z0350-23#Text>

241. ДСТУ ISO 9001:2015 Системи управління якістю. Вимоги (ISO 9001:2015, IDT) https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=64013

242. Матеріали офіційного сайту Ради національної безпеки і оборони України[Електронний ресурс]. Режим доступу : <http://www.rnbo.gov.ua>.

243. Матеріали сайту Національного інституту стратегічних досліджень при Президентові України [Електронний ресурс]. Режим доступу: <http://www.niss.gov.ua>.

244. Ситнік Є. Науково-практичні аспекти розбудови та управління системою економічної безпеки підприємства на основі інноваційних цифрових

технологій. *Вчені записки Університету КРОК*. 2025. № 2(78). С. 390–397.
<https://doi.org/10.31732/2663-2209-2025-78-390-397>

245. Ситнік Є. Обґрунтування стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій. *Сталий розвиток економіки*. 2025. № 56. С. 302-306.
<https://doi.org/10.32782/2308-1988/2025-56-41>

246. Ситнік Є.І. Впровадження інноваційних цифрових технологій в забезпеченні економічної безпеки підприємства. *Economics, accounting, finance and management: strategic priorities for development in the context of globalization: тези доповідей Міжнародної науково-практичної конференції (21 березня 2025)*. Tampere, Finlan. 2025. С. 21-23. <https://www.economics.in.ua/2025/03/21-2025.html>

247. Ситнік Є.І. Показники використання цифрових технологій в забезпеченні економічної безпеки підприємств. *Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку- 2025: тези доповідей науково-практичної конференції (грудень, 2025р)*. Київ: Університет "КРОК", 2025.
<https://conf.krok.edu.ua/SRE/SRE-2025/paper/view/3169> (0,25 д.а.).

248. Ситнік Є.І. Впровадження управління системою економічної безпеки підприємства та основі інноваційних цифрових технологій. *Національна економіка в умовах війни: безпека та розвиток: тези Всеукраїнської науково-практичної конференції (14 листопада 2025 року)*. Львів: Львівський державний університет внутрішніх справ, 2025. С.407-410.(0,25 д.а.).

ДОДАТКИ

ДОДАТОК А.1

Список публікацій здобувача,

в яких опубліковані основні наукові результати дисертації:

1. Ситнік Є. Концептуальні засади та наукові підходи до розуміння поняття сутності економічної безпеки підприємства. Вчені записки Університету «КРОК». 2024. № 4 (76). С. 249–255. <https://doi.org/10.31732/2663-2209-2024-76-249-255> (0,8 д. а).
2. Ситнік Є. Теоретичні основи впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства. Вчені записки Університету «КРОК». 2025. № 1(77). С. 371–378. <https://doi.org/10.31732/2663-2209-2025-77-371-378> (1 д. а).
3. Ситнік Є. Науково-практичні аспекти розбудови та управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій. Вчені записки Університету «КРОК». 2025. № 2(78). С. 390–397. <https://doi.org/10.31732/2663-2209-2025-78-390-397> (1 д. а).
4. Ситнік Є. Аналіз та ідентифікація показників впровадження цифрових технологій в забезпеченні економічної безпеки підприємств. Вчені записки Університету «КРОК». 2025. №3(79). С. 351–359. <https://doi.org/10.31732/2663-2209-2025-79-351-359> (1 д. а).
5. Ситнік Є. Обґрунтування стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій. Сталий розвиток економіки. 2025. № 56. С. 302-306. <https://doi.org/10.32782/2308-1988/2025-56-41> (0,7 д. а).

які засвідчують апробацію матеріалів дисертації:

6. Ситнік Є.І. Сутність та наукові підходи до визначення поняття економічної безпеки підприємства. Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2024: тези доповідей науково-практичної конференції (квітень, 2024 р). Київ: Університет "КРОК» 2024. <https://conf.krok.edu.ua/MMO/MMO-2024/paper/view/2127> (0,25 д. а).

7. Ситнік Є.І. Наукові підходи до розбудови системи економічної безпеки підприємства. Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку- 2024: тези доповідей науково-практичної конференції (грудень, 2024 р.). Київ: Університет "КРОК", 2024. <https://conf.krok.edu.ua/SRE/SRE-2024/paper/view/2362> (0,25 д. а).

8. Ситнік Є. І. Поняття цифрової безпеки як складової економічної безпеки підприємства. Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2025: тези доповідей міжнародної науково-практичної конференції (квітень, 2025 р.). Київ: Університет "КРОК", 2025. <https://conf.krok.edu.ua/MMO/MMO-2025/paper/view/2851> (0,25 д. а).

9. Ситнік Є.І. Впровадження інноваційних цифрових технологій в забезпеченні економічної безпеки підприємства. Economics, accounting, finance and management: strategic priorities for development in the context of globalization: тези доповідей Міжнародної науково-практичної конференції (березень, 2025 р.). Tampere, Finlan. 2025. С. 21-23. <https://www.economics.in.ua/2025/03/21-2025.html> (0,25 д. а).

10. Ситнік Є.І. Показники використання цифрових технологій в забезпеченні економічної безпеки підприємств. Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку- 2025: тези доповідей науково-практичної конференції (грудень, 2025 р.). Київ: Університет "КРОК", 2025. <https://conf.krok.edu.ua/SRE/SRE-2025/paper/view/3169> (0,25 д.а.).

11. Ситнік Є.І. Впровадження управління системою економічної безпеки підприємства та основі інноваційних цифрових технологій. Національна економіка в умовах війни: безпека та розвиток: тези Всеукраїнської науково-практичної конференції (листопад, 2025 р.). Львів: Львівський державний університет внутрішніх справ, 2025. С.407-410.(0,25 д.а.).

ДОДАТОК А2

Відомості про апробацію результатів дисертації

1. Наукова конференція: «Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2024» (2024 р., Київ, Україна; участь онлайн);
2. Наукова конференція: «Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку 2024» (2024 р., Київ, Україна; участь онлайн);
3. Наукова конференція: «Сучасний менеджмент організації: витоки, реалії та перспективи розвитку 2025» (2025 р., Київ; участь онлайн);
4. Наукова конференція: «Economics, accounting, finance and management: strategic priorities for development in the context of globalization» (2025 р., Tampere, Finlan; участь онлайн).
5. Наукова конференція «Держава, регіони, підприємництво: інформаційні, суспільно-правові, соціально-економічні аспекти розвитку 2025» (2025 р., Київ, Україна; участь онлайн);
6. Міжнародна наукова конференція «Національна економіка в умовах війни: безпека та розвиток» (2025 р., Львів, Україна; участь онлайн).

ДОДАТОК Б.1.
ДОВІДКИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОГО
ДОСЛІДЖЕННЯ

"LEVI9 UKRAINE" Ltd.

01033 Kyiv, Ukraine
Volodymyrska Street, 101/1
Phone: +38 044 594 88 38
info@levi9.com
www.levi9.com



ТОВ "ЛЕВІ9 УКРАЇНА"

01033, м. Київ, Україна
вул. Володимирська, 101, корпус 1(Літ.3)
+38 044 594 88 38
info@levi9.com
www.levi9.com

Вих. № 29/9

Від 29 вересня 2025р.

ДОВІДКА

про впровадження результатів дисертації

на здобуття наукового ступеня

**доктора філософії в галузі знань 07 «Управління та адміністрування», за
спеціальністю 073 «Менеджмент»**

Ситніка Євгена Ігоровича

ТОВ «Леві9 Україна», підтверджує, що розроблені Ситніком Євгеном Ігоровичем в межах дисертаційного дослідження висновки та пропозиції щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій використані під час підготовки аналітичних матеріалів ТОВ «Леві9 Україна».

Заслуговує на увагу сформований автором механізм управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій, який виступає сукупністю елементів та забезпечує комплекс дій з розробки та реалізації планів і заходів відповідно до прийнятої стратегії забезпечення економічної безпеки та організації контролю за їх виконанням відповідно до прийнятих стандартів, норм із застосуванням адміністративно-організаційних, оперативних-розпорядчих, економічних, соціально-психологічних, техніко-технологічних методів та їх інструментів, що дає можливість забезпечувати стійкість та формує умови для подальшого ефективного розвитку підприємства завдяки впровадженню інновацій, передових інноваційних цифрових технологій у всіх сферах діяльності та в системі економічної безпеки; забезпечує захист підприємства від внутрішніх та зовнішніх небезпек та загроз, забезпечує утримання ринкових позицій, зростання конкурентоспроможності та подальший розвиток підприємства.

Довідка надана для представлення за місцем захисту дисертаційної роботи.

Генеральний директор



Коряко В.С.

ДОДАТОК Б.1.



Вих. № 08/09-04 від 08.09.25 року

ДОВІДКА

**Про впровадження науково-прикладних розробок
які виконані в рамках дисертаційної роботи
на здобуття наукового ступеня доктора філософії в галузі знань 07 «Управління
та адміністрування», за спеціальністю 073 «Менеджмент»
Ситніка Євгена Ігоровича**

Цим підтверджуємо, що розроблені Ситніком Євгеном Ігоровичем в межах дисертаційного дослідження висновки та пропозиції, щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій використані у роботі ТОВ "ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНИХРОМ". Зокрема, прийнято до уваги такі науково-практичні положення дисертаційної роботи:

- систематизовані наукові концепти сутності та узагальнені функції застосування цифрових технологій в управлінні;
- запропоновані підходи до дослідження управління системою економічної безпеки підприємства та аналізу управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій;
- сформовану проекцію впливу застосування інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства;
- розроблену стратегію управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій, яка включає реалізацію стратегічних та оперативних цілей дії за напрямками реалізації та передбачає цифровізацію процесів здійснення управлінської, операційної, безпекової діяльності підприємства завдяки впровадженню та використанню нових інноваційних цифрових технологій та дає можливість удосконалити процеси управління та здійснювати безпекову діяльність, розбудову та функціонування системи управління та механізму управління економічною безпекою підприємства на сучасному техніко-технологічному рівні.

Результати дисертаційного дослідження використані в роботі ТОВ "ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНИХРОМ", при дослідженні та підготовці відповідної документації.

Довідка видана для подання за місцем захисту дисертаційної роботи

З повагою,
Директор
ТОВ ВКК «УКРНИХРОМ»



Зеленський О.В.

ТОВ «ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ «УКРНИХРОМ»

ДОДАТОК Б.1



ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ДОСЛІДНИЙ ЗАВОД
ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ
ІМ. С.О. ПАТОНА НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ»



№ 04/003/9

Від 22 вересня 2025р.

АКТ

про впровадження результатів дисертації

Ситніка Євгена Ігоровича

ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ ІМ. С.О. ПАТОНА" НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ засвідчує, що результати дисертаційної роботи Ситніка Євгена Ігоровича впроваджені у практичну діяльність і використовуються в управлінні системою економічної безпеки підприємства.

Зокрема прийнято до уваги такі науково-практичні положення дисертаційної роботи:

— розроблену модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства, що передбачає розрахунок інтегральних індексів впровадження інновацій за суб'індексами, що разом забезпечує нові можливості для проведення аналізу, оцінювання та отримання об'єктивних комплексних даних щодо стану та рівня впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства;

— практичні рекомендації щодо формування механізму управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій, який виступає сукупністю елементів та забезпечує комплекс дій з розробки та реалізації планів і заходів відповідно до прийнятої стратегії забезпечення економічної безпеки та організації контролю за їх виконанням відповідно до прийнятих стандартів, з застосуванням адміністративно-організаційних, оперативно-розпорядчих, економічних, соціально-психологічних, техніко-технологічних методів та їх інструментів.

Заслужовують на увагу, з огляду на практичну цінність, розроблені здобувачем підходи до управління системою економічної безпеки та сформовані механізми і інструменти управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій.

Акт наданий для подання за місцем захисту дисертаційної роботи.

З повагою,

Директор ТОВ "ДЗЗМ І Е ІМ. С.О. ПАТОНА" НАНУ



ДОДАТОК Б.1.

07809, Київська область,
смт. Бородинка, вул. Вокзальна, 6.2
e-mail: office.eurocitygreen@gmail.com



ЄДРПОУ 40165275
АТ "РВС БАНК"
IBAN: UA123390720000026000164101001

**ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
«ЄВРОУКРСІТІГРІН»**

№ 003/18

Від 18. 09 2025р.

ДОВІДКА

**про впровадження результатів дисертаційного дослідження
на здобуття наукового ступеня
доктора філософії в галузі знань 07 «Управління та
адміністрування»,
за спеціальністю 073 «Менеджмент»
Ситніка Євгена Ігоровича**

Підтверджуємо, що розроблені Ситніком Євгеном Ігоровичем в межах дисертаційного дослідження результати та рекомендації, щодо управління системою економічної безпеки підприємства на основі інноваційних цифрових технологій використані у роботі ТОВ «ЄВРОУКРСІТІГРІН».

Зокрема, прийнято до уваги такі науково-практичні положення дисертаційної роботи як:

- обґрунтовану структуру, елементи та визначені складові системи економічної безпеки підприємства розбудованої із застосуванням цифрових технологій, до складу яких входить: правова, фінансова, кадрова, інтелектуальна, виробничо-операційна, майнова-матеріальна, техніко-технологічна, інноваційно-інвестиційна, інформаційно-цифрова, інтерфейсна, ринкова, фізична складові системи економічної безпеки, цифровізація якої дає можливість автоматизувати, оптимізувати процеси управління, зменшити витрати, забезпечити зростання ефективності та результативності у всіх функціональних сферах діяльності підприємства, як єдиної цілісної системи і таким чином досягнути зростання рівня їх стабільності, надійності, економічної безпеки;
- розроблену модель комплексного оцінювання впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства.

Довідка надана для представлення за місцем захисту дисертаційної роботи.

Директор



П.Ю. Коншин

ДОДАТОК В

ЛИСТ ОПИТУВАННЯ

Підприємство (повна назва) _____

Сайт підприємства _____

Просимо вас оцінити показники впровадження інноваційних цифрових технологій в управлінні системою економічної безпеки підприємства за допомогою експертного оцінювання кожного показника в балах від 1 до 10, де 10 відповідає найвищій (найкращій) оцінці що відповідає 100%, а 0 найнижчій.

№	Показник	Оцінка в балах (від 0 до 10) або у % від 0 до 100%
	1.Показники цифровізації загальних процесів функціонування підприємства:	
1	1.1.Наявність доступу до мережі Інтернет та його використання в роботі підприємства	
2	1.2.Кількість зайнятих працівників підприємства, які мають доступ до мережі Інтернет	
3	1.3.Наявність мобільного додатку для просування і реалізації продукції та послуг	
4	1.4. Наявність веб-сайту підприємства	
5	1.5.Активність використання підприємством соціальних медіа	
6	1.6.Активність використання блогів та мікроблогів	
7	1.7.Активність використання веб сайтів чи веб-додатків	
8	1.8.Активність використання інструментів обміну знаннями на основі Wiki	
9	1.9. Оснащення комп'ютерною технікою робочих місць в обсягах достатніх для забезпечення роботи з ІКТ на сучасному технологічному рівні	
10	1.10. Наявність серверу та формування внутрішньої інформаційної мережі підприємства	
11	1.11. Наявність ліцензованого необхідного підприємству програмного забезпечення та його своєчасне оновлення	
12	1.12. Частота та відповідність оновлення комп'ютерної техніки та ПЗ підприємства	
13	1.13.Наявність штатних працівників чи договору з відповідними ІТ компаніями про технічний супровід, обслуговування інформаційно комунікаційної мережі підприємства	
14	1.14. Впровадження навчання працівників підприємства роботі з ІКТ та ПЗ	
	2 Показники впровадження цифрових технологій для управління бізнес-процесами діяльності:	
15	2.1. Впровадження та використання підприємством ERP-технології	
16	2.2. Впровадження та використання підприємством CRM-технологій	
17	2.3. Впровадження та використання підприємством BI технології	
18	2.4.Здійснення електронного обміну інформацією в ланцюгах постачання з партнерами, постачальниками чи покупцями	
19	2.5. Впровадження аналізу «Великих даних» з метою виконання різних завдань операційної, виробничої чи комерційної діяльності	

20	2.6. Використання підприємством послуг «хмарних обчислень»	
21	2.7. Використання в роботі підприємства технологій «штучного інтелекту»	
22	2.8. Реалізація продукції підприємства з застосуванням засобів електронної торгівлі	
23	2.9. Реалізація продукції послуг через власні веб-сайти веб-додатки підприємства	
24	2.10. Використання цифрових електронних платформ для просування та реалізації продукції на внутрішньому ринку	
25	2.11. Використання цифрових електронних платформ для просування та реалізації продукції на міжнародному ринку	
26	2.12. Реалізація продукції, послуг з використанням повідомлень типу EDI, з обміном стандартизованими електронними повідомленнями між підприємствами та автоматизацією бізнес-процесів.	
	3. Впровадження цифрових технологій в забезпеченні економічної безпеки	
27	3.1. Наявність на підприємстві документації яка регламентує проведення заходів, дій чи процедур дотримання забезпечення безпеки ІКТ	
28	3.2. Розробка та затвердження та підприємстві документів, які регламентують питання безпеки ІКТ для віддаленого доступу	
29	3.3. Показник впровадження документації - регламентів які визначають безпеку інформаційно- комунікаційних технологій під час онлайн-заходів в режимі реального часу, з застосуванням інтернет	
30	3.4. Наявність на підприємствах програмного забезпечення для захисту, безпеки віддаленого доступу	
31	3.5. Впровадження, використання штучного інтелекту для забезпечення безпеки інформаційно- комунікаційних технологій	
32	3.6. Частота появи проблем в діяльності підприємства через інциденти безпеки ІКТ	
33	3.7. Частота виникнення проблем недоступності послуг ІКТ через відмови в роботі апаратного або ПЗ	
34	3.8. Частота виникнення проблем недоступності послуг ІКТ через кібер атаки та відмови в обслуговуванні (DoS attack)	
35	3.9. Впровадження заходів безпеки ІКТ в інформаційно- комунікаційних системах, а саме:	
36	3.9.1. Застосування автентифікація за допомогою надійного пароля	
37	3.9.2. Застосування автентифікація за допомогою біометричних методів	
38	3.9.3. Застосування автентифікації на основі комбінування принаймні двох та більше механізмів, засобів	
39	3.9.4. Застосування шифрування даних, документів або електронної пошти	
40	3.9.5. Застосування резервного копіювання інформації в окремі сховища	
41	3.9.6. Застосування контролю доступу до мережі та VPN	
42	3.9.7. Застосування системи моніторингу безпеки ІКТ, яка дозволяє виявити підозрілу активність в системах інформаційних комунікацій та інформує про це	

43	3.9.8. Застосування ведення журналів реєстрації подій (лог-файлів), які дають можливість здійснювати аналіз після інцидентів безпеки ІКТ	
44	3.9.9. Застосування на підприємстві оцінювання ризику ІКТ	
45	3.9.10. Застосування на підприємстві тестування безпеки ІКТ	
46	3.10.Частота виникнення проблем через знищення чи пошкодження інформації внаслідок збоїв у роботі апаратного або ПЗ	
47	3.11.Застосування підприємством технологій «інтернету речей»	
48	3.12. Застосування купівлі послуг «хмарних обчислень» з розміщенням програмного забезпечення для безпеки (антивірусних програм, контролю доступу до мережі, тощо)	
49	3.13. Впровадження програмного забезпечення для безпеки (антивірусних програм, контролю доступу до мережі, тощо)	
50	3.14.Впровадження на підприємстві страхування від інцидентів безпеки ІКТ	
51	3.15. Впровадження нових технічних засобів сигналізації та забезпечення безпеки приміщень	
52	3.16. Застосування датчиків та засобів аудіо та відео спостереження	

ДЯКУЄМО ЗА ВАШІ ВІДПОВІДІ І СПІВПРАЦЮ!!!

ДОДАТОК Д

Таблиця Д 1.

Результати розрахунку нормованих показників цифровізації загальних процесів функціонування підприємства

№	Показник	Вагові кое-ти	ТОВ «Леві 9 Україна»	ТОВ «ЄВРОУКРСІПІРІН»	ТОВ «ЕПАМ ДІДЖИ ТАЛ»	ТОВ "ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНІХРОМ"	ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ ІМ.С.О.ПАТОНА НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ"
1	1.1.Наявність доступу до мережі Інтернет та його використання в роботі підприємства	0,0730	0,073	0,073	0,073	0,0657	0,0584
2	1.2.Кількість зайнятих працівників підприємства, які мають доступ до мережі Інтернет	0,0720	0,072	0,072	0,072	0,072	0,0576
3	1.3.Наявність мобільного додатку для просування і реалізації продукції та послуг	0,0710	0	0	0,0213	0,0284	0,0142
4	1.4. Наявність веб-сайту підприємства	0,0720	0,072	0	0,072	0,072	0,072
5	1.5.Активність використання підприємством соціальних медіа	0,0700	0,07	0,021	0,07	0,042	0,049
6	1.6.Активність використання блогів та мікроблогів	0,0710	0,071	0,0071	0,0568	0,0284	0,0355
7	1.7.Активність використання веб сайтів чи веб-додатків	0,0720	0,0576	0,0576	0,0576	0,0576	0,0432
8	1.8.Активність використання інструментів обміну знаннями на основі Wiki	0,0710	0,0426	0,0568	0,0426	0,0497	0,0426

Продовження таблиці Д1.

9	1.9.Оснащення комп'ютерною технікою робочих місць в обсягах достатніх для забезпечення роботи з ІКТ на сучасному технологічному рівні	0,0720	0,072	0,072	0,072	0,072	0,0576
10	1.10.Наявність серверу та формування внутрішньої інформаційної мережі підприємства	0,0720	0,072	0,036	0,072	0,0648	0,0648
11	1.11.Наявність ліцензованого необхідного підприємству програмного забезпечення та його своєчасне оновлення	0,0720	0,072	0,072	0,072	0,072	0,072
12	1.12. Частота та відповідність оновлення комп'ютерної техніки та ПЗ підприємства	0,0710	0,071	0,0568	0,071	0,071	0,071
13	1.13.Наявність штатних працівників чи договору з відповідними ІТ компаніями про технічний супровід, обслуговування інформаційно комунікаційної мережі підприємства	0,0710	0,071	0,0355	0,071	0,071	0,071
14	1.14. Впровадження навчання працівників підприємства роботі з ІКТ та ПЗ	0,0700	0,07	0,07	0,07	0,07	0,07

Джерело: розраховано автором

ДОДАТОК Д

Таблиця Д 2.

Результати розрахунку нормованих показників впровадження цифрових технологій для управління бізнес-процесами діяльності

№	Показник	Вагові коефіцієнти	ТОВ «Леві9 Україна»	ТОВ «ЄВРОУКРСІТІПРІН»	ТОВ «ЕПАМ ДІДЖИТАЛ»	ТОВ " ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНІХРОМ"	ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ ІМ.С.О.ПАТОНА НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК І ВПРОВАДЖЕННЯ
1	2.1.Впровадження та використання підприємством ERP-технології	0,0850	0,068	0,0765	0,068	0,051	0,0595
2	2.2.Впровадження та використання підприємством CRM- технологій	0,0840	0,0672	0,0588	0,0672	0,0672	0,0588
3	2.3.Впровадження та використання підприємством ВІ технології	0,0820	0,082	0,041	0,082	0,0492	0,0656
4	2.4.Здійснення електронного обміну інформацією в ланцюгах постачання з партнерами, постачальниками чи покупцями	0,0830	0,0664	0,0664	0,0664	0,0664	0,0664
5	2.5. Впровадження аналізу «Великих даних» з метою виконання різних завдань операційної, виробничої чи комерційної діяльності	0,0810	0,0729	0,0243	0,0729	0,0405	0,0567
6	2.6.Використання підприємством послуг «хмарних обчислень»	0,0840	0,084	0,0336	0,084	0,0672	0,084
7	2.7.Використання в роботі підприємства технологій «штучного інтелекту»	0,0840	0,0672	0,0168	0,0672	0,042	0,0504
8	2.8.Реалізація продукції підприємства з застосуванням засобів електронної торгівлі	0,0810	0	0	0,0162	0,0648	0,0486
9	2.9. Реалізація продукції послуг через власні веб-сайти веб-додатки підприємства	0,0840	0	0	0,0168	0,084	0,0504

Продовження таблиці Д2.

10	2.10.Використання цифрових електронних платформ для просування та реалізації продукції на внутрішньому ринку	0,0830	0,0415	0,0415	0,0415	0,0747	0,0415
11	2.11.Використання цифрових електронних платформ для просування та реалізації продукції на міжнародному ринку	0,0850	0,0765	0,051	0,0765	0,0765	0,0595
12	2.12.Реалізація продукції, послуг з використанням повідомлень	0,0840	0,0756	0,0168	0,0672	0,042	0,0504

Джерело: розраховано автором

ДОДАТОК Д

Таблиця Д 3.

**Результати розрахунку нормованих операційних показників
впровадження цифрових технологій в забезпеченні економічної безпеки**

№	Показник	Вагові коефіцієнти	ТОВ «Леві9 Україна»	ТОВ «ЄВРОУКРСІПІРІН»	ТОВ «ЕПАМ ДІДЖИТАЛ»	ТОВ " ВИРОБНИЧО-КОМЕРЦІЙНА КОМПАНІЯ УКРНІХРОМ"	ТОВ "ДОСЛІДНИЙ ЗАВОД ЗВАРЮВАЛЬНИХ МАТЕРІАЛІВ ІНСТИТУТУ ЕЛЕКТРОЗВАРЮВАННЯ
1	3.1.Наявність на підприємстві документації яка регламентує проведення заходів, дій чи процедур дотримання забезпечення безпеки ІКТ	0,0400	0,04	0,04	0,04	0,04	0,04
2	3.2.Розробка та затвердження та підприємстві документів, які регламентують питання безпеки ІКТ для віддаленого доступу	0,0390	0,039	0,039	0,039	0,039	0,039
3	3.3.Показник впровадження документації - регламентів які визначають безпеку інформаційно- комунікаційних технологій під час онлайн- заходів в режимі реального часу, с застосуванням інтернет	0,0380	0,038	0,038	0,038	0,038	0,038
4	3.4.Наявність на підприємствах програмного забезпечення для захисту, безпеки віддаленого доступу	0,0360	0,036	0,018	0,036	0,036	0,036
5	3.5. Впровадження, використання штучного інтелекту для забезпечення безпеки інформаційно-комунікаційних технологій	0,0400	0,028	0,016	0,028	0,02	0,02
6	3.6.Частота появи проблем в діяльності підприємства через інциденти безпеки ІКТ	0,0380	0	0	0	0	0
7	3.7.Частота виникнення проблем недоступності послуг ІКТ через відмови в роботі апаратного або ПЗ	0,0390	0	0	0	0	0

Джерело: розраховано автором

Продовження таблиці ДЗ.

8	3.8.Частота виникнення проблем недоступності послуг ІКТ через кібер атаки та відмови в обслуговуванні (DoS attack)	0,0390	0	0	0	0	0
9	3.9.Впровадження заходів безпеки ІКТ в інформаційно-комунікаційних системах, а саме:	0,0380	0	0	0	0	0
10	3.9.1.Застосування автентифікація за допомогою надійного пароля	0,0370	0,037	0,037	0,037	0,037	0,037
11	3.9.2.Застосування автентифікація за допомогою біометричних методів	0,0390	0,039	0,0234	0,039	0,039	0,039
12	3.9.3. Застосування автентифікації на основі комбінування принаймні двох та більше механізмів, засобів	0,0360	0,036	0,036	0,036	0,036	0,036
13	3.9.4. Застосування шифрування даних, документів або електронної пошти	0,0390	0,039	0,039	0,039	0,039	0,039
14	3.9.5. Застосування резервного копіювання інформації в окремі сховища	0,0390	0,039	0,039	0,039	0,039	0,039
15	3.9.6. Застосування контролю доступу до мережі та VPN	0,0390	0,039	0,0234	0,039	0,039	0,039
16	3.9.7. Застосування системи моніторингу безпеки ІКТ, яка дозволяє виявити підозрілу активність в системах інформаційних комунікацій та інформус про це	0,0390	0,039	0,0078	0,039	0,0234	0,0312

Джерело: розраховано автором

Продовження таблиці ДЗ.

17	3.9.8. Застосування ведення журналів реєстрації подій (лог-файлів), які дають можливість здійснювати аналіз після інцидентів безпеки ІКТ		0,0390	0,039	0,039	0,039	0,039	0,039
18	3.9.9. Застосування на підприємстві оцінювання ризику ІКТ		0,0400	0,04	0,04	0,04	0,032	0,032
19	3.9.10. Застосування на підприємстві тестування безпеки ІКТ		0,0390	0,039	0,0234	0,039	0,0312	0,0312
20	3.10.Частота виникнення проблем через знищення чи пошкодження інформації внаслідок збоїв у роботі апаратного або ПЗ		0,0390	0	0	0	0	0
21	3.11.Застосування підприємством технологій «інтернету речей»		0,0370	0,0074	0,0037	0,0111	0,0148	0,0074
22	3.12. Застосування купівлі послуг «хмарних обчислень» з розміщенням програмного забезпечення для безпеки (антивірусних програм, контролю доступу до мережі, тощо)		0,0390	0,039	0,0234	0,039	0,039	0,039
23	3.13. Впровадження програмного забезпечення для безпеки (антивірусних програм, контролю доступу до мережі, тощо)		0,0360	0,036	0,036	0,036	0,036	0,036
24	3.14.Впровадження на підприємстві страхування від інцидентів безпеки ІКТ		0,0380	0,0266	0,0152	0,0266	0,0152	0,0152
25	3.15. Впровадження нових технічних засобів сигналізації та забезпечення безпеки приміщень		0,0390	0,039	0,039	0,0312	0,039	0,0351
26	3.16. Застосування датчиків та засобів аудіо та відео спостереження		0,0390	0,039	0,039	0,039	0,039	0,039

Джерело: розраховано автором