

**Львівський державний університет внутрішніх справ
Міністерство внутрішніх справ України
Львівський державний університет внутрішніх справ
Міністерство внутрішніх справ України**

Кваліфікаційна наукова
праця на правах рукопису

ШТАНГРЕТ ІРИНА АНДРІЇВНА

УДК: 658.14:65.012.8

ДИСЕРТАЦІЯ

**РОЗВИТОК СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В
УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ**

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

_____ І. А. Штангрет
(підпис, ініціали та прізвище здобувача)

Науковий керівник
Мельник Степан Іванович,
доктор економічних наук, професор

Львів – 2024

АНОТАЦІЯ

Штангрет І. А. Розвиток системи економічної безпеки підприємства в умовах цифрової трансформації економіки. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії зі спеціальності 073 – «Менеджмент». – Львівський державний університет внутрішніх справ МВС України, Львів, 2024.

Дисертаційна робота присвячена вирішенню наукового завдання, що полягає в теоретичному обґрунтуванні і розробці методичних підходів стосовно розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.

У вступі обґрунтовано актуальність дисертаційної роботи, сформульовано мету, завдання, предмет, об'єкт і методи дослідження, викладено наукову новизну та практичне значення отриманих результатів, окреслено особистий внесок здобувачки, наведено дані про апробацію результатів дослідження і публікації.

У першому розділі «Теоретичні аспекти розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки» обґрунтовано, що динамічність змін умов функціонування українських підприємств вимагає постійного й ретельного осучаснення теоретичного базису безпекової діяльності, зважаючи на реалії та перспективи. Простежено видозміну сприйняття безпеки з часів свідомого сприйняття людиною навколишнього світу і до наших днів, що послугувало основою для окреслення змісту й виділення основних підходів у розумінні економічної безпеки підприємства. Конкретизовано мету та основні завдання економічної безпеки українських підприємств, які полягають у цілеспрямованій активності стосовно забезпечення стабільного функціонування підприємства із формуванням безпечних умов для його розвитку шляхом реалізації заходів із виявлення, протидії та/або адаптації до внутрішніх та зовнішніх викликів, ризиків і загроз.

Доведено, що система економічної безпеки підприємства – це поєднання суб'єктів та об'єктів безпеки, в межах безпекозабезпечувальних процесів, шляхом реалізації механізму забезпечення та дотримання політики безпеки, задля досягнення мети й визначених цілей в сфері економічної безпеки відповідно до специфіки й умов функціонування підприємства. Обґрунтовано, що розвиток системи економічної безпеки підприємства – це процес контрольованого і економічно обґрунтованого здійснення кількісно-якісних змін задля посилення захищеності підприємства відповідно до коригування стратегії його розвитку й динаміки внутрішнього й зовнішнього середовища функціонування.

З'ясовано, що поточна діяльність підприємств характеризується і здійснюється під впливом різних трансформацій. Обґрунтовано, що пасивність підприємства в питаннях цифрової трансформації в сучасних умовах провокує втрату конкурентних позицій із подальшим ймовірним припиненням діяльності через невідповідність темпам цифрової трансформації економіки. Простежено видозміну в розумінні поняття «цифрова економіка» із подальшим установленням сутності основних факторів, що виникають при збільшенні частки цифрової економіки, які безпосередньо впливають на процес забезпечення економічної безпеки підприємства. Систематизовано широкий перелік нових ринкових можливостей, ризиків і загроз, що спричинені цифровою трансформацією на різних рівнях управління, та є обов'язковим інформаційним підґрунтям для розвитку системи економічної безпеки підприємства.

Сформовано концептуальне підґрунтя розвитку системи економічної безпеки підприємства, в основу якого покладено авторське розуміння того, що в поточних умовах цифрова трансформація економіки задає параметри для відповідних процесів у масштабах підприємства, але першочергові зміни повинні відбутися в системі економічної безпеки підприємства для формування безпечних умов розвитку суб'єкта господарювання загалом. Концептуальне підґрунтя враховує відому видову відмінність розвитку та містить цілісне

поєднання складових безпекової діяльності, зокрема в частині оцінювання розвитку системи економічної безпеки підприємства, розроблення варіантів програми розвитку та її реалізації, спираючись на безпековий потенціал та необхідність забезпечення безпечних умов для розвитку підприємства.

У другому розділі «Комплексне аналітичне підґрунтя розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки» узагальнено та ретельно проаналізовано аналітичні матеріали, які складаються із міжнародних рейтингів та офіційних статистичних даних щодо активності використання цифрових технологій в Україні. З'ясовано основні аспекти діяльності підприємств видавничо-поліграфічної галузі, продукція яких значно пов'язана із задоволенням інформаційних потреб населення, а також характеризується трансформацією, тобто дедалі більшою мірою представлення в цифровому варіанті на заміну традиційному у вигляді надрукованих на папері книг, брошур, газет і журналів. Охарактеризовано основні перепони для цифрової трансформації підприємств видавничо-поліграфічної галузі як об'єкта безпекової діяльності, ліквідація яких визначається характером цифрової трансформації економіки та створює основу для розвитку бізнесу.

Розроблено теоретико-методичний підхід, який передбачає встановлення рівня п'ятнадцяти якісних індикаторів, котрі визначають зміну основних параметрів системи економічної безпеки в динаміці та щодо зрушень у зовнішньому та внутрішньому середовищі, із наступним їх об'єднанням у п'ять груп та розрахунком інтегрального показника, значення якого утворює необхідну інформаційну основу для розроблення й контролю за виконанням програми розвитку. Апробація практичного застосування розробленого теоретико-методичного підходу відбувалася в умовах п'яти підприємств видавничо-поліграфічної галузі. Згідно з розробленою шкалою було визнано факт поєднання поступальних дій із подальшою нездатністю своєчасно реагувати на вплив ключових факторів. Поступ був зафіксований стосовно кадрової та інформаційно-аналітичної складових, але відставання змін в адміністративно-правовому й техніко-технологічному елементів частково

нівелює їх, позбавляючи підприємство загалом можливості більш швидшими темпами адаптуватися до нових умов ведення бізнесу.

Розроблено модель підсистеми інформаційного забезпечення розвитку системи економічної безпеки підприємства, яка передбачає здійснення змін (організаційні перебудови, технологічні зрушення, технічне оновлення, кадрове підсилення, економічна підтримка), які необхідно провести в межах наявного на кожному підприємстві інформаційного забезпечення, що забезпечить встановлення підстав, які виникають у зв'язку із цифровою трансформацією економіки і підприємства й результатами безпекової діяльності, та інформаційно супроводжувати виконання програми розвитку.

У третьому розділі «Удосконалення методичних засад розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки» доведено, що механізм забезпечення економічної безпеки підприємства потрібно розглядати цілісно в двох площинах, тобто зважаючи на внутрішню побудову (склад елементів) та порядок реалізації безпекової діяльності, яка повинна уможливити функціонування й розвиток підприємств в умовах цифрової трансформації економіки шляхом розроблення й прийняття суб'єктами безпеки оперативних, тактичних і стратегічних рішень як стосовно об'єктів безпеки, так і суб'єктів зовнішнього середовища. Обґрунтовано необхідність виділення в межах такого механізму, як систем нижчого порядку, механізм управління розвитком системи економічної безпеки підприємства. Розроблено механізм управління розвитком системи економічної безпеки підприємства, стосовно якого деталізовано такі його елементи як: методи та інструменти здійснення керуючого впливу; етапи реалізації (діагностика, оцінювання, планування, реалізація, контроль); цільове спрямування (інформаційне, адміністративно-правове, кадрове, економічне, техніко-технологічне). Застосування такого механізму має сприяти постійному осучасненню засад функціонування системи економічної безпеки підприємства відповідно до тенденцій в цифровій трансформації економіки та створювати сприятливі умови для цифрової трансформації підприємства.

Сформульовано методичні засади розвитку системи економічної безпеки підприємства, які спираються на авторське тлумачення цифрових компетентностей суб'єктів безпеки як знання, уміння, навички та здібності, що набуваються упродовж життя в процесі навчання та їх практичного застосування, які уможливають виконання завдань у сфері безпекової діяльності. Уточнено предметну площину застосування цифрових компетентностей за основними функціональними складовими економічної безпеки підприємства та акцентовано увагу, що їх формування й розвиток повинні здійснюватися на постійній основі упродовж життя та відповідати тенденціям у цифровій трансформації економіки.

Сформовано науково-практичний підхід до розвитку системи економічної безпеки підприємства, в основі якого лежить застосування методу функціонального моделювання IDEF0, що створює основу цілісного бачення етапності у визначенні підстав, встановленні ресурсних можливостей та розробленні програми, виконання якої дозволить своєчасно здійснити зміни в безпековій діяльності підприємства, які сприятимуть цифровій трансформації підприємства.

Ключові слова: економічна безпека, економічна безпека підприємства, цифрова трансформація, цифрова трансформація економіки, цифрова трансформація підприємства, підприємства видавничо-поліграфічної галузі, загроза, ризик.

ANNOTATION

Stanhret I. A. Development of the economic security system of the enterprise in the conditions of digital transformation of the economy. – Qualification scientific work as a manuscript.

Thesis stands for a Doctor of Philosophy degree in Economic Sciences, specialty 073 – «Management». – Lviv State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine, Lviv, 2024.

The dissertation work is dedicated to the solution of the scientific task, which consists in the theoretical substantiation and development of methodological approaches regarding the development of the economic security system of the enterprise in the conditions of digital transformation of the economy.

The introduction substantiates the relevance of the dissertation, formulates the goal, task, subject, object and research methods, outlines the scientific novelty and practical significance of the obtained results, outlines the personal contribution of the researcher, provides data on the approval of the research results and publication.

In the first chapter "Theoretical aspects of the development of the economic security system of the enterprise in the conditions of the digital transformation of the economy", it is substantiated that the dynamism of changes in the conditions of functioning of Ukrainian enterprises requires constant and careful modernization of the theoretical basis of security activities, taking into account the realities and prospects. Changes in the perception of security from the time of conscious perception of the surrounding world by man to the present day have been traced, which served as a basis for outlining the content and highlighting the main approaches in understanding the economic security of the enterprise. The purpose and main tasks of the economic security of Ukrainian enterprises have been specified, which consist in purposeful activity to ensure the stable functioning of the enterprise with the formation of safe conditions for its development through the implementation of measures to identify, counter and/or adapt to internal and external challenges, risks and threats. It is proved that the system of economic security of the enterprise is a combination of subjects and objects of security, within the security processes, by implementing a mechanism for ensuring and complying with the security policy, in order to achieve the goal and defined goals in the field of economic security in accordance with the specifics and conditions of the enterprise's operation. It is substantiated that the development of the economic security system of the enterprise is a process of controlled and economically justified implementation of quantitative and qualitative changes in order to strengthen the security of the enterprise in

accordance with the adjustment of its development strategy and the dynamics of the internal and external environment of functioning.

It was found that the current activity of enterprises is characterized and carried out under the influence of various transformations. It is substantiated that the company's passivity in matters of digital transformation in modern conditions provokes the loss of competitive positions with the subsequent probable termination of activity due to non-compliance with the pace of digital transformation of the economy. A change in the understanding of the concept of "digital economy" was traced, with further establishment of the essence of the main factors that arise when the share of the digital economy increases, which directly affect the process of ensuring the economic security of the enterprise. A wide list of new market opportunities, risks and threats caused by digital transformation at different levels of management is systematized and is a mandatory information basis for the development of the enterprise's economic security system.

The conceptual basis for the development of the economic security system of the enterprise has been formed, which is based on the author's understanding that in the current conditions, the digital transformation of the economy sets the parameters for the relevant processes at the enterprise scale, but the primary changes must take place in the economic security system of the enterprise to form safe conditions for the development of sub business entity in general. The conceptual basis takes into account the well-known specific differences in development and contains a holistic combination of components of security activities, in particular in terms of assessing the development of the economic security system of the enterprise, developing options for the development program and its implementation, based on the security potential and the need to ensure safe conditions for the development of the enterprise.

In the second chapter "Comprehensive analytical basis for the development of the system of economic security of the enterprise in the conditions of digital transformation of the economy" analytical materials consisting of international ratings and official statistical data on the activity of the use of digital technologies in Ukraine are summarized and carefully analyzed. The main aspects of the activities of

enterprises in the publishing and printing industry, the products of which are significantly related to the satisfaction of the information needs of the population, and are also characterized by transformation, i.e. increasingly being presented in a digital version to replace the traditional one in the form of books, brochures, and newspapers printed on paper, have been clarified and magazines. The main obstacles to the digital transformation of enterprises in the publishing and printing industry as objects of security activity are characterized, the elimination of which is determined by the nature of the digital transformation of the economy and creates a basis for business development.

A theoretical and methodological approach has been developed, which involves establishing the level of fifteen qualitative indicators that determine the change in the main parameters of the economic security system in dynamics and in relation to changes in the external and internal environment, followed by their unification into five groups and the calculation of an integral indicator, the value of which forms the necessary information basis for developing and monitoring the implementation of the development program. Approbation of the practical application of the developed theoretical and methodological approach took place in the conditions of five enterprises of the publishing and printing industry. According to the developed scale, the fact of combining progressive actions with the subsequent inability to respond in a timely manner to the influence of key factors was recognized. Progress was recorded in terms of personnel and information-analytical components, but the backlog of changes in administrative-legal and technical-technological elements partially neutralizes them, depriving the company in general of the opportunity to adapt to new business conditions at a faster pace.

A model of the subsystem of information support for the development of the economic security system of the enterprise has been developed, which provides for the implementation of changes (organizational restructuring, technological shifts, technical updating, personnel reinforcement, economic support), which must be carried out within the limits of the information support available at each enterprise, which will ensure the establishment of grounds that arise in connection with the

digital transformation of the economy and the enterprise and the results of security activities, and informationally accompany the implementation of the development program.

In the third chapter "Improving the methodological foundations of the development of the economic security system of the enterprise in the conditions of the digital transformation of the economy" it is proved that such a mechanism for ensuring the economic security of the enterprise must be considered holistically in two planes, that is, taking into account the internal structure (composition of elements) and the order of implementation of security activities, which should enable the functioning and development of enterprises in the conditions of digital transformation of the economy through the development and adoption by security subjects of operational, tactical and strategic decisions both in relation to security objects and subjects of the external environment. The need to allocate within such a mechanism as lower-order systems a mechanism for managing the development of the enterprise's economic security system is substantiated. A mechanism for managing the development of the enterprise's economic security system has been developed, in relation to which such elements as: methods and tools for exercising managerial influence are detailed; stages of implementation (diagnosis, assessment, planning, implementation, control); target orientation (informational, administrative-legal, personnel, economic, technical-technological). The application of such a mechanism should contribute to the constant modernization of the principles of the functioning of the economic security system of the enterprise in accordance with the trends in the digital transformation of the economy and create favorable conditions for the digital transformation of the enterprise.

The methodical principles of the development of the economic security system of the enterprise are formulated, which are based on the author's interpretation of the digital competences of security subjects as knowledge, abilities, skills and abilities acquired throughout life in the process of learning and their practical application, which enable the performance of tasks in the field of security activities. The subject area of application of digital competences according to the main functional

components of the economic security of the enterprise has been specified, and it has been emphasized that their formation and development should be carried out on a permanent basis throughout life and correspond to trends in the digital transformation of the economy.

A scientific and practical approach to the development of the enterprise's economic security system has been formed, which is based on the application of the IDEF0 functional modeling method, which creates the basis for a holistic vision of phasing in determining the basis, establishing resource capabilities and developing a program, the implementation of which will allow timely changes in the enterprise's security activities, which will contribute to the digital transformation of the enterprise.

Keywords: economic security, economic security of the enterprise, digital transformation, digital transformation of the economy, digital transformation of the enterprise, enterprises of the publishing and printing industry, threat, risk.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, в яких опубліковані основні наукові результати дисертації

1. Штангрет І. А. Розвиток системи економічної безпеки в умовах цифрової трансформації підприємства. *Ефективна економіка*. 2022. № 6. URL: <https://www.nayka.com.ua/index.php/ee/article/view/120/122>. DOI: 10.32702/2307-2105.2022.6.34.

2. Штангрет І. А. Теоретичні засади формування системи економічної безпеки підприємства. *Ефективна економіка*. 2022. № 4. URL: <http://www.economy.nayka.com.ua/?op=1&z=10173> DOI: 10.32702/2307-2105-2022.4.150.

3. Штангрет І. А. Інформаційне забезпечення розвитку системи економічної безпеки промислового підприємства в умовах цифрової трансформації економіки. *Східна Європа: економіка, бізнес та управління*. 2023. №4 (41). С. 110–115. DOI: <https://doi.org/10.32782/easterneurope.41-17>.

4. Штангрет І. А. Оцінювання розвитку системи економічної безпеки підприємства. *Інфраструктура ринку*. 2023. Вип. 74. С. 85–89. DOI: <https://doi.org/10.32782/infrastructure74-16>.

5. Штангрет І. А. Трансформаційні процеси в діяльності підприємств видавничо-поліграфічної галузі. *Держава та регіони*. 2023. № 2 (128). С. 50–55. DOI: <https://doi.org/10.32782/1814-1161/2023-2-7>.

6. Штангрет І. А. Механізм управління розвитком системи економічної безпеки підприємства в умовах цифрової трансформації економіки. *Інфраструктура ринку*. 2023. № 71. С. 194–199. DOI: <https://doi.org/10.32782/infrastructure71-34>.

7. Мельник С. І., Штангрет І. А. Методичні засади розвитку системи економічної безпеки підприємства. *Ефективна економіка*. 2024. № 1. URL: <https://www.nauka.com.ua/index.php/ee/article/view/2863/2899> DOI: <http://doi.org/10.32702/2307-2105.2024.1.17> (особистий внесок здобувачки: розроблено методичні засади розвитку системи економічної безпеки підприємствана основі формування цифрових компетентностей у суб'єктів безпеки).

8. Andriyiv N., Pushak H., Petrukha N., Kokhan V., Shtangret I. Transformation of threats to demographic security and sustainable development of the region due to increased military actions. *International Journal of Sustainable Development and Planning*. 2022. Vol. 17. No. 7. P. 2221–2227. DOI: <https://doi.org/10.18280/ijstdp.170722>. (особистий внесок здобувачки: визначення впливу військових дій на демографічну безпеку України, із конкретизацією тих загроз, що пов'язані з втратою трудових ресурсів та негативно впливають на економічну безпеку підприємств. (наукове видання (журнал) індексується міжнародною наукометричною базою Scopus).

Праці, які засвідчують апробацію матеріалів дисертації

9. Штангрет І. А. Безпекові аспекти управління мотивацією працівників промислових підприємств. *Соціально-економічний розвиток і безпека України:*

стан та перспективи : матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Львів, 25 березня 2021 р.). Львів : Галицька видавнича спілка, 2021. С. 150–152.

10. Штангрет І. А. Система економічної безпеки підприємства: теоретичний базис формування. *Сучасні підходи до креативного управління економічними процесами* : матеріали XIII Міжнародної науково-практичної конференції (м. Київ, 14–15 квітня 2022 р.). Київ : НАУ, 2022. С. 122–124.

11. Штангрет І. А. Методичні засади забезпечення економічної безпеки підприємства. *Менеджмент і безпека: теоретичні та прикладні аспекти* : матеріали науково-практичної конференції (м. Львів, 13 травня 2022 р.). Львів : ЛьвДУВС, 2022. С. 127–129.

12. Штангрет І. А. Безпекові аспекти цифрової трансформації промислових підприємств. *Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення* : матеріали IX Всеукраїнської науково-практичної конференції (м. Львів, 20–22 травня 2022 р.). Львів : УАД, 2022. С. 102–104.

13. Штангрет І. А. Концептуальне підґрунтя розвитку системи економічної безпеки підприємства. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні* : матеріали VIII Всеукраїнської науково-практичної конференції (м. Львів, 24–26 листопада 2022 р.). Львів : УАД, 2022. С. 136–138.

14. Штангрет І. А. Механізм забезпечення економічної безпеки підприємства. *Соціально-економічний розвиток і безпека України: стан та перспективи* : матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Львів, 23 березня 2023 р.). Львів : ЛьвДУВС, 2023. С. 151–153.

15. Штангрет І. А. Механізм управління розвитком системи економічної безпеки підприємства: теоретичні засади. *Сучасні підходи до креативного управління економічними процесами* : матеріали XIV Міжнародної науково-

практичної конференції (м. Київ, 13–14 квітня 2023 р.). Київ : НАУ, 2023. С. 231–233.

16. Штангрет І. А. Розвиток системи економічної безпеки підприємства: необхідність та варіант реалізації. *Економічна безпека держави та суб'єктів підприємницької діяльності в Україні : проблеми та шляхи їх вирішення* : матеріали X Всеукраїнської науково-практичної конференції (м. Львів, 25–27 травня 2023 р.). Львів : УАД, 2023. С. 125–127.

17. Штангрет І. А. Система інформаційного забезпечення безпекової діяльності підприємства. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні* : матеріали ІХ Всеукраїнської науково-практичної конференції (м. Львів, 23–26 листопада 2023 р.). Львів : УАД, 2023. С. 192–194.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВПГ – видавничо-поліграфічна галузь

ВРЗ – виклик, ризик, загроза

ЕБ – економічна безпека

ЕБД – економічна безпека держави

ЕБП – економічна безпека підприємства

ІЗ – інформаційне забезпечення

ПП – промислове підприємство

ПР – промислова революція

СЕС – соціально-економічна система

ЦТ – цифрова трансформація

ЦТЕ – цифрова трансформація економіки

ЦТП – цифрова трансформація підприємства

ЗМІСТ

ВСТУП	17
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ РОЗВИТКУ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ	26
1.1. Теоретичні засади формування та розвитку системи економічної безпеки підприємства.....	26
1.2. Цифрова трансформація економіки: систематизація наукових поглядів.....	50
1.3. Концептуальне підґрунтя розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.....	71
ВИСНОВКИ ДО РОЗДІЛУ 1	92
РОЗДІЛ 2. КОМПЛЕКСНЕ АНАЛІТИЧНЕ ПІДґРУНТЯ РОЗВИТКУ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ	94
2.1. Дослідження умов розвитку системи економічної безпеки підприємств видавничо-поліграфічної галузі.....	94
2.2. Теоретико-методичний підхід до оцінювання розвитку системи економічної безпеки підприємства.....	116
2.3. Інформаційне забезпечення розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.....	131
ВИСНОВКИ ДО РОЗДІЛУ 2	146
РОЗДІЛ 3. УДОСКОНАЛЕННЯ МЕТОДИЧНИХ ЗАСАД РОЗВИТКУ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ	148
3.1. Механізм управління розвитком системи економічної безпеки підприємства в умовах цифрової трансформації економіки.....	148
3.2. Методичні засади розвитку системи економічної безпеки підприємства.....	167
3.3. Моделювання розвитку системи економічної безпеки підприємства.....	185
ВИСНОВКИ ДО РОЗДІЛУ 3	199
ВИСНОВКИ	202
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	205
ДОДАТКИ	227

ВСТУП

Обґрунтування вибору теми дослідження. Для українських підприємств постпандемічний період збігся із активізацією військових дій, які зі стану конфлікту в межах окремих територій країни розширилися до повномасштабної війни, коли об'єкти ракетних ударів географічно не обмежені. Набуття досвіду безпекової діяльності в умовах COVID-19 та військових дій зміцнює практичну основу безпекознавства і лише тимчасово змінює пріоритетність цільового спрямування стосовно постійної актуальності врахування тенденцій в цифровій трансформації економіки. Висока активність у поширенні цифрових технологій визначає конкурентну позицію кожного підприємства, що в ракурсі безпекознавства характеризується як необхідністю відстеження і створення умов для ефективного використання нових можливостей, так і виникненням раніше не існуючих ризиків і загроз, протидія і ліквідація яких неможлива без поступу в безпековій діяльності. Потреба слідування за цифровою трансформацією економіки вимагає переосмислення й внесення змін у діяльність підприємств, результати чого визначаються рівнем розвитку існуючої системи економічної безпеки. Ситуація для українських підприємств ускладнюється тимчасовим відставанням цифрової трансформації національної економіки при відкритості внутрішнього ринку, що визначає необхідність своєчасного здійснення якісно-кількісних змін у системі їх економічної безпеки, зважаючи на аспекти діяльності в тактичному й стратегічному вимірах, задля збереження й покращення конкретних позицій в умовах подальших динамічних цифрових трансформацій на макро- та мікрорівнях. Поширені сьогодні підходи в організації системи економічної безпеки підприємств не надають належної уваги питанню її розвитку, тому на практиці відбувається слідування за змінами із намаганням ліквідувати негативні наслідки загроз. Випереджальний характер функціональної дієвості системи економічної безпеки підприємства потребує переосмислення засад і

розроблення відповідного теоретичного базису розвитку такої системи, стимулятором чого є цифрова трансформація економіки.

Розробці питань щодо забезпечення безпеки підприємств багато уваги приділяють вітчизняні та закордонні вчені, зокрема: О. Ареф'єва, Т. Васильців, В. Геєць, З. Герасимчук, Л. Гнилицька, В. Гобела, В. Духов, М. Єрмошенко, Я. Жаліло, З. Живко, В. Засанський, О. Захаров, О. Іляш, С. Кавун, М. Камлик, Г. Козаченко, М. Копитко, О. Куриліна, О. Ляшенко, В. Мартинюк, С. Мельник, І. Мойсеєнко, Т. Момот, В. Мунтіян, Г. Пастернак-Таранушенко, Н. Пойда-Носик, В. Пономаренко, Я. Пушак, І. Ревак, Є. Рудніченко, М. Флейчук, В. Франчук, М. Швець, Л. Шемаєва, Т. Шира та інші. Віддаючи належне науковій і практичній значущості праць провідних вчених, слід зазначити, що у сучасній науковій літературі й практиці господарювання українських підприємств недостатньо досліджені важливі питання розвитку системи економічної безпеки підприємства. Переважає вибірково-фрагментарний підхід до зазначеної проблеми, який ускладнює її вирішення. Отже, питання розроблення теоретико-методичної бази розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки є актуальним, що обумовило вибір теми дисертації, її мету та завдання

Наукове завдання дослідження полягає в теоретичному обґрунтуванні і розробці методичних підходів стосовно розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано згідно з планами наукових досліджень Львівського державного університету внутрішніх справ в межах науково-дослідної роботи «Економічна безпека соціально-економічних систем: проблеми теорії та практики» (номер державної реєстрації 0121U112498, 2021–2024 рр.), в якій сформовано методичні засади розвитку системи економічної безпеки підприємства, а також Української академії друкарства у рамках державних бюджетних і господарських договірних робіт за темами: «Моделювання механізмів управління економічною безпекою підприємства» (номер державної

реєстрації 0113U008320, 2013–2023 рр.), в якій авторка розробила механізм управління розвитком системи економічної безпеки підприємства; «Стан, проблеми та напрямки вдосконалення обліку, аналізу та аудиту підприємницьких структур видавничо-поліграфічної галузі» (номер державної реєстрації 0113U008319, 2013–2023 рр.), в якій здобувачка здійснила оцінювання середовища розвитку системи економічної безпеки підприємств видавничо-поліграфічної галузі; «Інформаційно-аналітичне забезпечення управління економічною безпекою підприємства» (номер державної реєстрації 0120U103566, 2020–2023 рр.), в межах якої розроблено модель підсистеми інформаційного забезпечення розвитку системи економічної безпеки підприємства.

Мета і завдання дослідження. *Метою* дисертаційного дослідження є наукове обґрунтування теоретико-методичних положень та розробка практичних рекомендацій щодо розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.

Досягнення обраної мети обумовило необхідність вирішення таких *завдань*:

- здійснити систематизацію передумов розвитку системи економічної безпеки підприємства;
- сформувати концептуальне підґрунтя розвитку системи економічної безпеки підприємства;
- обґрунтувати теоретико-методичний підхід до оцінювання розвитку системи економічної безпеки підприємства;
- розробити модель підсистеми інформаційного забезпечення розвитку системи економічної безпеки підприємства;
- розробити механізм управління розвитком системи економічної безпеки підприємства;
- сформувати методичні засади розвитку системи економічної безпеки підприємства;

– запропонувати науково-практичний підхід до розвитку системи економічної безпеки підприємства.

Об'єкт дослідження – процес розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.

Предмет дослідження – теоретико-методичні, наукові та прикладні положення розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.

Методи дослідження. В основу методології дисертаційної роботи покладено системний підхід, у межах якого застосовано такі методи: *індукції та дедукції, порівняння і систематизації* – при дослідженні сутнісних характеристик та еволюції базових понять дисертаційної роботи; *аналізу та синтезу* – для окреслення тенденцій в цифровій трансформації економіки України та характеристики розвитку підприємств видавничо-поліграфічної галузі; *непараметричні статистичні* – для оцінювання суттєвості впливу факторів на економічну безпеку підприємств видавничо-поліграфічної галузі; *анкетування та експертного аналізу* – для створення переліку базових індикаторів, визначення їх граничних значень та вагових коефіцієнтів при оцінюванні розвитку системи економічної безпеки підприємства, а також вивчення досвіду безпекової діяльності і встановлення суттєвості впливу загроз, що виникають у процесі цифрової трансформації підприємства; *моделювання* – для розробки моделі підсистеми інформаційного забезпечення розвитку системи економічної безпеки підприємства та механізму управління розвитком системи економічної безпеки підприємства; *функціонального моделювання IDEF0* – для моделювання процесу розвитку системи економічної безпеки підприємства; *морфологічного аналізу* – для уточнення понятійно-категоріального апарату за проблемою; *графічний* – під час наочного подання теоретичного та методичного матеріалу; *абстрактно-логічний* – задля теоретичних узагальнень і висновків дослідження.

Інформаційною базою дослідження є законодавчі та нормативно-правові акти України, вітчизняна і зарубіжна наукова література, статистичні дані

Державної служби статистики України, звітність і первинна документація підприємств видавничо-поліграфічної галузі, результати анкетування менеджменту промислових підприємств, ресурси мережі Інтернет.

Наукова новизна отриманих результатів полягає в узагальненні і обґрунтуванні науково-теоретичних засад та формуванні методичних й прикладних підходів до розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки. У процесі дослідження одержано такі найсуттєвіші результати:

удосконалено:

– концептуальні засади розвитку системи економічної безпеки підприємства, які у порівнянні з відомими, враховують зміни, що відбуваються в національній економіці, містять деталізацію різних варіантів її реалізації та є складовими параметрів програми безпекової діяльності, виконання якої створює сприятливі умови для досягнення стратегічних цілей підприємства;

– теоретико-методичний підхід до оцінювання розвитку системи економічної безпеки підприємства, який відрізняється якісно-кількісними індикаторами вимірювання в динаміці з урахуванням змін у зовнішньому середовищі та внутрішньогосподарських процесах, що створює необхідну інформаційну базу для розроблення й реалізації програми розвитку з метою постійного поступу в безпековій діяльності;

– механізм управління розвитком системи економічної безпеки підприємства, який, порівняно із відомими, передбачає сучасне інформаційне, адміністративно-правове, кадрове, економічне та техніко-технологічне забезпечення, що покликано підтримувати необхідні темпи змін у зазначеній системі відповідно до тенденцій в цифровій трансформації економіки;

– науково-практичний підхід до розвитку системи економічної безпеки підприємства, який у порівнянні з відомими, передбачає застосування методу функціонального моделювання IDEF0, що створює основу цілісного бачення етапності у визначенні підстав, встановленні ресурсних можливостей та

розробленні відповідної програми, виконання якої створює умови для цифровій трансформації підприємства;

набули подальшого розвитку:

– систематизація передумов розвитку системи економічної безпеки підприємства, яка, порівняно із відомими, визначає змістове наповнення та логічно поєднує сутність таких понять як «трансформація», «цифрова трансформація економіки», «четверта промислова революція», «цифрова економіка» та «цифрова трансформація підприємства», що забезпечує формування цілісного бачення обставин й характеру цифрової трансформації на різних рівнях управління та слугує орієнтирами у безпековій діяльності для виконання дій на випередження;

– модель підсистеми інформаційного забезпечення розвитку системи економічної безпеки підприємства, яка відрізняється від відомих у науці та практиці структурними елементами (організаційні перебудови, технологічні зрушення, технічне оновлення, кадрове підсилення, економічна підтримка), наповнення яких конкретною інформацією дозволяє визначати зміст тих змін, які необхідно провести у зв'язку з цифровою трансформацією економіки й підприємства та результатами безпекової діяльності, а також інформаційно супроводжувати виконання програми розвитку;

– методичні засади розвитку системи економічної безпеки підприємства, які, у порівнянні з існуючими, передбачають удосконалення цифрових компетентностей суб'єктів безпеки з урахуванням досвіду безпекової діяльності українських підприємств в умовах цифрової трансформації національної економіки, COVID-19 та воєнних дій, що сприяє протидії загрозам на основі результативнішої роботи з інформаційними ресурсами.

Практичне значення отриманих результатів полягає в обґрунтуванні рекомендацій щодо розвитку системи економічної безпеки підприємства. Теоретичні висновки, науково-практичні рекомендації та інші результати наукових досліджень, викладені в дисертаційній роботі, безпосередньо використані такими підприємствами: ТзОВ «Видавничий Дім «Високий замок»

(довідка про впровадження № 423-75-С від 19.04.2023 р.), ПП «СаЮл» (довідка про впровадження № 153/42 від 21.06.2023 р.), НВТ ТзОВ «Поліграфічні плівки та послуги» (довідка про впровадження № 184-3/23 від 12.09.2023 р.), ТзОВ «Видавництво «Свічадо» (довідка про впровадження № 74/15/24 від 23.02.2024 р.).

Наукові розробки та теоретичні узагальнення дисертаційної роботи впроваджені в освітній процес та наукову діяльність, зокрема:

– під час викладання навчальних дисциплін «Основи безпекознавства», «Фінансова безпека» й «Бюджетно-податкова безпека» (акт впровадження в освітній процес Львівського державного університету внутрішніх справ від 02.01.2024 р. № 03) та «Комплексне забезпечення фінансово-економічною безпекою», «Менеджмент економічної безпеки підприємства», «Антикризове управління підприємством», «Соціально-економічна безпека» та «Наукове та методичне забезпечення діяльності фахівців з фінансово-економічної безпеки» (довідка про впровадження в освітній процес Української академії друкарства № 64-11/690 від 16.11.2023 р.);

– для проведення подальших наукових досліджень з проблем: систематизації передумов розвитку системи економічної безпеки підприємства; формування концептуального підґрунтя розвитку системи економічної безпеки підприємства; обґрунтування теоретико-методичного підходу до оцінювання розвитку системи економічної безпеки підприємства; розроблення моделі підсистеми інформаційного забезпечення розвитку системи економічної безпеки підприємства; побудови механізму управління розвитком системи економічної безпеки підприємства; формування методичних засад розвитку системи економічної безпеки підприємства; розроблення науково-практичного підходу до розвитку системи економічної безпеки підприємства (акт впровадження у наукову діяльність Львівського державного університету внутрішніх справ від 04.01.2024 р. № 4).

Особистий внесок здобувача полягає у розробці й обґрунтуванні наукових положень, висновків і рекомендацій щодо розвитку системи

економічної безпеки підприємства в умовах цифрової трансформації економіки.

Дисертаційна робота є самостійно виконаним дослідженням, у якому викладено нові авторські науково-методичні підходи та практичні рекомендації щодо розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки. Внесок у роботах, виконаних у співавторстві, відображено у публікаціях [7–8] за списком праць.

Апробація результатів дисертації. Основні результати дисертації доповідалися та обговорювалися на міжнародних і всеукраїнських науково-практичних конференціях: міжвузівській науково-практичній конференції здобувачів вищої освіти і молодих вчених «Соціально-економічний розвиток і безпека України: стан та перспективи» (м. Львів, 25 березня 2021 р.); XIII Міжнародній науково-практичній конференції «Сучасні підходи до креативного управління економічними процесами» (м. Київ, 14–15 квітня 2022 р.); науково-практичній конференції «Менеджмент і безпека: теоретичні та прикладні аспекти» (м. Львів, 13 травня 2022 р.); IX Всеукраїнській науково-практичній конференції «Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення» (м. Львів, 20–22 травня 2022 р.); VIII Всеукраїнській науково-практичній конференції «Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні» (м. Львів, 24–26 листопада 2022 р.); міжвузівській науково-практичній конференції здобувачів вищої освіти і молодих вчених «Соціально-економічний розвиток і безпека України: стан та перспективи» (м. Львів, 23 березня 2023 р.); XIV Міжнародній науково-практичній конференції «Сучасні підходи до креативного управління економічними процесами» (м. Київ, 13–14 квітня 2023 р.); X Всеукраїнській науково-практичній конференції «Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення» (м. Львів, 25–27 травня 2023 р.); IX Всеукраїнській науково-практичній

конференції «Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні» (м. Львів, 23–26 листопада 2023 р.).

Публікації. Положення та висновки, сформульовані у дисертації, опубліковано у 17 наукових працях, серед яких: 1 стаття у науковому періодичному виданні, яке індексується у наукометричній базі даних Scopus; 7 статей у наукових фахових виданнях України категорії «Б»; 9 наукових праць у збірниках за матеріалами конференцій, що засвідчують апробацію матеріалів дисертації.

Структура і обсяг роботи. Дисертація складається з анотації українською та англійською мовами, вступу, трьох розділів, висновків, списку використаних джерел (212 найменувань на 22 сторінках) і 4 додатків, розміщених на 22 сторінках. Загальний обсяг наукової роботи становить 248 сторінок, з яких основний текст – 190 сторінок, які містять 48 рисунків.

РОЗДІЛ 1

ТЕОРЕТИЧНІ АСПЕКТИ РОЗВИТКУ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

1.1. Теоретичні засади формування та розвитку системи економічної безпеки підприємства

Ключовою передумовою розвитку національної економіки за подальшого посилення глобалізаційних, інноваційних та цифровізаційних процесів й продовження внутрішніх трансформаційних змін, які супроводжуються політичною нестабільністю, соціальними збуреннями та руйнівними наслідками військових дій, стає стабільне функціонування із орієнтацією на посилення конкурентних позицій первинної ланки, тобто підприємства. Попри відмінності в масштабах, ефективна фінансово-господарська діяльність більшості таких суб'єктів створює необхідний сумарний ефект для позитивних змін на рівні національної економіки. Водночас різні умови функціонування кожного підприємства, як і чисельність таких суб'єктів, суттєво ускладнює вирішення проблематики здійснення ними ефективної фінансово-господарської діяльності, орієнтованої на розвиток через досягнення економічних, соціальних, екологічних та інших цілей без максимального приділення уваги безпековим аспектам. Саме безпека, як і на інших рівнях, тобто людини, регіону, галузі, держави, формує необхідну основу існування й розвитку кожної СЕС, зокрема й підприємства. Пріоритетність забезпечення безпеки, що передбачає не лише захист певної системи в процесі взаємодії із суб'єктами зовнішнього середовища, а й виявлення нових можливостей доводить важливість подальшого наукового пошуку стосовно формування й розвитку СЕБП, зважаючи на те, що саме економічний ракурс є результуючим у підприємницькій ініціативі, а системний підхід сприяє встановленню зв'язку між усіма складовими систем, а також у взаємодії із системами вищого та

нижчого порядку із чіткою організацією захисних редутив та отримання інформації про внутрішні та зовнішні процеси, що визначають стан і можливі зміни в умовах певного підприємства. З огляду на такі позиції, в межах цього підрозділу встановлені такі завдання: дослідити сутність поняття ЕБП із подальшим розглядом умов формування СЕБП, яка здатна забезпечити досягнення корпоративних інтересів; розглянути сутність терміна «розвиток» для уточнення умов розвитку підприємства та системи його ЕБ.

Відповідно до визначеного переліку завдань, сконцентруємо увагу на першочерговому дослідженні ЕБП, основу якої становлять такі терміни як «безпека», ЕБ та «підприємство». Кожен із зазначених термінів характеризується багатоаспектністю, яку складно повною мірою відобразити в межах окремого підрозділу дисертаційної роботи, що змушує зосередитися лише на окремих важливих моментах. Так, трактування безпеки як підсвідоме уявлення кожної особи про власний стан домінувало до XVIII ст., що було відображено у філософських публікаціях Ж. Ж. Руссо, Н. Маккіавеллі та інших. У подальшому, завдяки напрацюванням Т. Гоббса, Д. Локка Ф. Гегеля, Ю. Бека та інших, відбулося переосмислення суті цього базового поняття, коли забезпечення безпеки особи розглядалося у взаємозв'язку із безпекою суспільства та держави, виводячи на перший план національну безпеку, обов'язковою складовою якої була ЕБ. Підтвердженням таких змін є визначення Г. Форда, який під безпекою розумів «...стан захищеності життєво важливих інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз» [152, с. 35]. Суттєвою специфікою поняття «безпека» є те, що воно було і залишається міждисциплінарним, будучи притаманним у підсвідомості кожній людині, а також виокремлене як самостійна категорія філософами із подальшим поглибленням розуміння у соціології, політології, психології і економіці. Зазначене є підставою, щоб стверджувати: в трактуванні ЕБП наявні моменти, які запозичені з інших галузей науки і у подальшому адаптовані економістами. Так, з соціології було перейнято розуміння безпеки як «життєвої стійкості», з політології – врахування факторів, які уможливають

розвиток, із психології – можливість об'єднання індивідуумів задля спільного досягнення й підтримання необхідного рівня безпеки. В подальшому нами будуть виділені основні підходи в трактуванні ЕБД, де явними будуть вказані запозичення, що сприяли розвитку цього напрямку в безпекознавстві. Потрібно зазначити, що міждисциплінарність безпеки також сприяла поступовому переходу у її тлумаченні від пасивного очікування змін до діяльності, яка передбачає усунення суперечностей та використання усіх можливостей задля покращення поточного стану й створення умов для розвитку кожної СЕС.

Формування ЕБ як окремого напрямку відбулося через усвідомлення того факту, що важелі економічного впливу дають змогу отримати кращі результати порівняно із провадженням військових дій, а забезпечення міжнародної ЕБ створює умови для стабілізації ситуації, посилення конкурентних позицій на світових ринках та пришвидшення соціально-економічного розвитку абсолютно усіх країн. Вище зазначене багаторівневе сприйняття безпеки, тобто держави-суспільства-особистості, яке стосовно ЕБ, було видозмінено у побудову ієрархічної структури, в якій виділяють міжнародну, національну, регіональну та мікрорівневу (підприємство, підприємець, особа). Поруч з цим, в основі трактування ЕБ залишилося загальне розуміння безпеки як основи збереження певної СЕС, яке було доповнено розумінням можливості досягнення цієї мети на різних рівнях.

Обмежуючись коротким історичним екскурсом щодо формування сучасного розуміння ЕБ, доцільно підкреслити наступні моменти: по-перше, окреслення змісту терміна відбулося на рівні держави у 30-х роках ХХ ст. із подальшою конкретизацією його змісту як складової національної безпеки у 40-60-х роках; по-друге, усвідомлення пріоритетності забезпечення міжнародної ЕБ відбулося у 80-х роках як основи досягнення основних цілей існування й розвитку людства; по-третє, лише в 90-х роках була здійснена спроба визначення суті нижчих рівнів в ієрархії, тобто регіону, галузі, підприємства; по-четверте, початок ХХІ ст. ознаменувався потребою комплексного розгляду процесу забезпечення ЕБ на усіх рівнях.

Серед численних визначень ЕБ доцільно виділити також позицію Г. Калетніка й Г. Пчелянської [64, с. 31], які розглядають її сутність комплексно, тобто в якості стану, процесу і системи. Безпека як стан є результатом впливу різних факторів, що створює основу для подальшого протікання відтворювальних процесів. Безпека як процес передбачає формування умов для існування й розвитку. Безпека як система уможливорює поєднання різних елементів із встановленням відповідних зв'язків, які забезпечують їх збереження та здатність адаптуватися до зміни умов існування. Важливо, що усі три параметри лежать в основі трактування ЕБ на усіх рівнях ієрархічної структури, а також формують уявлення про загальну орієнтацію не лише на захист, але й на розвиток. Також доцільно підкреслити, що на кожному рівні існують свої певні відмінності, які лягають в основу предметного поля й потребують більш ретельного дослідження. Водночас можна констатувати той факт, що, окрім існуючого взаємозв'язку в межах ієрархії ЕБ, одне із ключових місць займає саме підприємство як основна структурна одиниця економіки, тобто й командно-адміністративної, й ринкової, місце використання особистого потенціалу кожного працівника, що створює умови для забезпечення його особистої безпеки, та містоутворююча організація, функціонування якої сприяє вирішенню важливих економічних, соціально-культурних та інших проблем у межах певної місцевості. Відповідно до цього, перш ніж зосередитися на з'ясуванні суті ЕБП, коротко розглянемо сутність підприємства як окремої СЕС.

Правовий ракурс дослідження суті підприємства [90, с. 18] дає змогу конкретизувати позиції забезпечення безпеки в ракурсі кількох моментів: по-перше, йдеться про самостійність, що передбачає перш за все власну ініціативність щодо створення безпечних умов функціонування, що неможливо без формування відповідної СЕБП; по-друге, важливість у задоволенні суспільних потреб є підґрунтям для узгодженого досягнення цілей в сфері ЕБ на інших суміжних рівнях, що можливо в умовах підконтрольності внутрішніх процесів та здатності взаємодіяти з іншими рівнями; по-третє, підприємство

створюється для досягнення певних цілей, зокрема для задоволення інтересів власників, що потребує дієвої реалізації комплексу заходів, які повинні здійснюватися, виходячи із поточної ситуації та можливих змін, тобто із урахуванням безпекових аспектів у кожному управлінському рішенні. Останній момент є особливо важливим, адже дозволяє акцентувати увагу на дієвості як ключової ознаки підприємства, яка, забезпечуючи досягнення інтересів, водночас спричиняє порушення стану рівноваги, а відтак і зміни рівня безпеки. Цей же момент є підставою, щоб стверджувати: динамічність підприємства вимагає змін у процесі забезпечення ЕБП, тобто потребує розвитку такої системи.

Хоча трансформаційні процеси в національній економіці мають місце уже впродовж останніх тридцяти років, але ще сьогодні наявні прогалини щодо розуміння суті ЕБП. Так, спадком планової економіки можна вважати твердження, що:

- безпека будь-якого підприємства повинна бути виключно гарантована відповідними органами державної влади;
- ЕБ зводиться до організації перепускного пункту та фізичного захисту території по периметру;
- ключові загрози для підприємства виникають унаслідок дій фіскальних органів;
- процес забезпечення безпеки потребує мінімальних витрат, адже не передбачає отримання доходу;
- для стабілізації ситуації достатнім є застосування оперативних заходів на основі даних, які містяться у фінансовій звітності;
- під ЕБ розуміють виключно реагування на загрози у фінансовій сфері.

Цей перелік можна продовжити, але й зазначені позиції демонструють як нездатність частини менеджменту критично оцінити реальність ведення бізнесу в швидкозмінних умовах національної економіки, так і відсутність необхідного досвіду і бажання здобути знання в сфері організації й розвитку системи безпеки власного підприємства. Здійснене узагальнення, перед подальшим

розглядом основних підходів у трактуванні ЕБП, повинно актуалізувати важливість практичного застосування теоретичних напрацювань і пріоритетність подальшого поступу у розвитку безпекознавства.

Здійснене узагальнення дозволило виявити як суттєву активність наукової спільноти в дослідженні ЕБП, так й одночасне неоднозначне трактування цього поняття, що ускладнює практичні аспекти формування й розвитку СЕБП. Нами виділено ряд ключових підходів, які дозволяють об'єднати окремі позиції, із подальшим викладенням авторського трактування сучасних ключових параметрів ЕБП. Доволі значна кількість експертів у трактуванні ЕБП акцентують увагу на стані й процесі використання корпоративних ресурсів, що дозволило виділити так званий ресурсно-функціональний підхід. Так, Т. Васильців обґрунтовує необхідність розуміти під ЕБП «...стан найбільш ефективного використання корпоративних ресурсів для запобігання загрозам та забезпечення стабільного функціонування підприємства в даних час і в майбутньому» [13, с. 155]. Безперечно, без ресурсного забезпечення неможлива реалізація будь-яких захисних заходів, поруч з цим і надмірна орієнтація на ефективність використання корпоративних ресурсів призводить до хибної переорієнтації ЕБП на вирішення другорядних для неї завдань.

Другий підхід полягає в домінуванні захисних функцій ЕБП. Серед прихильників цього підходу можна виділити позицію Ж. Дерій та В. Базилевич, які визначають досліджуване поняття як «...стан захищеності усіх систем підприємства при здійсненні господарської діяльності в певній ситуації» [34, с. 98]. Загалом можна погодитися з тим, що досягнення й підтримання необхідного рівня захищеності усіх складових системи підприємства є одним із ключових завдань ЕБП. Водночас орієнтація виключно на протидію загрозам звужує реальні можливості суб'єктів безпеки стосовно формування безпечних умов для розвитку, в основі чого повинно лежати прогнозування можливих змін у середовищі функціонування, виявлення викликів і зменшення ризиків.

На відміну від попереднього підходу, в основі якого лежить пасивне реагування на виникнення й можливу дію загроз, наступний – третій – можна

вважати дієвим, тобто таким, що орієнтований на розроблення й здійснення заходів, які уможливають досягнення поставлених корпоративних цілей. Такої позиції дотримується З. Береза, обґрунтовуючи сутність ЕБП як «...системи постійних дій, які спрямовані на недопущення негативного впливу зовнішніх і внутрішніх факторів на діяльність підприємства і забезпечення сприятливих умов його коротко- та довгострокового розвитку відповідно до поставлених цілей» [6, с. 60]. Вважаємо за доцільне акцентувати увагу, що йдеться саме про постійні дії, спрямовані на формування безпечних умов для функціонування й розвитку підприємства.

Прихильники четвертого підходу в розумінні ЕБП відштовхуються від загальних засад створення й функціонування підприємства, тобто через досягнення певних інтересів, на чому наголошувалося вище. Так, Г. Козаченко та В. Пономарьов розглядають ЕБП як «...гармонізацію в часі та просторі економічних інтересів підприємства з інтересами, пов'язаних з ним, суб'єктами зовнішнього середовища, що діють за межами підприємства» [71, с. 4]. Власники, менеджмент, працівники та суб'єкти зовнішнього середовища у своїх діях орієнтуються на досягнення певних інтересів, які не завжди збігаються, що спричиняє виникнення внутрішніх і зовнішніх загроз. Отримання достовірної інформації для розуміння поточного стану й можливих варіантів розвитку подій зі здійсненням заходів, які б забезпечили досягнення корпоративних інтересів, можна вважати однією із ключових цілей ЕБП.

В останній – п'ятий – підхід нами об'єднано позиції науковців стосовно забезпечення стійкості й стабільності функціонування підприємства завдяки діям суб'єктів безпеки. Зазначене спирається на те, що у закордонних публікаціях існує один термін, який в українському варіанті умовно розділений на «стабільність» і «стійкість». Так, Н. Подлужна визначає ЕБП з позиції стабільності функціонування як «...характеристику системи, що самоорганізовується та саморозвивається, стан, за якого економічні параметри дозволяють зберегти її властивості: рівновагу і стійкість за мінімізації загроз» [114, с. 3]. Розглядаючи це визначення, можна виділити деякі важливі моменти:

по-перше, доцільно акцентувати на самоорганізованості та саморозвитку, в якому вбачається першочергова необхідність забезпечення безпеки самим бізнесом із подальшим систематичним удосконаленням відповідно до поточної ситуації та можливих змін у майбутньому; по-друге, не зовсім можна погодитися із міркуваннями щодо «мінімізації» загроз, можливо, потрібно здійснювати певні заходи щодо їх ліквідації або ж адаптації.

Окрім виділених п'яти ключових підходів існують й інші, але загалом вони або конкретизують певний окремий аспект процесу забезпечення ЕБП із урахуванням галузевої специфіки, або ж є комплексними. Саме з позиції комплексності цікавими є два визначення. Перше належить В. Геєцю, в якому він обґрунтовує ЕБП як «...складну динамічну систему, що забезпечує стійкість функціонування й розвитку підприємства за допомогою своєчасної мобілізації й найбільш раціонального використання трудових, фінансових, техніко-технологічних та інших ресурсів в умовах дії зовнішніх і внутрішніх загроз» [101, с. 26]. В цьому визначенні наявні складові кількох вище розглянутих підходів із доволі вдалим їх поєднанням. Для прикладу, не йдеться про ефективність використання ресурсів загалом, а їх мобілізацію й застосування для реалізації захисних заходів. Також ключовим є й акцент на необхідності формування відповідної системи, що забезпечує високий рівень узгодженості СЕБП із підприємством як системою вищого порядку. Друге визначення сформульовано Т. Гладченко, який визначає ЕБП як «...захищеність життєво важливих інтересів підприємства від внутрішніх та зовнішніх загроз, організація якої здійснюється адміністрацією й колективом підприємства шляхом реалізації системи заходів правового, економічного, організаційного, інженерно-технічного й соціально-психологічного характеру» [24, с. 112]. На нашу думку, в цьому визначенні та інших матеріалах Т. Гладченко заслуговують на особливу увагу такі аспекти: організація системи ЕБП через узгоджену взаємодію менеджменту та усіх працівників; динамічність процесу забезпечення ЕБП, що передбачає своєчасне реагування та саморозвиток такої

системи; приділення уваги не лише зовнішнім загрозам, а й внутрішнім, зокрема шляхом посилення взаємодії із правоохоронними органами.

Здійснене узагальнення, виокремлення та критичний огляд основних підходів сприяли конкретизації мети й цілей ЕБ в умовах українських підприємств (рис. 1.1).

Представлений в графічному варіанті матеріал потребує певного уточнення й пояснення. Так, в основі визначеної мети та ключових цілей є раніше проведене дослідження із узгодженням позицій та формуванням авторського розуміння. Необхідно підкреслити, що уже на цьому етапі нами формується необхідне підґрунтя для розгляду як однієї із цілей розвиток СЕБП. В умовах високої динаміки середовища функціонування незмінність такої системи ускладнює досягнення інших цілей та знижує ефективність дій суб'єктів безпеки загалом. СЕБП повинна бути на крок попереду, тобто за рахунок власного саморозвитку формувати умови для безпечного розвитку підприємства загалом. Цей момент також є вихідним пунктом для подальшого розгляду теоретичних і практичних аспектів формування СЕБП, адже лише системний підхід забезпечує необхідний рівень контролю усіх змін стосовно кожного окремого елемента та взаємозв'язок із системами вищого та нижчого порядку.

Під час розгляді процесів формування й розвитку СЕБП доцільно першочергово зосередитися на виявленні загальних параметрів системи, які і визначають місце й можливість виконання основних завдань ЕБП. Найперше можна констатувати той факт, що історичні корені поняття «система» є не менш глибокими, ніж безпеки. Зазначене ґрунтується на тому, що до виокремлення й формування теоретичних асів застосування були причетні такі відомі філософи й мислителі як Анаксагор, Левкіпп, Демокрит, Епікур, Евклід, Платон, Аристотель та інші. Лише коротко зазначимо, що параметри першої філософської системи були обґрунтовані Аристотелем. В основі результатів наукового пошуку античних філософів було визначення наявності й

взаємозв'язку між «частиною» та «цілим», зокрема і стосовно такої системи як держава.

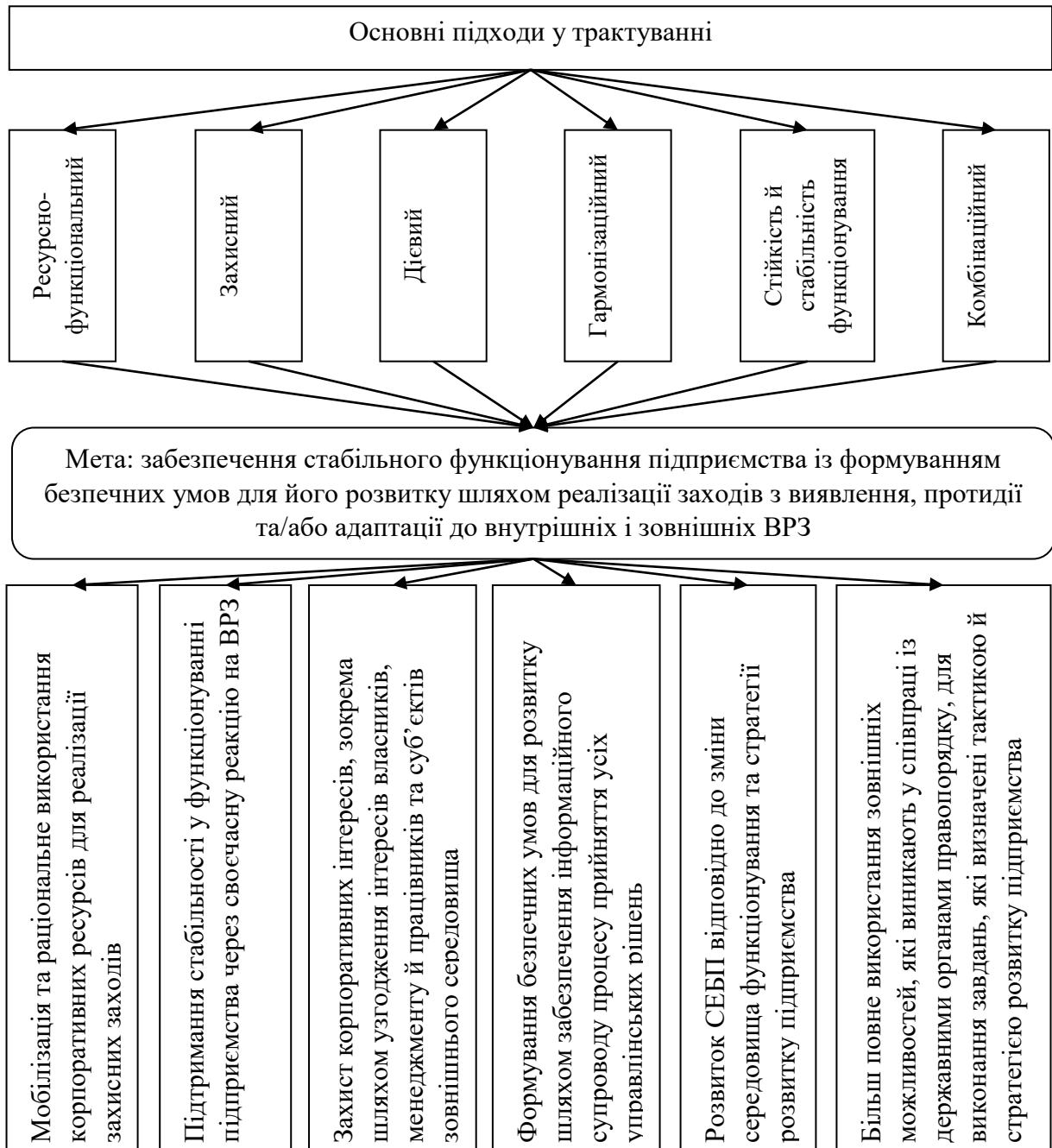


Рис. 1.1. Сутність, мета та основні цілі ЕБП, сформовано автором

Можна стверджувати, що кожна наукова школа й напрям були певною мірою дотичні до розвитку базових параметрів системи в різних сферах людської діяльності. Для прикладу, Г. Гегель розглядав, окрім названих вище складових

системи, ще й «елементи», які формують «частини», при цьому обґрунтовуючи необхідність першочергового виявлення усіх складових із подальшим встановленням взаємозв'язків між ними для формування уявлення про ціле. До науковців, роботи яких суттєво вплинули на створення теорії систем, належить Л. фон Берталанфі, в розумінні якого система становить «...комплекс елементів, що перебувають у взаємодії» [193, с. 58], а загально визнаним досягненням стала систематизація складових та визначення характеру взаємозв'язків між ними, що набуло практичного застосування і в безпекознавстві.

Зважаючи на те, що сьогодні відомі більш як 500 визначень поняття «система», нами виділено лише окремі, які в подальшому дозволили чітко окреслити базові параметри формування й розвитку СЕБП. Так, І. Зятковський доводить, що система «...складається із підсистем, що, своєю чергою, сформовані елементами, які є системами на нижчому рівні ієрархії» [57, с. 49]. Цей параметр важливий, оскільки формує уявлення як про взаємозв'язок СЕБП із підприємством як системи вищого порядку, так й структурою самої СЕБП, в межах якої доцільно виділяти системи нижчого порядку, які орієнтовані на забезпечення окремих функціональних складових ЕБП. Хибним є підхід, відповідно до якого ЕБП зводиться виключно до виявлення й протидії загрозам для фінансової безпеки через можливість їх виявлення за результатами складання фінансової звітності. За таких умов сам процес забезпечення ЕБП є пасивним із низьким рівнем результативності дій суб'єктів безпеки, адже потребує суттєво більших витрат на реалізацію захисних заходів стосовно фінансової безпеки, як результуючої складової, на відміну від послідовної ідентифікації загроз, які виникають в інших функціональних складових із подальшим реальним проявом у фінансових показниках діяльності підприємства.

О. Кутовська доводить, що під системою потрібно розуміти «...спосіб розв'язання певної проблеми, тобто як сукупність усіх необхідних знань, інформації, матеріальних засобів і способів їх використання, організації

діяльності людей, що спрямована на розв'язання проблеми» [84, с. 45]. З позиції безпекознавства проблема забезпечення ЕБП є ключовою для функціонування кожного підприємства, а відтак потребує застосування не шаблонного, а креативного й економічно обґрунтованого підходу до формування захисних редутів та пошуку нових ресурсів розвитку. Відтак актуальним є ресурсне забезпечення на належному рівні, тобто такому, що дозволить виконувати поставлені завдання, зокрема і щодо відбору, підготовки та систематичного підвищення кваліфікації співробітників служби безпеки із посиленням їх злагодженої взаємодії з іншим персоналом підприємства та зовнішніми суб'єктами безпеки.

Е. Кеннет і Н. Уотт обґрунтовують необхідність розуміння системи як «...взаємодіючий інформаційний механізм економічної діяльності підприємства, що характеризується багатьма причинно-наслідковими взаємодіями» [202, с. 15]. Найперше потрібно визнати, що основним ресурсом в діяльності суб'єктів безпеки виступає інформація. Відповідно, таке тлумачення є актуальним. Окрім цього, процес дослідження зміни рівня безпеки вимагає встановлення взаємозв'язку між динамікою внутрішньогосподарських процесів, активності суб'єктів зовнішнього середовища, ймовірності виникнення й впливу основних ВРЗ. Отримані результати, поруч із даними про спроможність суб'єктів безпеки, створюють необхідне інформаційне підґрунтя для розроблення варіантів й реалізації захисних заходів.

Здійснене узагальнення інших тлумачень поняття «система», що було здійснено з огляду на мету й ключові цілі ЕБП, дозволило виділити ключові параметри, які повинні бути покладені в основу процесу формуванні й розвитку СЕБП (рис. 1.2).

Авторська позиція щодо сукупності базових параметрів системи передбачає узагальнення наукового доробку із його інтерпретацією з позиції забезпечення ЕБП. Відповідно до цього загалом отриманий результат відрізняється від існуючих, не спричиняючи жодні суттєві суперечності,

поглиблює наукове пізнання системи й створює умови для подальшого поступу в безпекознавстві.

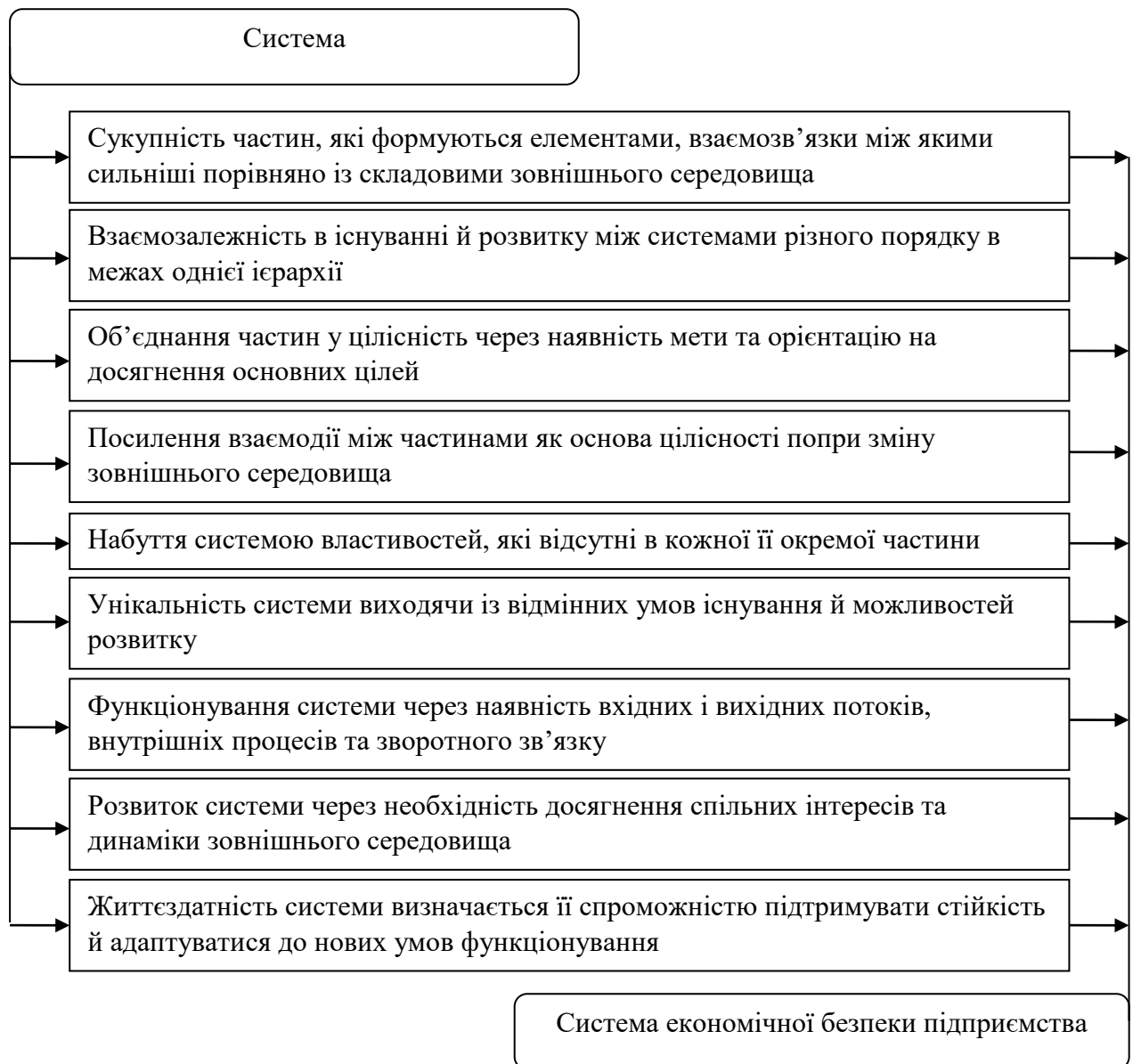


Рис. 1.2. Основні параметри системи як основа формування й розвитку СЕБП, сформовано автором

На основі послідовного розгляду суті термінів «ЕБП» та «система» сформовано необхідне теоретичне підґрунтя для виконання наступного завдання, яке полягає в окресленні методичних засад формування СЕБП. При цьому як вихідний пункт потрібно взяти той факт, що безпека є базовою

категорією для будь-якої системи, зокрема підприємства, але сама СЕБП повинна бути створена відповідно до специфіки фінансово-господарської діяльності та ступеня агресивного впливу зовнішнього середовища. Отож, актуальною є максимальна увага до процесу формування СЕБП із урахуванням складності застосування типових алгоритмів та схем без належної адаптації.

Здійснене узагальнення дозволяє стверджувати, що менеджмент більшості українських підприємств усвідомлює важливість формування СЕБП, поруч з цим виникають проблеми на рівні реалізації бажання захистити бізнес шляхом організаційних змін в межах усього підприємства, а не лише створенням окремого підрозділу із обмеженими функціями. Ускладнює вирішення цієї проблеми відсутність на теоретичному рівні узгодженого розуміння суті базового поняття, тобто СЕБП. Нами виділено три підходи, які узагальнюють позицію науковців щодо розуміння СЕБП. Так, перший підхід визначено як «структурний», адже його прихильники першочергово перелічують певні складові, які повинні бути включені як елементи в таку систему. Для прикладу, науковці під керівництвом В. Ортинського визначають СЕБП як «...комплексне утворення, до якого належать суб'єкти, об'єкти та механізми реалізації безпеки на підприємстві» [43, с. 84]. Безперечною перевагою такого розуміння СЕБП є чіткість у структуризації, яка сприяє визначенню усіх елементів із подальшою конкретизацією в умовах кожного окремого підприємства. Для цього підходу також характерна певна пасивність, адже визначення елементів без орієнтації на здійснення певних дій в більшості провокує констатацію фактів, а не реальне забезпечення високого рівня захисту.

У межах другого підходу, який нами умовно названий як «організаційний», домінують моменти, які пов'язані не лише із окресленням складу основних елементів такої системи, але й визначенням їх дій в межах безпекової діяльності. Так, О. Ілляшенко тлумачить СЕБП через «...стійку впорядкованість елементів, зв'язків та відносин між ними, які визначаються метою функціонування системи та виконуваними нею функціями і залишаються незмінними під час виконання системою її функції у різних

режимах функціонування» [61, с. 102]. Вважаємо, що в процитованому визначенні наявне трактування СЕБП як підсистеми підприємства, яка містить певну кількість елементів, функціонування яких орієнтовано на захист інтересів та забезпечення умов для розвитку. Попри те, вказується лише на досягнення окремих цілей без необхідної конкретизації процесу забезпечення безпеки, який повинен бути максимально інтегрований у всі внутрішньогосподарські процеси.

Третій підхід, який можна позначити як «діяльнісний», характеризується більшою орієнтацією на визначення можливих варіантів впливу суб'єктів безпеки на об'єкти та складові зовнішнього середовища задля досягнення поставлених перед ЕБП цілей. Ці моменти доволі чітко відображені в позиції О. Ляшенко та Ю. Погорелова, які тлумачать СЕБП як «...комплекс організаційно-управлінських, режимних, технічних, профілактичних і пропагандистських заходів, спрямованих на кількісну реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх загроз» [135, с. 25]. У межах цього підходу заслуговує на увагу зосередження уваги на визначенні інструментарію, який може бути застосований суб'єктами безпеки для реалізації захисних заходів. Певним доповненням може стати уточнення взаємозв'язку із стратегією розвитку підприємства, основні позиції якої і повинні визначати цілі й завдання для СЕБП.

Критичний огляд трьох основних підходів до трактування сутності СЕБП дозволив визначити теоретичний базис формування такої системи в умовах українських підприємств (рис. 1.3).

Авторська позиція потребує такого пояснення:

– визначення теоретичних основ нами здійснювалося із урахуванням раніше сформованої мети і цілей ЕБП, а також основних параметрів системи, що дало змогу більш чітко окреслити зміст основних трьох підходів у трактуванні СЕБП;

– вважаємо, що усі три підходи розуміння СЕБП у поданому трактуванні їх змісту є взаємодоповнюючими, що ліквідує певні, раніше існуючі, розбіжності;

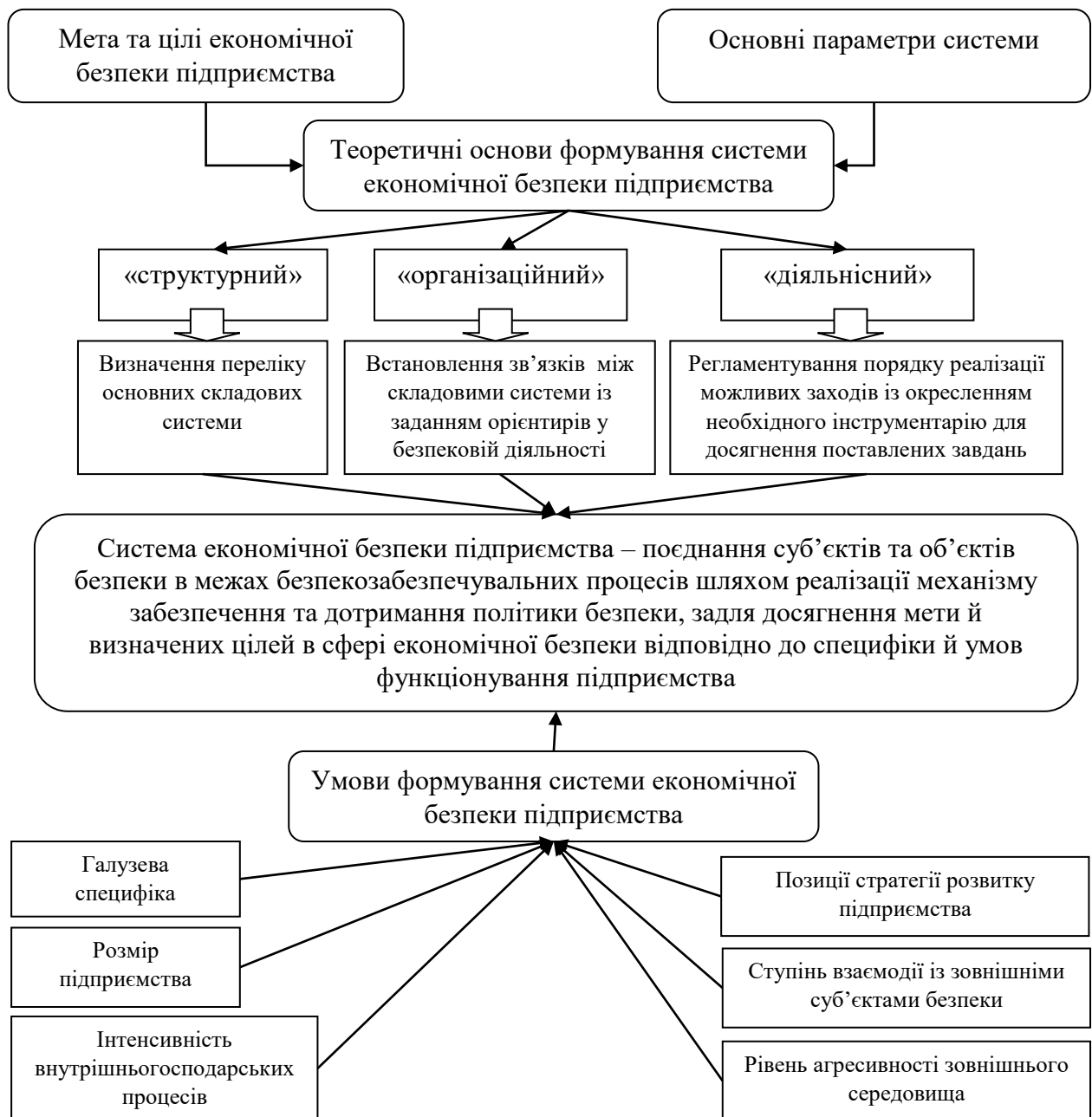


Рис. 1.3. Теоретичний базис формування СЕБП, розроблено автором

– процес формування СЕБП повинен спиратися не лише на теоретичні основи, але й здійснюватися із врахуванням низки параметрів, які безпосередньо пов'язані із конкретним підприємством. Для прикладу, перелік внутрішніх й зовнішніх ВРЗ буде відмінним для малого машинобудівного

підприємства, яке функціонує в невеличкому населеному пункті, та великої торговельної компанії в місті із чисельністю населення більше мільйона мешканців.

Попри те, що у запропоновану визначенні акцентовано увагу на таких важливих елементах як суб'єкти, об'єкти й механізм реалізації, не вважаємо за доцільне приділяти їм значну увагу. Зазначене пояснюється наявністю узгодженої позиції щодо визначення об'єктів безпеки через встановлення в межах кожного окремого підприємства того, що виконує важливу роль у його функціонуванні і потребує захисту. Суб'єктами безпеки вважаються усі підрозділи, які можуть бути задіяні для реалізації захисних заходів, а формування їх переліку й визначення функціональних завдань потребує застосування індивідуального підходу із максимальним урахуванням умов функціонування певного підприємства. Доречним буде зауваження, що оптимальним є варіант, коли формується спеціалізований підрозділ, який фактично виконує роль командного центру із додатковим доповненням функціональних завдань для усіх інших організаційних складових підприємства. Така побудова СЕБП дозволяє рівномірно концентрувати увагу на усіх функціональних складових ЕБП шляхом своєчасного виявлення й адекватного реагування на усі суттєві внутрішні й зовнішні ВРЗ. Додаткові можливості в забезпеченні ЕБП формуються за рахунок налагодження й посилення взаємодії із зовнішніми суб'єктами безпеки, зокрема правоохоронними органами. Зазначений напрям є особливо актуальним стосовно протидії рейдерському захопленню, коли власні ресурси можуть виявитися недостатніми для організації та здійснення повноцінного захисту бізнесу. Зворотній напрям взаємодії передбачає надання необхідної інформації, сприяння у підтриманні соціальної інфраструктури й розвитку місцевих громад. Питання формування й застосування механізму забезпечення ЕБП нами буде розглянуто в подальших частинах дисертаційної роботи.

СЕБП як основа життєзабезпечення кожного підприємства покликана виконувати цілий комплекс функцій. Серед науковців відсутня єдність в цьому

питанні, але в більшості дискусія триває навколо термінологічного означення. Так, І. Франчук та З. Живко доводять необхідність визначення лише двох базових функцій, які позначені як «превентивно-профілактична та оперативно-інформаційна» [50, с. 38; 155, с. 36]. М. Копитко розширює перелік таких функцій, виділяючи «...адміністративно-господарчу, господарську-розпорядчу, обліково-контрольну, організаційно-технічну, планово-виробничу, матеріально-технічну, науково-методичну, інформаційно-аналітичну, навчально-організаційну, соціально-кадрову» [75, с. 66]. Як певний проміжний варіант можна визнати позицію Н. Серебрякової, С. Волкової й Т. Волкової, які описують сутність таких функцій як «...захисна, інформаційна, регулятивна, превентивна (попереджувальна), інноваційна і соціальна» [133, с. 462]. Загалом кожен підхід характеризується наявністю раціонального змісту, свідченням чого є зосередження уваги не на фізичному захисті майна, а участі в абсолютно усіх процесах із супроводом їх реалізації, враховуючи безпекові аспекти. Поруч з цим, на нашу думку, шляхом узагальнення й критичного переосмислення, можна виділити наступні функції:

- інформаційну (передбачає відстежування змін у внутрішньому й зовнішньому середовищі з метою виявлення змін, які вказують на появу та посилення ВРЗ);
- аналітичну (узагальнення, перевірка, аналіз, визначення тенденцій та розроблення прогнозів щодо поточного рівня й можливих змін рівня безпеки під впливом внутрішніх і зовнішніх факторів);
- забезпечувальну (організації ресурсного й організаційного забезпечення, яке необхідне для розроблення й реалізації захисних заходів);
- захисну (розроблення й реалізації заходів щодо протидії та/або адаптації до впливу внутрішніх й зовнішніх загроз);
- контрольну (відстежування зміни рівня ЕБП під час реалізації управлінського впливу суб'єктів та об'єктів безпеки з метою своєчасного внесення змін та забезпечення високої ефективності безпекової діяльності й раціонального використання ресурсного й організаційного забезпечення).

Виділені нами безпекозабезпечувальні процеси полягають у здійсненні комплексу оперативних, тактичних й стратегічних заходів, які орієнтовані як на виявлення й захист підприємства від зовнішніх й внутрішніх ВРЗ, так й пошук нових ринкових можливостей для подальшого розвитку. В межах цих безпекозабезпечувальних заходів повинні виконуватися наступні завдання:

- своєчасне виявлення зовнішніх і внутрішніх ВРЗ із прогнозуванням можливого рівня їх впливу на ЕБП;
- розроблення й реалізація управлінських рішень превентивного характеру для мінімізації можливих втрат та зменшення витрат на здійснення захисних заходів;
- систематичний моніторинг рівня ЕБП та рівня агресивності впливу суб'єктів зовнішнього середовища;
- пошук й формування умов та більш повного використання ринкових можливостей, які виникають в процесі зміни середовища функціонування, як основа для розвитку;
- розвиток СЕБП шляхом удосконалення на основі набутого досвіду та прогнозів зміни в безпековій діяльності в тактичному й стратегічному часових вимірах.

Виходячи із складності формування СЕБП, цей процес повинен здійснюватися і відповідно до певних принципів, які становлять правила та умови, які дозволяють досягнути визначених цілей. Відповідно до зазначеного можна виділити таку сукупність принципів, застосування яких повинно сприяти створенню надійної та ефективної СЕБП:

- відповідності (СЕБП повинна враховувати особливості фінансово-господарської діяльності підприємства, інтенсивність внутрішньогосподарських процесів та динаміки зовнішнього середовища функціонування);
- інтегрованості (імплантація спеціалізованих підрозділів безпеки в організаційну структуру підприємства);

- безперервності (організація процесу оцінювання ЕБП, розроблення й реалізація управлінських рішень на постійній основі);
- гнучкості (здатність адаптуватися до зміни умов функціонування й коригування стратегії розвитку підприємства);
- комплексності (розроблення й реалізація заходів з огляду на результати їх впливу на усі функціональні складові ЕБП);
- раціональності (розроблення альтернативних варіантів захисних заходів й вибір оптимального виходячи із мінімізації затрат для виконання поставлених завдань);
- цілеспрямованості (орієнтація на виконання поставлених завдань відповідно до сформованого ресурсного й організаційного забезпечення);
- економічної доцільності (витрати на реалізацію захисних заходів не можуть бути більшими за можливі втрати від реалізації певних загроз).

Формування СЕБП є доволі складним процесом, який повинен здійснюватися згідно з наперед розробленим планом із конкретизацією основних етапів (рис. 1.4).

Доцільно підкреслити, що основою процесу формування СЕБП є вищерозглянуті теоретичні основи й базові умови формування, а також сформовані щодо певного підприємства функції, завдання і принципи. Як СЕБП, так і процес її формування, мають індивідуальний характер, тому нами визначено лише певні ключові етапи як орієнтири. Вважаємо за доцільне наголосити, що ключовим є останній етап, який передбачає розвиток СЕБП, адже створення не забезпечує досягнення поставлених цілей, а є лише вихідною точкою для подальшої клопіткої роботи з отриманими результатами, тобто як успіхами, так і помилками. Зважаючи на унікальність кожної СЕБП, результати її функціонування саме залежать від здатності розвиватися, що сьогодні залишається однією із найменш досліджуваних сфер у безпекознавстві.

Фактична відсутність напрацювань щодо трактування самого поняття «розвиток СЕБП» вимагає першочергового зосередження уваги на дослідженні сутності терміна «розвиток» із подальшим логічним пошуком ЕБ безпеки,

враховуючи усі вищезазначені результати щодо процесу формування такої системи.

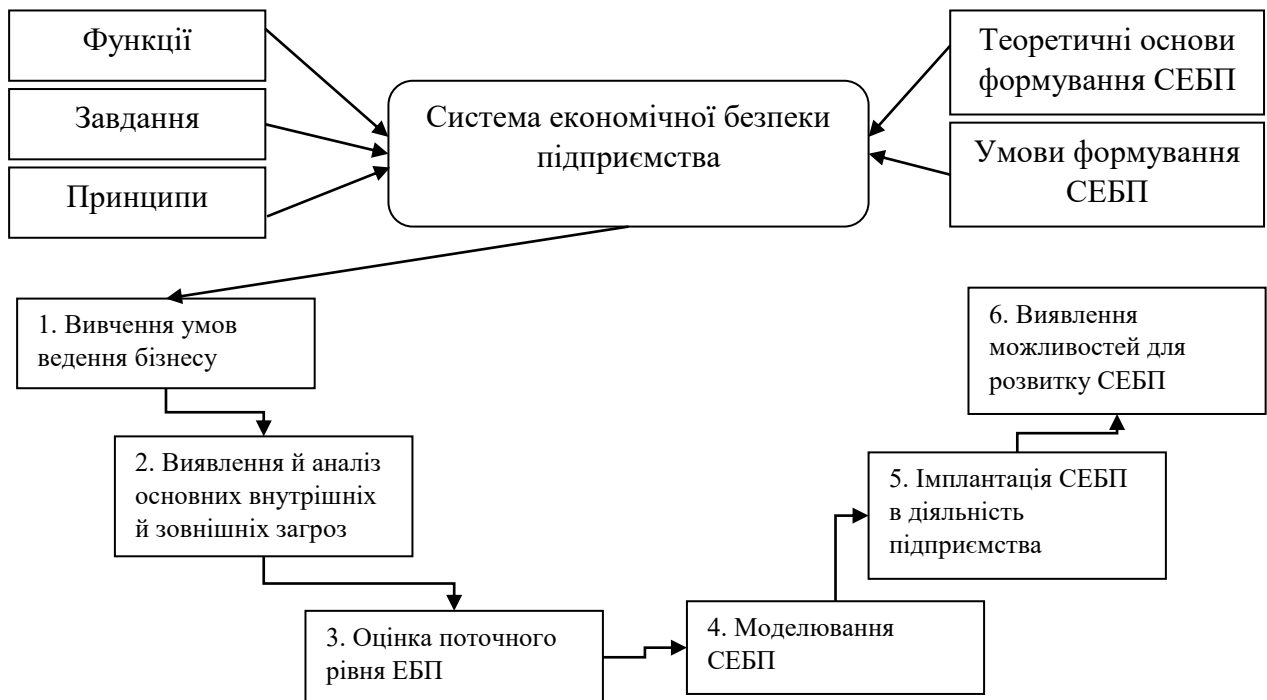


Рис. 1.4. Етапність формування СЕБП, розроблено автором

Одні із перших міркувань стосовно сутності терміна «розвиток» належать Геракліту, що вказує на значимість цієї категорії не лише для економіки, але й формування світогляду людини, починаючи з часів античності. Неоднозначність розвитку прослідковується у його відомих висловлюваннях: «...все тече, все змінюється ... не можна двічі вступити в одну й ту саму річку» [146, с. 38], в яких філософ підкреслював той факт, що не може існувати світ у стані абсолютного спокою, для нього характерні зміни, перехід до нового через руйнування попереднього. З позиції безпекознавства СЕБП повинна бути здатною адекватно реагувати на усі зміни, що неможливо за умов незмінності самої такої системи, тобто вона також повинна розвиватися.

В основі сучасного розуміння суті розвитку лежать дві концепції, тобто діалектична, поштовхом до розвитку якої стали напрацювання Г. Гегеля, та метафізична, в основу якої були покладені постулати Аристотеля. Для

формування засад розвитку СЕБП цікавою є думка Г. Гегеля про те, що «...механізм та джерело розвитку – виникнення, боротьба та подолання протилежностей» [67, с. 42]. Якщо взяти до уваги, що на рівні суб'єктів господарювання протилежності виникають через суперечності в намаганні досягнути інтереси, чим спричиняють появу ВРЗ, то СЕБП повинна постійно перебувати в режимі високої готовності для тимчасової стабілізації ситуації, контролю за видозміненням параметрів функціонування підприємства та формуванням умов до переходу на рівень, який характеризується кращим використанням ресурсів та поліпшенням конкурентного становища на ринку. Ідеї Г. Гегеля лягли в основу так званого закону «...єдності і боротьби протилежностей, який передбачає як еволюційний (безперервність, поступовість), так і революційний (перервність, стрибок) типи розвитку» [147, с.115]. У сучасному розумінні суті цього закону йдеться про розвиток не лише матеріальних об'єктів, але й нематеріальних ідей, знань, досвіду, мислення тощо. Кожен із варіантів розвитку повинен бути актуальним для СЕБП, адже поряд із покращенням ресурсного забезпечення більш важливим є накопичення досвіду та здобуття нових знань і покращення кваліфікаційного рівня суб'єктів безпеки.

Перш ніж розглянути основні підходи до трактування поняття «розвиток», вважаємо за необхідне процитувати його визначення, які містяться у філософському словнику: «... незворотна, спрямована, закономірна зміна матеріальних (організм, екосистема, підприємство) та ідеальних (мова, культура, релігія) об'єктів» [151, с. 555]. Філософи також наполягають на тому, що лише наявність трьох вказаних умов засвідчує саме розвиток, а не будь-які випадкові зміни в системі. Якщо ж зважити на доробок широкого кола науковців, то в більшості розвиток розглядають через процес, рух та зміну системи. Кожен із таких підходів має численну групу прихильників, відтак зупинимося лише на цитуванні окремих, які дотично сприятимуть формуванню теоретичних засад розвитку СЕБП. Одне із найбільш лаконічних визначень розвитку сформуване В. Бусел, в якому його подано як «...процес, внаслідок

якого відбувається зміна якості чого-небудь, перехід від одного якісного стану до іншого» [19, с. 932]. На нашу думку, будь-які зміни в умовах кожного окремого підприємства провокують порушення стану його рівноваги, тобто йдеться про виникнення нових ВРЗ, що повинно бути об'єктом уваги суб'єктів безпеки. Водночас і сам розвиток СЕБП має бути цілеспрямованим й контрольованим для досягнення поставлених завдань у межах стратегії розвитку підприємства.

Другий із визначених підходів передбачає розгляд розвитку як руху, що доволі чітко відображено у визначенні авторства С. Єрохіна: «...розвиток – особливий тип руху, що характеризує прогресивний характер взаємодії речей» [47, с. 47]. З позиції забезпечення безпеки рух характеризується високою динамікою усіх параметрів функціонування підприємства, що вимагає формування надійної інформаційно-аналітичної системи, основою якої є робота аналітиків, здатних виявити й розпізнати слабкі сигнали в зміні рівні безпеки. В контексті третього підходу О. Єрохіна доводить, що розвитком можна вважати «...якісну зміну складу, зв'язків (тобто структури) і функціонування системи, або, будь-яка якісна зміна системи» [47, с. 67]. В межах наголошеної важливості створення інформаційно-аналітичної системи актуальним є розуміння характеру усіх змін, які виникають у зовнішньому та внутрішньому середовищі, з метою як виявлення ВРЗ, так і додаткових можливостей для розвитку підприємства.

Визначені та розглянуті вище підходи стосовно суті розвитку без конкретизації сфери його застосування повною мірою відповідають тим параметрам, які використовуються при визначенні сутності терміна «розвиток підприємства». Внаслідок цього в подальшому нами будуть виділені лише окремі позиції із відповідним тлумаченням у безпековій площині. Так, у вузькому розумінні розвиток підприємства полягає у зміні діяльності, спричинені внутрішніми і зовнішніми факторами. У широкому трактуванні йдеться про структурні кількісні й якісні зміни, які забезпечують перехід на новий вищий рівень функціонування. Під кількісними змінами розуміють

фізичне укрупнення шляхом створення нових підрозділів, нарощування обсягів виробництва продукції, вихід на нові ринки збуту тощо. Якісні зміни передбачають покращення функціональності, тобто підвищення кваліфікації працівників, більш ширше застосування цифрових каналів просування товарів, виявлення резервів підвищення продуктивності праці тощо.



Рис. 1.5. Категоріальний силогізм розвитку СЕБП, сформовано автором

Авторський колектив у складі В. Пономаренка, О. Тридіда й М. Кизима розглядають розвиток як «...процес кількісно-якісних змін у системі,

ускладнення структури і складу, в результаті чого підвищується ефективність функціонування та стійкість до дестабілізуючого впливу зовнішнього середовища» [120, с. 62]. На нашу думку, вартим уваги є твердження зазначених науковців, що розвиток підприємства повинен сприяти посиленню його здатності протидіяти негативному впливу зовнішніх ризиків й загроз, тим самим покращуючи життєздатність та можливість досягнення стратегічних цілей.

Обмежуючи подальшу деталізацію окремих аспектів розгляду розвитку підприємств, нами здійснено узагальнення, яке в графічному вигляді представлено на рис. 1.5.

Нами логічно вибудовано взаємозв'язок між термінами «розвиток» і «розвиток підприємства» із актуалізацією сфери відповідальності суб'єктів безпеки в умовах певного підприємства. Отримані результати засвідчують ключову роль СЕБП у процесі розвитку підприємства. Також запропоновано власне визначення терміна «розвиток СЕБП», в якому наявний взаємозв'язок із розвитком підприємства й змінами у зовнішньому середовищі.

Отримані результати формують необхідне теоретичне підґрунтя для подальшого вибудовування методологічних засад розвитку СЕБП як ключової основи розвитку кожного підприємства в умовах високої динаміки та складно передбачуваної зміни середовища функціонування.

1.2. Цифрова трансформація економіки: систематизація наукових поглядів

Середовище функціонування українських підприємств характеризується високим динамізмом. Попри суттєвість впливу COVID-19 та військових дій на ЕБП, їх характер у часовому ракурсі все-таки можна охарактеризувати як тактичний, тобто обмежений певними нетривалими часовими рамками. В іншій площині лежать зміни стратегічного характеру, які провокують як загрози, так і

додаткові ринкові можливості. Такими змінами можна вважати ЦТЕ, яка наявна, хоча і з різною інтенсивністю, в межах кожної національної економіки. Глибоке дослідження ЦТЕ, яка безпосередньо суттєво впливає на ЕБП, вимагає послідовного виконання в межах цього підрозділу низки взаємопов'язаних завдань. Зокрема, йдеться про: виявлення етимологічних основ трансформації; характеристику ключових аспектів ПР; розгляд впливу ЦТ на стан економіки та діяльність кожного підприємства; характеристику сучасних параметрів цифрової економіки.

Відповідно до визначеного переліку завдань, першочерговим є з'ясування сутності поняття «трансформація». Можна зазначити, що його ототожнення із змінами є доволі обмеженим і не забезпечує сприйняття усієї глибини тих процесів, які тривають у будь-якій системі. Вірність цих міркувань знаходить підтвердження у трактуванні цього терміна в різних сферах застосування. Для прикладу, в математиці трансформація розглядається через перетворення Лапласа та Фур'є, в сільському господарстві йдеться про генетичну трансформацію з метою виведення більш стійкіших до зміни зовнішнього середовища та шкідників нових сортів рослин, в електромеханіці застосовуються пристрої для перетворення змінного струму, тобто трансформатори, а вивчення суспільних процесів здійснюється через фіксацію соціальних трансформацій, які стають наслідками політичних й економічних змін. Відповідно до зазначеного, поняття «трансформація» можна вважати міждисциплінарним, що проковує до більш глибокого з'ясування його сутності і стосовно економічної сфери застосування.

Окреслене вище широкє застосування поняття «трансформація» спричинило існування доволі відмінних трактувань стосовно його сутності. Нами обґрунтовано можливість визначення трьох базових підходів, які спираються на узагальнення позицій представників наукових кіл. У межах кожного підходу нами будуть уточнюватися окремі параметри безпекової діяльності в масштабах окремого підприємства як основа подальшого формування методичних засад розвитку СЕБП. Відтак перший підхід –

процесний – вбачає необхідність розуміння в трансформації певної послідовності різноспрямованих змін. Привертає увагу позиція С. Мочерного, згідно з якою під цим поняттям доцільно розуміти «...процес перетворення однієї економічної системи на іншу, що супроводжується відмиранням одних елементів, рис, властивостей і появою інших» [44, с. 687]. На нашу думку, ключовим у процесному підході є те, що такі зміни відбуваються на постійній основі, але з різною інтенсивністю внаслідок різної сили впливу зовнішніх і внутрішніх факторів. Тобто, з позиції безпекової діяльності, трансформація не сприяє становленню на будь-який тривалий період стану рівноваги, що, відповідно, вимагає як відстеження впливу ключових факторів, так і здійснення заходів для стабілізації ситуації шляхом підтримання належного рівня контролю.

Сутність другого – системного – підходу доволі лаконічно сформовано у визначенні С. Єрохіна, який трансформацію подає як «...зміну структури певного об'єкта в рамках процесу, що самоорганізовується» [47, с. 37]. На нашу думку, принципова відмінність між процесним й системним підходами полягає в тому, що перший передбачає перетворення певної системи із набуття нею нових властивостей, коли інший – окреслює внутрішні зміни, оновлення структури та взаємодії між окремими елементами. З позиції безпекової діяльності, суб'єкти безпеки повинні не лише відстежувати такі зміни, але й бути їх учасниками як консультанти через формування необхідного інформаційно-аналітичного забезпечення, розроблення прогнозів із подальшим внесенням змін у кожне управлінське рішення для мінімізації ризиків та зменшення негативного впливу ключових загроз.

В основі третього – кардинального – підходу покладено не поступові зміни, а радикальні, які можуть спровокувати суттєву видозміну будь-якої системи. Е. Тоффлер обґрунтовує доцільність розуміння під трансформацією «...значні якісні стрибки у розвитку суспільства, кожен з яких є не продовженням розвитку суспільства у попередньому напрямку, а його радикальною зміною, що можливо, заперечує попередній досвід» [21, с. 15].

Будь-які радикальні зміни провокують дестабілізацію ситуації, наслідком чого стає зміна рівня безпеки, що вимагає застосування стабілізуючих заходів із пошуком нового стану рівноваги. В межах цього підходу науковці наполягають на переході до нового стану, коли наявний досвід є малопримотний. Відтак завдання СЕБП, стосовно підтримання необхідного для функціонування й розвитку рівня безпеки, суттєво ускладнюється, потребуючи реалізації креативних рішень із здатністю оперативного корегувати процеси виконання кожного управлінського рішення.

Підводячи проміжні підсумки, можна стверджувати, що в економіці сутність терміна «трансформація» в більшості розглядається стосовно макрорівня, хоча усі виділені підходи і зроблені висновки стосовно їх суті відповідають змісту цього поняття на інших рівнях, тобто галузі, регіону й підприємства та й СЕБП. Своєю чергою ми при розгляді кожного підходу намагалися акцентувати увагу на безпекових аспектах, які виникають у межах кожного окремого суб'єкта господарювання. Узагальнення особливостей виділених трьох підходів із можливими наслідками здійснено на рис. 1.6.

Подані в графічному вигляді результати можна доповнити ще й такими уточненнями окремих позицій: хоча нами в межах відомих визначень виокремлено три основні підходи, але в межах кожного з них є спільні моменти, на яких і акцентовано увагу; незалежно від рівня розгляду трансформації, для кожної системи будуть характерні наслідки, серед яких прослідковується як порушення функціонування, так і створюються передумови для розвитку; потрібно наголосити, що для СЕБП важливим є відстеження трансформації не лише стосовно підприємства, але й на вищих рівнях, тобто держави, регіону й галузі, з метою адаптації до нових умов функціонування; трансформація характерна і для СЕБП як системи нижчого порядку, що вимагає розроблення відповідного методичного забезпечення, застосування якого сприятиме розвитку й виконанню усіх поставлених завдань.



Рис. 1.6. Сутність і наслідки трансформації системи, *сформовано автором*

Практична реалізація трансформації на макрорівні найбільш чітко проявляється у вигляді ПР, яка спричиняє суттєві зміни в економічному просторі та соціальних структурах. Сьогодні розрізняють чотири ПР, які вплинули на розвиток людства. Коротко охарактеризуємо зміст кожної із подальшим акцентом на останній, яка є актуальною сьогодні і безпосередньо впливає на процес розвитку СЕБП. Перша із згаданих революцій відбулася 1760–1830 рр., розпочалася у Великобританії і у подальшому охопила більшість країн Європи і Америки та передбачала поступовий перехід від аграрного виробництва до інтенсивного розвитку промисловості завдяки винаходу парових двигунів та широкому використанню залізниці. Важливими характеристиками першої ПР можна вважати також: зменшення частки фізичної праці на користь машинного виробництва; поступове витіснення новоствореними фабриками мануфактур; зростання продуктивності праці із

відповідним нарощуванням товарообороту; покращення рівня життя населення із одночасною розбудовою міст.

Друга ПР, яка відбулася в межах 1860–1960 рр., спираючись на досягнення першої, полягала в удосконаленні промислового виробництва через застосування конвеєрів, виробництво електродвигунів і двигунів внутрішнього згорання та застосування телеграфу для швидкого обміну інформацією. Збільшення ресурсної бази стало можливим через удосконалення технології виплавлення сталі та суттєвий поступ у добуванні й переробці нафти. Завдяки розвитку такого напрямку, як «промислова інженерія», відбулася поступова переорієнтація на задоволення потреб населення у виробництві промислових товарів, попит на які був підкріплений зростанням рівня добробуту.

У межах третьої ПР (1960–2010 рр.) автоматизація промислового виробництва та розвиток інформаційно-комп'ютерних технологій супроводжувалися розширенням кола споживачів, які почали використовувати мобільні засоби зв'язку та отримали можливість широкого застосування персональних комп'ютерів із підключенням до мережі Інтернет для задоволення власних інформаційних потреб. Технологічний прорив супроводжувався поступовою переорієнтацією на використання альтернативних джерел енергії та більш раціональною експлуатацією природних ресурсів з метою досягнення цілей сталого розвитку.

Перш ніж розглянути сутність четвертої ПР, яка відбувається у сьогоdnішніх реаліях, необхідно підкреслити факт неоднорідності трансформації в межах кожної країни, коли чітко виділяється група країн-лідерів, які стали флагмани технологічного поступу, але є й регіони, у яких виникають труднощі із повномасштабною реалізацією другої та третьої ПР. Це становить необхідну основу для розгляду четвертої ПР, до здійснення якої долучилися сьогодні лише окремі країни, тим самим поглиблюючи технологічний розрив із іншими та поступово відводячи їм роль сировинної бази.

Експерти в своїх оцінках обґрунтовують те, що в основі четвертої Пр лежать здобутки попередньої, тобто третьої. Так, автоматизація переходить на вищій рівень, коли машини взаємодіють між собою з мінімальною участю людини, крім того, створюються повністю автономні заводи, де отримання ресурсів, сам процес виробництва та відвантаження продукції потребує лише загального контролю обмеженого кола фахівців. Цей приклад ілюструє лише незначну частину трансформацій, які радикально змінюють економічне середовище, а відтак і усі соціально-економічні процеси. Розвиток робототехніки й нанотехнологій уможливили об'єднання фізичних, біологічних та цифрових технологій із подальшим створенням кіберфізичних систем.

Зважаючи на те, що трансформації в межах четвертої Пр відбуваються сьогодні, тобто фактично в реальному часі, то існує проблема чіткості характеристики усіх змін. Підтвердженням цієї тези можуть слугувати результати опитування 150 експертів таких країн-лідерів, як Німеччина, США, Японія, Китай, Південна Корея та Великобританія, щодо розуміння основних параметрів цієї новітньої Пр. Серед опитаних домінуючими були наступні точки зору: «...26% – розроблення мереж та цифрових технологій; 20% – смарт-товари; 20% – оптимізація виробництва; 18% – автоматизація і 16% – нові бізнес-моделі» [201]. Іншим, не менш важливим, моментом є те, що в публікаціях доволі часто здійснюється ототожнення четвертої Пр та терміна «Індустрія 4.0». Початково Індустрія 4.0 окреслювала стратегію розвитку промисловості в Німеччині (орієнтація на створення автономних ПП для утвердження технологічного лідерства у міжнародному економічному просторі), але в подальшому отримані результати в процесі її реалізації сприяли розширенню значення цього терміна до розуміння під ним суті усіх трансформацій. Поруч з цим у межах кожної країни-лідера розроблений свій стратегічний план із відмінними акцентами технологічного поступу. Для прикладу, в США з 2014 р. реалізується стратегія «Промисловий Інтернет», в межах якої, завдяки посиленню взаємодії між науковими установами, державними органами та представниками бізнесу, здійснюється виробництво і

популяризація «інтернету речей». Японія (стратегія «Промисловий ланцюжок створення вартості») вбачає можливість отримання кращих результатів завдяки створенню кіберфізичних систем, а Франція (стратегія «Індустрія майбутнього») нарощує кількість робіт, які використовуються не лише в промисловості, в усіх секторах економіки. Україна також робить кроки з метою недопущення технологічного відставання від інших країн (у 2018 р. була затверджена стратегія «Індустрія 4.0»), але в більшості зусилля скеровуються на розвиток не високотехнологічного промислового виробництва, а системи продукування інформаційних послуг. Можна стверджувати, що на фоні збільшення фізичного й морального зносу технічної бази ПП та їх фактичної інноваційної пасивності орієнтація виключно на сферу послуг не сприятиме повноцінній ЦТ національної економіки. Не менш важливим моментом є констатація того, що Індустрія 4.0 здійснюється не в межах окремих компаній, а роль ініціатора та джерела енергії, зокрема в фінансових ресурсах, виконує держава. Так, сукупні інвестиції в реалізацію згаданої стратегії в Німеччині у 2020 р. перевищили 2 млрд євро, а динаміка їх обсягу має характер до поступового суттєвого зростання із 0,35 млрд євро у 2013 р. [142, с. 63]. У США створений Консорціум промислового інтернету, учасниками якого є понад 170 організацій, діяльність яких за урядової підтримки орієнтована на виготовлення високотехнологічної продукції із її подальшим просуванням на глобальному ринку для досягнення національних інтересів США.

В основі Індустрії 4.0. лежить чимало технологій, комплексне застосування яких і забезпечує трансформацію національної економіки у межах кожної окремої країни-лідера. Зважаючи на те, що розгляд суті кожної з таких технологій загалом не сприяє вирішенню поставлених в межах підрозділу завдань, нами виокремлено ключові параметри, які їх об'єднують та дотичні до проблематики розвитку СЕБП у промисловості: високий рівень автоматизація із об'єднанням усіх машин на основі промислового інтернету; потокове виробництво із встановленням на вході на сировині й матеріалах міток для контролю не окремої операції, а процесу загалом, з мінімальною участю

людини; орієнтація на задоволення індивідуальних потреб споживача через максимальну гнучкість виробничого процесу; зниження матеріало- та енергомісткості виробництва; пріоритетність повторного використання ресурсів; застосування відновлювальних джерел енергії та зменшення негативного впливу на навколишнє середовище. Порч із суттєвими перевагами, які створюються завдяки Індустрії 4.0, необхідно наголосити на тому, що зменшення кількості працівників унаслідок автоматизації із одночасним зростанням вимог до кваліфікації й здатності генерувати нові ідеї й приймати креативні рішення, певним чином видозмінюють перелік завдань для СЕБП, тим самим актуалізуючи її розвиток.

Завершуючи розгляд суті четвертої ПР як трансформації, що виникає в країнах-лідерах та стає життєво важливою для інших задля розвитку й досягнення національних інтересів, вважаємо за необхідне наголосити на актуалізації низки проблем, які дотично впливають на розвиток СЕБП. Перша така проблема пов'язана із зменшенням потреби в людських ресурсах через високий рівень автоматизації, що провокує загострення соціальної нестабільності. Поруч із цієї проблемою постає й інша, яка полягає у збільшенні розриву у рівні доходів між працівниками, котрі здатні генерувати нові знання, та іншими, які виконують роботи, що не можна замінити машинами, але не є складними. Розрив у рівні життя в різних за технологічним розвитком країнах провокує міграційну проблему із подальшим загостренням демографічної кризи. Нові можливості, які створюються завдяки цифровізації, супроводжуються й посиленням проблеми із безпекою даних та поглибленням цифрової нерівності не лише в ракурсі окремих країн, але й регіонів та місця проживання. Відбувається зміна структури економіки, коли частка промислового виробництва зменшується внаслідок зростання торгівлі через активну розбудову торговельних мереж на основі широкоформатного Інтернету із постійним збільшенням кількості абонентів. Поруч із орієнтацією на більш раціональне використання корисних копалин сам процес трансформації вимагає збільшення обсягів видобування таких ресурсів для створення більшої кількості

роботів, не обмежуючи потреби населення планети, чисельність якого зростає. Визначений неповний перелік проблем створює необхідну основу для подальшого розгляду ЦТ для обґрунтування варіантів розвитку СЕБП.

Поруч із необхідністю розвитку СЕБП в умовах ЦТ актуалізується ще й питання своєчасності здійснення цього процесу, що визначається швидкою динамікою структурних змін у національній економіці. Серед результатів досліджень українських аналітиків можна виділити кілька ключових моментів. Так, вказується, що «...95% підприємств не відповідають вимогам нового цифрового бізнесу, а 12% у своїй діяльності користуються застарілими інформаційними технологіями» [30, с. 6]. Зважаючи на те, що дослідники засвідчують факт визнання підприємствами, які уже здійснили реальні кроки з ЦТ, про зростання рівня конкуренції у кілька разів, то розроблення методичних засад розвитку СЕБП для підконтрольності й керованості такими процесами на більшості українських підприємств стає особливо актуальним. Відповідно до цього, нами виокремлено і в графічному вигляді подано як основні параметри ЦТ без заглиблення у технічні нюанси, так і нові можливості та виклики й загрози, які можуть стати актуальними для певного ПП (рис. 1.7).

Суть і можливі наслідки трансформації на рівні окремого підприємства доцільно доповнити розглядом ЦТЕ. Обґрунтуванням такого підходу є хоча б те, що створення необхідного середовища, яке уможливило розширення цифрового обміну між суб'єктами господарювання, споживачами, органами державної влади, місцевими громадами тощо створюється в процесі реалізації масштабних інфраструктурних проектів. Окрім цього, потрібно пам'ятати, що стимулюючим фактором також виступає зростаючий попит, підсилений реальним покращенням купівельної спроможності населення. Загалом розгляд безпекових аспектів ЦТ повинен урахувати, окрім вище виділених можливостей, викликів й ризиків, суттєво ширше коло факторів, яке пов'язано зі змінами на рівні національної економіки.



Рис. 1.7. Ключові параметри та можливі результати ЦТП з позиції забезпечення його економічної безпеки, *сформовано автором*

Нами виділено ряд таких факторів, тобто сприяючих і гальмуючих, зважаючи на реальне становище поточного рівня ЦТЕ в Україні. Так, до стимулюючих факторів належать:

– покращення мережі мобільного зв'язку із розширенням кола користувачів швидкісного Інтернету, застосування технології BigData, «хмарних» технологій тощо, що створюють кращі умови для просування товарів малими та середніми товаровиробниками;

- активне впровадження новітніх технологій, які ґрунтуються на використанні штучного інтелекту, нейронних мереж, цифрових платформ тощо, що дозволяє вітчизняним підприємствам виходити й конкурувати на зовнішні ринки, зокрема і країн-лідерів технологічного поступу;

- спрощення процесу взаємодії бізнесу, органів державної влади й місцевого самоврядування на основі ЦТ регулювання підприємницької діяльності (е-урядування), сплати податків, контролю за використанням бюджетних ресурсів;

- покращення системи підготовки фахівців, задіяних у розвитку інформаційно-комунікаційних технологій, як на основі створення представництв іноземних компаній, так і збільшення державного фінансування спеціалізованих закладів освіти;

- створення сприятливих умов для функціонування ІТ-компаній на місцевому рівні, зважаючи на високий рівень оплати праці її персоналу, задоволення потреб якого формує підґрунтя для розвитку соціальної інфраструктури та створює додаткові робочі місця.

Окремо хочемо наголосити, що під час останньої пандемії, яка була спричинена вірусом COVID-19 і супроводжувалася значними обмеженнями щодо фізичного контакту, зокрема функціонування значної кількості підприємств, цифровий стрибок окремих країн дозволив продовжувати роботу компаніям на основі технології віддаленого доступу до робочого місця. Відтак завдяки ЦТЕ бізнес продовжив роботу, тим самим знизивши рівень падіння виробництва, а відтак і запобігши більш суттєвим загрозам для соціальної сфери.

Вплив гальмуючих факторів нами уже частково розглядався в процесі дослідження сутності терміна «трансформація», зокрема стосовно потреби в робочій силі та зміни вимог до кваліфікації персоналу на фоні дедалі вищої автоматизації промислового виробництва. Відтак конкретизуємо орієнтовний перелік таких факторів:

– зменшення потреби в робочій силі проявляється не лише стосовно працівників, які виконують фізичну працю, але й так званих «білих комірців» через дедалі активніше застосування штучного інтелекту, наслідком чого стало посилення соціальних збурень, так і зниження купівельної спроможності населення. Так, за прогнозами експертів, «...передбачається, що до 2030 р. понад 60% процесів будуть автоматизовані» [35, с. 47];

– для компаній зменшення витрат на оплату праці через скорочення кількості працівників супроводжується одночасним зростанням потреби у висококваліфікованих фахівцях, які здатні обслуговувати складні кіберфізичні системи, залучення яких і підготовка ускладнюється поляризацією кадрів за рівнем отриманих знань і володінням цифровими технологіями;

– відмінність у рівні ЦТЕ проковує поглиблення міграційної кризи, зокрема щодо виїзду на постійне місце проживання ІТ-фахівців, рівень оплати праці яких в іноземних компаніях у кілька разів вищий, із створенням сприятливих умов для подальшого професійного зростання;

– подальша соціальна поляризація суспільства через зростання розриву в оплаті праці між працівниками, які виконують некваліфіковану фізичну працю, та тими, які задіяні в розвитку інформаційно-комунікаційних технологіях, із подальшим зростанням бар'єрів для переходу із однієї групи в іншу;

– поглиблення технологічного відставання з орієнтацією на видобування та реалізацію на зовнішніх ринках сировини із низьким рівнем доданої вартості, завдяки слабкому контролю за використанням природних ресурсів й наявністю дешевої робочої сили. Гальмування ЦТЕ відбувається через відсутність попиту як з боку підприємств, які не орієнтовані на удосконалення технології, так і населення, незначні доходи якого дозволяють пріоритетно задовольняти лише першочергові фізіологічні потреби.

Узагальнюючи, можна стверджувати, що визначений перелік різноспрямованих факторів, що виникають через ЦТЕ, формує необхідне інформаційне доповнення для розуміння умов розвитку СЕБП, зокрема у

чіткості визначення пріоритетів та обґрунтування ресурсного забезпечення для їх досягнення.

В основі попереднього розгляду термінів «трансформація», «ЦТ» та «ЦТЕ» наявні ключові ознаки цілеспрямованого процесу, який супроводжується певними змінами. Попри відмінності у рівнях реалізації, спільною є орієнтація. Можна стверджувати, що сучасною орієнтацією для ЦТ національної економіки країн-лідерів стала побудова цифрової економіки. Її параметри і сьогодні до кінця ще не визначені, адже формуються в межах двох останніх ПР, де інформація й знання, як нелімітовані ресурси, почали виконувати ключову роль у задоволенні потреб населення із дотриманням принципів сталого розвитку.

Вище ми уже згадували про внесок Д. Топскотта і Н. Негропонта в розвиток сучасного трактування поняття «цифровізація». Ці ж науковці започаткували теоретичне обґрунтування цифрової економіки, спростовуючи можливість застосування таких термінів як «нова економіка», «інтернет-економіка», «веб-економіка», аргументуючи посилення впливу інформаційно-комунікаційних технологій на усі сфери людської діяльності, а не лише стосовно процесу обміну інформацією. Д. Торскотт у своїй науковій праці «Електронно-цифрове суспільство: плюси і мінуси епохи мережевого інтелекту» запропонував розуміти під цифровою економікою «...економічну діяльність яка, на відміну від традиційної економіки, визначається мережевою свідомістю та залежністю від віртуальних технологій» [206]. Для обґрунтування власних міркувань Д. Торскотт назвав та розкрив зміст п'яти базових елементів такої економіки: «...ефективна особистість; високопродуктивний колектив; інтегроване підприємство; розширене підприємство; ділова активність міжмережевого середовища» [206]. Усі елементи наведені в ієрархічній послідовності, при цьому їх об'єднує приналежність до цифрового середовища, яке утворюється як кожною окремою особистістю, яка володіє необхідними знаннями для роботи з пристроями, підключеними до Інтернету, так і підприємством, яке завдяки інформаційно-

комунікаційним технологіям здатне, інтегруючи відокремлено функціонуючі підрозділи, швидко відгукуватися на потреби споживача, водночас діючи без будь-яких географічних обмежень. Відповідно до запропонованого визначення й виокремлених елементів йдеться про формування економіки, яка радикально змінює як засади здійснення фінансово-господарської діяльності підприємства, так і процес забезпечення його економічної безпеки. Зазначене також набуває підтвердження і в аргументах Н. Негропонта стосовно переваг цифрової економіки порівняно із традиційною: «...віртуальний характер господарських зв'язків; відсутність фізичної ваги продукції, еквівалентом якої є інформаційних обсяг; низький рівень витрат на виробництво електронних товарів та менша площа, яку займатимуть електронні засоби та носії; миттєвий глобальний обмін даними через Інтернет; поява нових цифрових валют» [204, с. 48]. Кожну із визначених переваг доцільно також розглядати і з точки зору безпечності як таку зміну, що сприяє досягненню певних цілей, але водночас є і джерелом нових викликів, які повинні бути вивченими суб'єктами безпеки із подальшим розробленням відповідних захисних заходів для недопущення виникнення нових загроз. Зважаючи на те, що сьогодні аналітики визначають частку, яку займає цифрова економіка в структурі національної окремих країн, то для СЕБП дедалі актуальнішим є саморозвиток для набуття здатності реагувати на типові та новітні ризики, виклики й загрози, що виникають у результаті ЦТ.

Фактичну високу швидкість формування цифрової економіки засвідчує хоча б те, що згадана вище книга Д. Топскотта була опублікована у 1996 р., а у 1998 р. цей термін застосовувався у щорічному звіті Міністерства торгівлі США для пояснення високих темпів розвитку окремих секторів, що стало результатом активного впровадження інформаційно-комунікаційних технологій. У 2015 р. у межах проведення саміту G20 обговорювалися нові можливості й виклики, виникнення яких стало результатом формування цифрової економіки. У 2016-му, в межах поглиблення співпраці країн-лідерів, цифрова економіка уже розглядалася як один із ключових факторів, що може

забезпечити зростання продуктивності праці та досягнення цілей сталого розвитку. Узагальнюючи короткий історичний екскурс, вважаємо за доцільне зазначити, що в цифровій економіці поруч із традиційними факторами виробництва (земля, праця й капітал) розрізняють й нові, тобто знання й інформацію, які є нелімітованими, а відтак сприяють більш ефективному використанню природних ресурсів для задоволення поточних потреб населення та майбутніх поколінь.

Перш ніж зосередитися на розгляді основних підходів до трактування цифрової економіки, доцільно підкреслити, що Україна навздогін за країнами-лідерами здійснює реальні кроки для збільшення частки цієї складової національної економіки, основою чого стала схвалена у 2018 р. Концепція розвитку цифрової економіки та суспільства на 2018–2020 рр. У цьому важливому документі зазначається, що «...у класичному розумінні поняття «цифрова економіка» означає діяльність, в якій основними засобами (факторами) виробництва є цифрові (електронні, віртуальні) дані як числові, так і текстові» [124]. Попри доволі загальне подання змісту цифрової економіки, до суттєвих особливостей цього документу можна віднести окреслені та обґрунтовані напрями цифрового розвитку, які охоплюють практично усі сфери діяльності сучасної людини, зокрема громадську безпеку.

Ретельне вивчення відомих визначень поняття «цифрова економіка» дало змогу виявити таку проблему як поступову зміну поглядів через результати подальшого технологічного поступу. Якщо на перших етапах йшлося про додаткові можливості, які отримували товаровиробники від використання Інтернету, то в подальшому визначення меж зміни економічних процесів унаслідок застосування інформаційно-комунікаційних технологій стає дедалі складнішим. Зазначене можна проілюструвати за допомогою трактування цифрової економіки, яке сформовано співробітниками Центру Разумкова, де зазначається, що «...це економіка, що базується на цифрових комп'ютерних технологіях та інформаційно-комунікаційних технологіях (ІКТ), але на відміну від інформатизації, ЦТ не обмежується впровадженням інформаційних

технологій, а докорінно перетворює сферу і бізнес-процеси на базі Інтернету та нових цифрових технологій» [161, с. 25]. На нашу думку, в цьому визначенні підтверджується те, що цифрова економіка є результатом ЦТ, але не йдеться про звичайне оцифрування, тобто переведення аналогових ресурсів у цифрові, чи забезпечення споживачам вільного доступу до нових джерел інформації, а вказується на докорінну зміну за рахунок нових технологій. Тобто Інтернет залишився на початковому рівні, а сьогодні для отримання конкурентних переваг потрібним є застосування таких технологій як Big Data, «Промисловий інтернет», «Інтернет речей», блокчейн тощо. Цим же вказується на те, що розвиток цифрової економіки не припиняється, а полягає в подальших ЦТ, що з позиції безпекознавства вимагає відповідного розвитку СЕБП.

Умовне відокремлення низки позицій, які сьогодні можна вважати проміжними, все-таки дозволило виділити два ключові підходи у розумінні цифрової економіки. В межах першого науковці розглядають цифрову економіку в ракурсі технологічного стрибка в задоволенні потреб сучасної людини. Так, у розумінні М. Нікрема досліджуване поняття визначає «...частину загального обсягу виробництва, створювана різними «цифровими ресурсами». Ці ресурси включають цифрові навички, цифрове обладнання (комплектуючі, програмне забезпечення і засоби зв'язку) і проміжні товари та послуги, що використовуються у виробництві» [208]. Основу цього підходу утворюють класичні параметри Індустрії 4.0 як стратегії промислового виробництва у Німеччині. Відповідно, прихильники цього підходу відштовхуються від ЦТП із подальшим поширенням цифрових технологій на процеси взаємодії із споживачем.

Другий підхід передбачає розгляд цифрової економіки в структурі національної економіки. Для прикладу, В. Пілінський дотримується думки, що «...цифрова економіка є складовою частиною економіки, в якій домінують знання суб'єктів та нематеріальне виробництво – основний показник під час визначення інформаційного суспільства» [112]. З цієї позиції формування

цифрової економіки є ключовим завданням для України в контексті здобуття належної конкурентної позиції відповідно до наявного потенціалу.

Узагальнюючи, можна стверджувати, що, без заглиблення в технічні аспекти, фактичне поєднання обох підходів формує цілісне уявлення про суть цифрової економіки як такої, яка на основі новітніх цифрових технологій переформатовує усі соціально-економічні процеси в межах національної економіки кожної країни, надаючи поштовх до розвитку. Ця теза може також слугувати основою для подальшого розгляду параметрів цифрової економіки, перший з яких полягає в уточненні структури та її місця в межах національної економіки.

В основі традиційного сегментування економіки лежить концепція, яку запропонував ще у 1841 р. Ф. Ліст у науковій праці «Національна система політичної економії, міжнародної торгівлі, торгова політика й німецький митний союз». Ця концепція, яка була в подальшому розгорнута К. Кларком, Ж. Фурастьє, А. Фішером та іншими послідовниками, передбачає виділення таких трьох секторів як «...первинний (сільське господарство), вторинний (промисловість), третинний (сфера послуг)» [79, с. 44]. Своєю чергою, науковці, які розпочали формувати теоретичні основи цифрової економіки, серед яких можна виділити Т. Мезенбурга, розглядають три її компоненти, зокрема такі як «...підтримуюча інфраструктура, електронний бізнес і електронна комерція» [207]. Ще один варіант структуризації цифрової економіки був запропонований Р. Клінгом та Р. Лемпом, які доводили необхідність виділення таких компонентів як «...високоцифрові товари і послуги; змішані цифрові товари та послуги; ІТ-інтенсивні послуги чи виробництво товарів; сегменти ІТ-індустрії» [203]. На нашу думку, фактично штучне відокремлення частини економічних процесів, які здійснюються із більш активним використанням ІКТ та цифрових технологій, сьогодні стає дедалі менш актуальним внаслідок активності поширення таких ЦТ стосовно більшості соціально-економічних процесів і не лише в країнах-лідерах. Відтак, з практичної точки зору, для здійснення аналізу частки цифрової економіки

доцільно використовувати методику ОЕСР, яка фактично поєднує класичне сегментування із бажанням виділити ті складові, які характеризуються більш активним застосуванням цифрових технологій. Умовний поділ передбачає розрізнення таких стратегічних секторів: «...перший і другий сектори охоплюють галузі високотехнологічного та середньо-високотехнологічної промисловості, четвертий і п'ятий – ділові послуги, а шостий – соціально спрямовані види діяльності сфери послуг, що забезпечують повноцінний розвиток людини» [205, с. 166]. Вважаємо, така структуризація дозволяє реально оцінити хід ЦТ у межах певної національної економіки, адже йдеться не про аналіз кількості мобільних телефонів, які використовує населення для доступу до інформаційних ресурсів й обміну даними в межах цільової аудиторії соціальних мереж, чи якість покриття інтернетом окремих регіонів, а пріоритетне виробництво високотехнологічної промислової продукції. Тобто в основі такої структуризації прослідковується ідея Індустрії 4.0, де найбільша увага приділяється промислому виробництву, тобто максимальній автоматизації фармацевтичних, хімічних та машинобудівних (комп'ютерна і телекомунікаційна техніка, авіа- і ракетобудування) підприємств, які становлять основу першого і другого секторів.

Як підсумок проведеного дослідження, нами визначено ті аспекти, стосовно усіх попередньо послідовно розглянутих понять, які безпосередньо актуалізують необхідність формування методичних засад розвитку СЕБП (рис. 1.8).

Додатково потрібно врахувати динаміку розвитку цифрової економіки. В матеріалах аналітичного агентства McKinse вказується, що «...частка цифрової економіки у ВВП країн ЄС складає 8,2%, США й Китаю – 10%» [163, с. 95]. Зважаючи на вище розглянуту відмінність у структуризації цифрової економіки, такі дані можна використовувати виключно як орієнтири. Відтак інформація про те, що частка цифрової економіки в Україні може становити лише 3%, є більше негативним фактом.

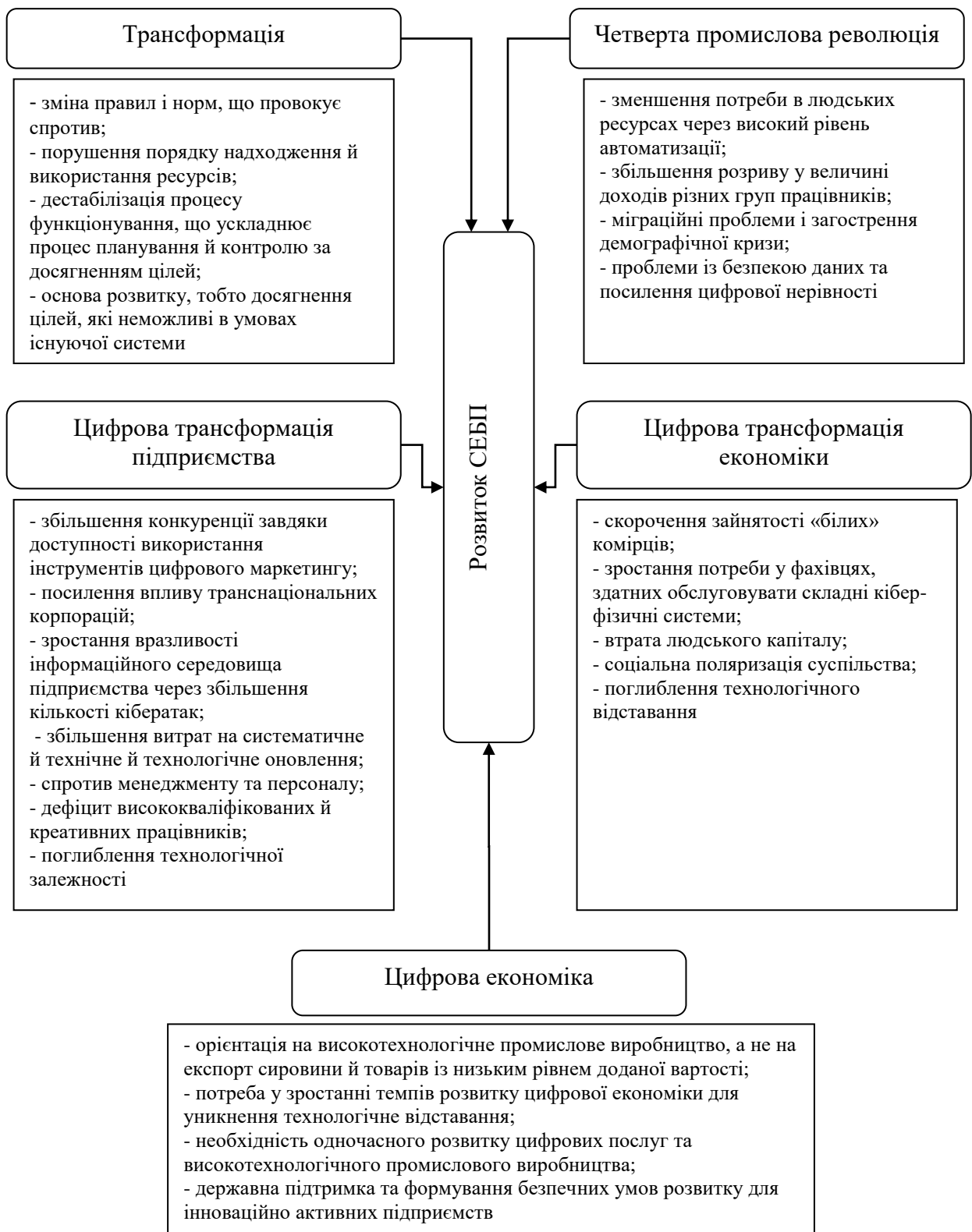


Рис. 1.8. Систематизація передумов розвитку ЕБП в умовах ЦТЕ, *сформовано автором*

Цей висновок можна вважати правильним з урахуванням того, що аналітики прогнозують зростання в країнах-лідерах зазначеної частки у складі ВВП 2025 року до рекордних 20–34%. Для нашої країни, внаслідок посилення поточної орієнтації на розвиток сільського господарства й видобування корисних копалин з подальшим експортом продукції із незначним рівнем доданої вартості, такі тенденції є швидше новим викликом, результатом чого може бути поглиблення технологічного відставання. Додатково потрібно зважити на ще одну особливість розвитку цифрової економіки в Україні, яка окреслена в публікації Г. Ус та О. Коваль як «...сервісна, що характеризується наданням державних послуг та послуг з реалізації товарів» [148, с. 71].

На відміну від практики країн-лідерів, які створюють сприятливі умови для розвитку ПП шляхом ЦТ із подальшим розширенням переліку й обсягів виробництва високотехнологічної продукції, в нашій країні домінує використання іноземної промислової продукції й цифрових технологій в сфері послуг. Безперечно, проект «Цифрова держава» та покращення сервісу в банківському секторі є важливими результатами ЦТ, але послуги вважаються вторинним в економічному механізмі національної економіки, коли первинним залишається виробництво, будучи визначальним за конкурентної боротьби на міжнародних ринках. Окрім цього, подальша орієнтація суто на сферу послуг буде провокувати посилення такої загрози як зростання техніко-технологічної залежності від іноземних товаровиробників комп'ютерного обладнання та ІКТ із одночасним руйнуванням власного промислового комплексу.

Вважаємо за доцільне підкреслити, що внаслідок наявного взаємозв'язку між базовими поняттями окремі аспекти щодо необхідності розвитку СЕБП є спільними. Також важливо, що нами сконцентровано увагу на кількох площинах із урахуванням поточних тенденцій. Так, йдеться про трансформацію будь-якої СЕС, із подальшою конкретизацією на рівні національної економіки та окремого підприємства. Такий підхід сприяв формуванню цілісного уявлення, а також доведенню наявності суттєвих підстав для розвитку СЕБП. Окремо акцентовано увагу на важливості створення безпечних умов для покращення

інноваційної активності ПП, адже саме високотехнологічна продукція, а не лише цифрові технології, можуть забезпечити формування цифрової економіки в нашій країні. Отримані результати будуть у подальшому доповнені аналітичними даними, а також використані як необхідне підґрунтя для створення теоретико-практичних засад розвитку СЕБП.

1.3. Концептуальне підґрунтя розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки

В основі розвитку СЕБП повинно бути покладено комплексне врахування активності в застосуванні новітніх технологій у виробництві й управлінні підприємством та виникнення й вплив нових ВРЗ із подальшим формуванням варіантів кількісно-якісних змін у процесі забезпечення ЕБП для досягнення тактичних і стратегічних цілей. Відповідно до зазначеного, в межах цього підрозділу нами буде здійснена спроба: уточнити теоретичні засади виникнення та впливу на ЕБП ВРЗ із урахуванням їх змісту в процесі ЦТП; конкретизувати ті зміни, які виникли під час ЦТП, спираючись на загальне розуміння ЦТ на макро- та мікрорівні, яке було окреслено у попередньому підрозділі; сформувавши концептуальне підґрунтя розвитку СЕБП, зважаючи на характер змін середовища функціонування підприємства та внутрішніх процесів через цифровізацію. Така постановка завдань ґрунтується на міркуваннях щодо необхідності досягнення синхронності в розвитку підприємства та його СЕБП. Крім того, можна стверджувати, що дії суб'єктів безпеки повинні формувати безпечну основу для таких змін, спираючись на можливості виникнення ризиків і загроз. Водночас зростає актуальність застосування цифрових технологій і в безпековій діяльності та формування безпекового потенціалу як основи розвитку СЕБП. Визначені завдання будуть виконуватися послідовно з метою формування відповідного концептуального підґрунтя розвитку СЕБП, належна увага чому сьогодні не приділяється.

Відповідно до визначеного переліку, зосередимося на уточненні сутності таких понять як «виклик», «ризик» та «загроза». Інколи їх об'єднують в певну групу і окреслюють як «деструктивні» або «дестабілізуючі» фактори, зважаючи на те, що їх виникнення та можливий вплив порушують стан рівноваги підприємства. Серед науковців немає одностайності щодо розгляду виклику як такого фактору, що спричиняє вплив на ЕБП. Зазначене пояснюється неоднозначністю розуміння його впливу та необхідності формування певної реакції, з огляду на складну протидію й ключові внутрішні й зовнішні загрози. Для уточнення цього складного питання було узагальнено позиції щодо розуміння виклику в довідниковій літературі та публікаціях науковців. У Великому тлумачному словнику виклик подається як «...вимога, спонукання до будь-яких дій, відносин; заклик до змагання, до участі в чому-небудь; категорична, різка пропозиція вступити в боротьбу, поєдинок» [19, с. 157]. Зважаючи на те, що процитоване визначення має загальний характер, без урахування специфіки безпекової діяльності, в його змісті насамперед наголошується на тлумаченні виклику як певних дій чи обставин, які спонукають до формування відповідної реакції, хоча не містять безпосередньої загрози для існування та розвитку системи. В Оксфордському словнику міститься термін «challenge», що, будучи відповідником виклику, трактується як «...завдання або ситуація, яка перевіряє чийсь здібності» [195]. Безперечно, така позиція також заслуговує на увагу, адже йдеться про спроможність суб'єктів безпеки діяти за раніше невідомих обставин і за відсутності необхідного досвіду, хоча не наголошується на реальності такої потреби. Дієздатність та гнучкість СЕБП є важливими параметрами, що забезпечують виконання поставлених завдань. Приклад відмінного розуміння виклику представлений у Великому економічному словнику, де його подано як «...постановку під сумнів питання, сумніватися» [18, с. 58]. Підґрунтям такого тлумачення є відсутність безпосереднього впливу виклику і конкретизації ймовірних наслідків, які можуть виявитися як позитивними, так і негативними. В цьому ж визначенні підкреслюється взаємозв'язок між викликом і ризиком

через високий рівень невизначеності внаслідок відсутності достовірної інформації щодо можливих результатів.

Серед наукових публікацій нашу увагу привернули кілька, які уточнюють зміст виклику й наближені до проблематики забезпечення безпеки. Так, О. Бодрук доводить необхідність розуміти під цим терміном «...проблему, що набула з певних причин та у певний відтинок часу сильного звучання і загострено сприймається політичною елітою, має, на її думку, важливе, пріоритетне значення» [10, с. 35]. Відкидаючи галузеву специфіку цього визначення, важливо те, що йдеться про проблему, яка потребує реакції через набуття актуальності в деяких часових межах. Тобто йдеться про проблему, яка характеризується динамікою, посиленням актуальності, але не безпосереднім впливом у цей момент.

У межах функціонування Львівської безпекової школи цікавими є два визначення досліджуваного поняття, які доповнюють одне одного. М. Копитко визначає виклики як «...певну сукупність обставин, вплив яких не обов'язково може бути негативний, на які необхідно задіяти певні ресурси, у разі бездіяльності ці обставини можуть призвести до позитивних чи негативних наслідків» [75, с. 48]. На нашу думку, авторка влучно наголошує на необхідності своєчасної реакції на виникнення виклику, підкреслюючи, що така реакція буде потребуватиме певного ресурсного забезпечення. С. Мельник дещо зміщує акценти, першочергово наголошуючи у розумінні виклику на тому, що це «...явище, яке може бути як негативного, так і позитивного спрямування, що вимагає від підприємства відповідної реакції та застосування тих чи інших заходів із метою недопущення негативних наслідків» [95, с. 173]. Наголос на неоднозначність подальших змін, які проявляються у вигляді виклику, вимагає від суб'єктів безпеки розгляду усіх можливих варіантів. Попри те, вважаємо, що реакція суб'єктів безпеки не може обмежуватися лише реакцією у випадку ймовірності реалізації негативних наслідків. Не менш важливим є виявлення й додаткових можливостей, які дозволять підприємству покращити своє конкурентне становище.

Шляхом узагальнення процитованих вище та інших визначень суті терміна «виклик» нами визначено його основні параметри і представлено в графічному вигляді на рис. 1.9.

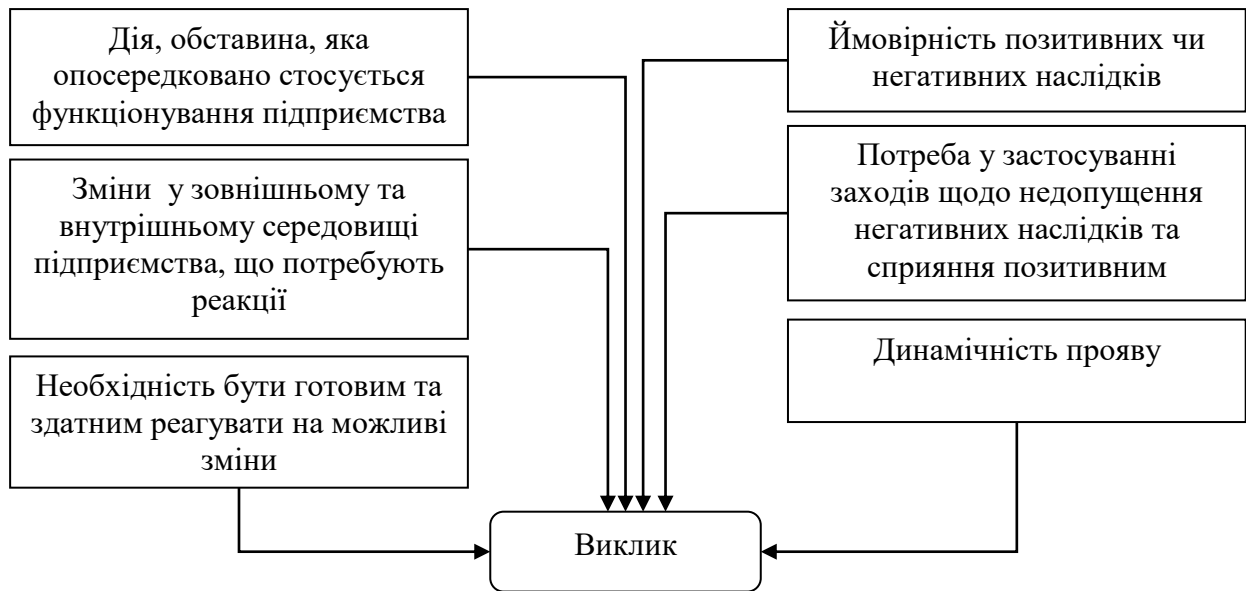


Рис. 1.9. Параметри виклику з позиції забезпечення ЕБП, сформовано автором

Серед виділених параметрів на особливу увагу заслуговує «динамічність прояву». Зазначене ґрунтується на тому, що відсутність реакції на виклик може призвести до негативних наслідків, якими будуть нові ризики та загрози. Невикористання додаткових можливостей також можна вважати втратами. Зазначене можна доволі чітко проілюструвати в контексті розглянутих у попередньому підрозділі тенденцій щодо активнішого застосування цифрових технологій. Сьогодні викликом можна вважати «необізнаність представників бізнесу із певною технологією», яка розроблена та починає застосовуватися в бізнесі. Із поширенням цієї технології та набуттям масовості у використанні, що спричиняє втрату конкурентних позицій певного підприємства, уже можна говорити про загрозу. Одне із завдань суб'єктів безпеки полягає у відстеженні появи та зміни викликів з метою недопущення їх трансформації у ризики й загрози. Стосовно змодельованої ситуації суб'єкти безпеки повинні бути орієнтовані на виявлення технологічних новацій із розглядом можливих варіантів їх впливу на конкурентне середовище у короткостроковій,

середньостроковій та довгостроковій перспективі, зважаючи на те, що «піонери» зазнають найбільших витрат, коли споживач ще не готовий до активного застосування, але «аутсайдери» можуть припинити діяльність через зростаючий інтерес клієнтів до тих речей, які стають повсякденними сьогодні, хоча ще у вчора були складовими наукової фантастики. З іншого боку, це й же приклад доводить, що перелік актуальних викликів постійно змінюється, а відтак вимагає застосування відповідної системи моніторингу. Ще одна обставина полягає в тому, що виклики виступають стимулюючими факторами для розвитку СЕБП та підприємства загалом, адже реакція потребує внесення відповідних змін.

Узагальнюючи, можна стверджувати, що виклик становить явища, процеси, обставини та інші зміни у зовнішньому та внутрішньому середовищі, які безпосередньо не впливають на функціонування підприємства, але потребують відповідної реакції задля уникнення можливої трансформації у нові ризики й загрози або більш повного використання додаткових можливостей. Відповідна реакція повинна спиратися на наявний безпековий потенціал та бути орієнтованою на удосконалення СЕБП. Таке визначення враховує усі ідентифіковані вище параметри виклику, а також формує необхідне концептуальне підґрунтя для розвитку СЕБП.

Розгляд терміна «ризик» у безпекознавстві є певним чином ускладнений через дещо інше розуміння його сутності порівняно із тим, що сформовано в ризикології. Основна відмінність полягає в тому, що в безпекознавстві ризик є складовою категоріального апарату безпеки, а відтак вимагає встановлення взаємозв'язку із викликом й загрозою та окресленням впливу на рівень безпеки певної системи й можливості зростання небезпеки через його ігнорування або ж хибне визначення рівня. В основі цих проблем лежить неоднозначність в історичних коренях його розуміння. Так, з грецької мови цей термін перекладається як «скеля» або ж «круча», а з італійської й французької – як «загроза», «небезпека», «обходити або ж обминати скелю, певну перешкоду». Лінгвістичне ототожнення проявляється в неоднозначності розуміння

зазначених термінів і в довідниковій літературі. Доволі яскравим прикладом може бути визначення, яке міститься у словнику Вебстера, де ризик подається як «...небезпека, загроза, випадковість, можливість піддатися руйнуванню, втратам чи пошкодженням» [209, с. 332]. Зважаючи на це, в подальшому наша увага буде спрямована на виявлення сутнісних параметрів ризику, які безпосередньо пов'язані із безпековою діяльністю.

О. Зурян, досліджуючи сутність ризику, визначає джерела його виникнення, серед яких, окрім тих, що пов'язані із сприйняттям ситуації людиною, що приймає рішення, та обставин, які виникають поза сферою її діяльності, виділено й «характер науково-технічного прогресу» [55, с. 142], що певним чином пов'язано із ЦТП. Ризик виникає у питаннях цифровізації загалом, чи інтенсивності впровадження окремих цифрових технологій, а результат його реалізації безпосередньо впливає на ЕБП. Відтак ризик, як і попередньо розглянутий «виклик», пов'язані із процесами цифрової трансформації на мікро- й макрорівні і не можуть залишатися поза увагою суб'єктів безпеки.

Залишаючи поза увагою загальні засади визначення ризику в ризикології, приділимо увагу уточненню його змісту в межах категоріального апарату безпеки. Так, окрема група науковців встановлює зв'язок між ризиком та небезпекою. Для прикладу, окремі науковці визначають ризики як «можливу небезпеку або дію, що може мати негативні наслідки» [95, с. 71]. З позицій розгляду методичного підґрунтя розвитку СЕБП складно погодитися з такими міркуваннями, спираючись на фактичне порівняння небезпеки та будь-якої дії, коли перша складова характеризує результати реалізації необмеженої кількості другої складової. Результатом реалізації ризику можуть бути негативні наслідки, але із однаковою ймовірністю вони набувають й позитивного характеру, або ж створюється ситуація без будь-яких змін. Суб'єкти безпеки повинні розглядати різні варіанти та, відповідно, формувати сценарії розвитку подій, намагаючись не допустити негативних наслідків та забезпечити отримання позитивного результату. Серед інших визначень, де йдеться про

виявлення зв'язку між ризиком і небезпекою, доцільно відзначити позицію В. Пироженка, який доводить, що ризик «...інтерпретується як міра небезпеки, що є похідною від ступеня ймовірності небажаної події та розміру можливих втрат при її настанні» [100, с. 22]. Хоча в цьому визначенні акцентовано увагу лише на можливих негативних наслідках, але уточнено причинно-наслідковий зв'язок, коли ризики може спричинити зростання небезпеки. Відповідно, завдання суб'єктів безпеки полягає як у недопущенні зниження рівня безпеки, так і формуванні умов для позитивного результату, зокрема за рахунок створення відповідного інформаційного супроводу при прийнятті кожного управлінського рішення.

В окремих публікаціях безпекознавців також розглядається зв'язок між ризиком і загрозою. Так, О. Ляшенко обґрунтовує суть ризику як «...усвідомлену частину загрози і як свідому дію, що може мати негативні наслідки та стати загрозою» [91, с. 49]. Тракткування ризику як частини загрози певним чином суперчить базовим засадам ризикології, спираючись хоча б на неоднозначність результатів. Разом з цим міркування щодо ризику як можливої причини виникнення загрози імпонує. Така позиція підтримана у публікації Н. Н. Пойда-Носик, де авторка, розглядаючи фінансові ризики, доводить, що «...ризики виступають джерелами загроз для фінансової безпеки, оскільки саме ризики генерують потенційну можливість завдання шкоди суб'єкту господарювання» [116, с. 289]. Зроблені вище узагальнення щодо ризику як можливого джерела небезпеки можна доповнити міркуваннями, що негативні результати реалізації ризику провокують виникнення загрози, яка спричиняє зростання небезпеки. Відповідно, завдання суб'єктів безпеки полягають в інформаційному супроводі прийняття управлінських рішень для зменшення ймовірності виникнення негативних наслідків, а за настання такого випадку – ліквідації відповідної загрози задля недопущення зниження рівня ЕБП.

Потребує уваги також позиція Є. Рудніченка, який розглядає ризик як «...об'єктивно-суб'єктивну категорію, що пов'язана з певною мірою невизначеністю результату внаслідок прийнятого рішення, дії або обставин»

[130, с. 192]. Відмінність цього підходу полягає в акцентуванні уваги на невизначеності результатів. На нашу думку, невизначеність доцільно розглядати не лише як результат, але й причину, яка пов'язана із неповною, неточною, несвоєчасною, зайвою й навмисно видозміненою чи створеною інформацією, яка ускладнює процес прийняття управлінського рішення. В цьому випадку завдання служби безпеки полягає у створенні інформаційно-аналітичної системи, яка, будучи складовою інформаційної системи управління підприємством, забезпечить необхідний інформаційний супровід розроблення й реалізації управлінських рішень.

Вище нами неодноразово підкреслювалася неоднозначність у можливих результатах реалізації ризику. Доволі чітко цей момент охарактеризовано І. Балановим: «...подія, яка може відбутися або не відбутися. У разі здійснення такої події можливі три економічні результати: негативний (програш, збиток, шкода), нульовий, позитивний (виграш, вигода, прибуток)» [4, с. 22]. Потрібно визнати, що в безпекознавстві ризик розглядається виключно в контексті можливих негативних наслідків, що звужує поле завдань суб'єктів безпеки через реагування лише на події та обставини, що знижують рівень безпеки, залишаючи поза увагою ті, які можуть сприяти зростанню.

Оскільки визначені параметри були доволі ретельно попередньо розглянуті (рис. 1.10), то, узагальнюючи, вважаємо за доцільне запропонувати власне трактування ризику як результату суб'єктивно-об'єктивних процесів, що може спровокувати виникнення загрози або додаткових можливостей, чим вплинути на рівень безпеки системи. В основі нашої позиції лежить переконання, що об'єктом моніторингу для суб'єктів безпеки повинні бути як можливі загрози, так і додаткові вигоди, що можуть виникнути в результаті реалізації певного ризику.

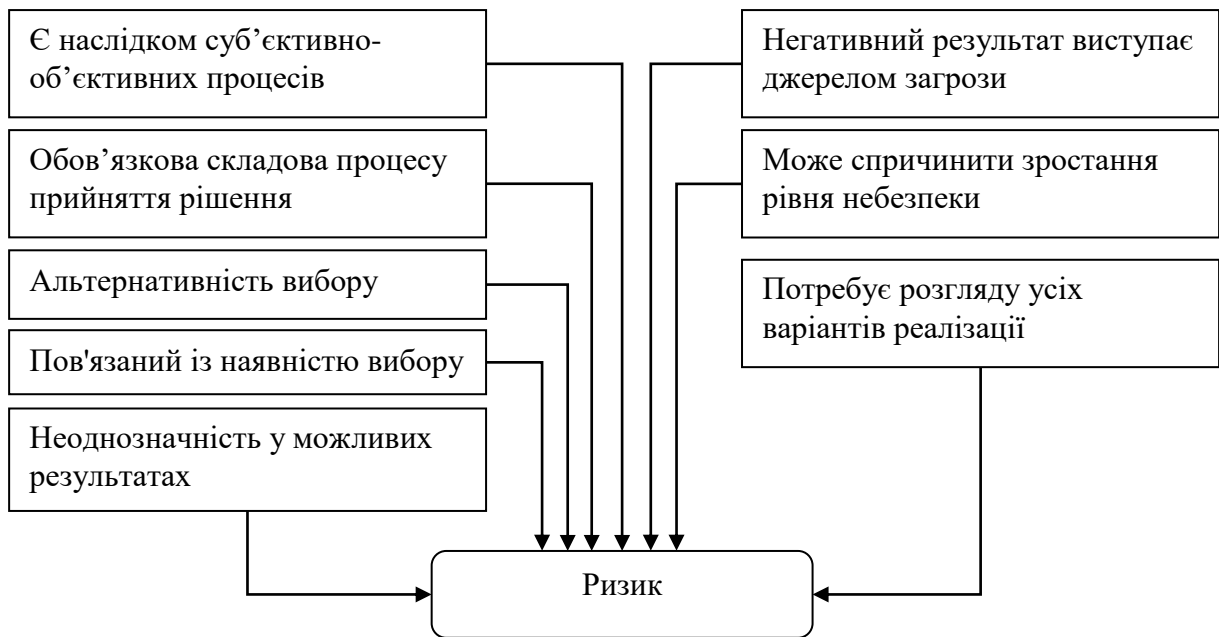


Рис. 1.10. Параметри ризику з позицій забезпечення ЕБП, сформовано автором

Контроль за підготовкою й реалізацією управлінських рішень повинен уможливити не лише ліквідацію загроз, але й досягнення позитивного результату, який сприятиме стабілізації ситуації та покращенню рівня ЕБП. У цьому контексті доволі цікавими є розробки О. Матвійченко [94, с. 93], який згрупував основні ризики, що виникають в умовах входження і невходження до концепції Індустрія 4.0. Отримані результати переконливо доводять багатоаспектність ЦТП, що передбачає виникнення не одного ризику щодо реалізації програми цифровізації, а поєднання сукупності, які стосуються абсолютно усіх аспектів змін у внутрішньому й зовнішньому середовищі. Попри те, важливою є та обставина, що в умовах кожного окремого підприємства перелік таких загроз буде відмінний і динамічно змінний. Водночас ключовим є те, що ЦТ провокує виникнення нових ризиків, які повинні бути об'єктом моніторингу суб'єктів безпеки.

Поруч із розглянутими вище викликом та ризиком, останньою складовою так званих «деструктивних» факторів є загроза. Як основу для розгляду сутності загрози можна взяти її загальнонаукове розуміння, яке доволі чітко сформульовано в Академічному тлумачному словнику як «...можливість або

неминучість виникнення чогось небезпечного, прикрого, важкого для когось, чогось... те, що може заподіювати будь-яке зло, якусь неприємність» [1]. Тобто йдеться про перебіг подій, ситуацію, поєднання впливу кількох факторів, які порушують попередньо стійкий стан та спричиняють зміни, які ускладнюють подальше існування певної системи. Можна стверджувати, що такі аспекти лежать в основі більшості підходів безпекознавців, хоча із відмінностями, які потребують уваги в контексті формування методичного підґрунтя розвитку СЕБП.

Доволі яскравою ілюстрацією неоднозначності у розумінні загрози може бути позиція В. Ліпкана, згідно з якою під цим терміном він пропонує розуміти «...ризик, який почав реалізовуватися за небажаним варіантом, або заздалегідь відомий сценарій несприятливого розвитку подій, що відповідно виходить за рамки поняття нормальної невизначеності умов господарської діяльності» [87, с. 48]. Як вище нами було обґрунтовано, негативний результат реалізації ризику є джерелом для виникнення загрози, але все-таки йдеться про два відмінні поняття. Зазначене ґрунтується ще й на тому, що виникнення загрози може бути не пов'язано із ризиком, на чому буде акцентовано увагу в подальшому.

Серед науковців також поширено ототожнення понять загрози та небезпеки. Так, О. Владіміров стверджує, що «...небезпеки – це загрози, що формуються...небезпеки відвертаються, нейтралізуються...натомість загрози – це небезпеки, що реалізуються...загрози відбиваються» [162, с. 111]. Наші міркування полягають у розумінні протилежностей і зв'язку між безпекою й небезпекою, які взаємно характеризують стан системи. Відтак реалізація загрози спричиняє зростання небезпеки і зниження безпеки. Своєю чергою, загрозу можна ліквідувати або адаптуватися до її впливу. Певний рівень небезпеки завжди наявний, оскільки «абсолютна» безпека можлива лише стосовно ізольованих і незмінних систем.

Іншим важливим параметром суті загрози, який можна вважати дискусійними, є ступінь впливу, тобто можливі результати реалізації. Так, позиція О. Сорочан та Д. Ігнатюк є доволі загальною, оскільки передбачає

окреслення наслідків реалізації загрози як «...дестабілізуючого впливу на функціонування і розвиток економічної системи» [137, с. 19]. Безперечно, кожна загроза відрізняється як за джерелом виникнення, так і за ступенем впливу на певну складову ЕБП. Попри це, на нашу думку, відсутність конкретизації не формує необхідні орієнтири, щоб задати параметри у постановці й реалізації завдань суб'єктами безпеки. В цьому контексті більш чітко обґрунтовують свою позицію інші науковці. М. Камлик розуміє під загрозою такий перебіг подій та «...потенційні або реальні умови, чинники чи дії фізичних та юридичних осіб, що порушують нормальний фінансово-економічний стан суб'єктів підприємницької діяльності і здатні заподіяти великої шкоди аж до припинення його діяльності» [65, с. 41]. Попри схожість такого трактування із попереднім через розгляд загрози як дестабілізуючого фактору, відмінністю є окреслення можливих наслідків у вигляді припинення діяльності, тобто повного руйнування системи. Доцільно уточнити, що більше йдеться не про вплив однієї загрози, а про поетапне накопичення результатів кількох. Окрім цього, потрібно пам'ятати, що вплив загрози проявляється не лише у втраті вигоди й збитках, а й у формуванні інших загроз, стосовно цієї або інших складових ЕБП.

Багатоаспектним можна вважати визначення, що запропонував В. Франчук, де загроза розглядається як «...дія дестабілізуючих природних і (або) суб'єктивних чинників, пов'язаних із недобросовісною конкуренцією, порушенням законів та норм, цілісності процесів чи об'єктів, що можуть спричинити потенційні або реальні збитки» [156, с. 65]. В цьому визначенні, окрім розгляду можливих наслідків, одночасно вказується на джерела виникнення загроз, що особливо важливо в процесі розроблення внутрішніх інструкцій стосовно моніторингу зовнішнього й внутрішнього середовища функціонування певного підприємства. Також вважаємо за доцільне доповнити можливі джерела виникнення загроз ще й внутрішніми, які доволі часто пов'язані із низькою кваліфікацією менеджменту, незадовільним рівнем

трудової дисципліни й мотивації працівників, протиріччями в інтересах працівників, управлінців різних рівнів та власників (акціонерів) тощо.

Шляхом ретельного вивчення наукового доробку безпекознавців стосовно суті загрози нами визначено її ключові параметри та представлено в графічному вигляді на рис. 1.11.

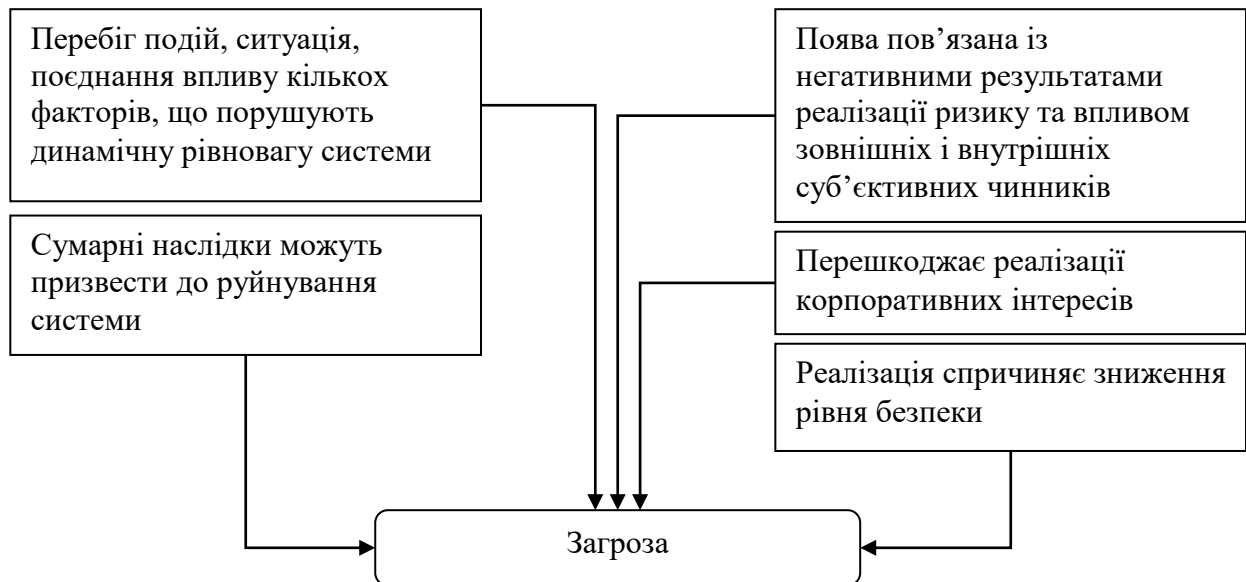


Рис. 1.11. Параметри загрози з позиції забезпечення ЕБП, сформовано автором

Узагальнюючи, можна стверджувати, що загроза становить ключову ланку в ланцюжку виклик-ризик-загроза-небезпека, зосередження уваги на якій дозволяє зберігати контроль над процесом забезпечення ЕБП. Відповідно до визначених параметрів у нашому розумінні, загроза, поява якої пов'язана із негативним результатом реалізації ризику та впливом внутрішніх і зовнішніх суб'єктивних чинників, провокує виникнення та збільшення втрат, що спричиняє зростання небезпеки аж до руйнування системи. Відповідно до цих міркувань, завдання суб'єктів безпеки полягає в ліквідації загроз або ж формуванні умов для адаптації до їх впливу. В контексті вищерозглянутих аспектів появи викликів і ризиків, які пов'язані із ЦТ, зосередження уваги на процесі виникнення й впливу загроз дозволяє на «останніх лініях оборони» підтримувати стійкість системи. Тобто реакція на виклики й ризики дає змогу застосувати превентивні заходи (на випередження), коли стосовно загроз –

виключно реактивні із очікуванням мінімізації втрат та зменшення витрат на відновлення рівноважного стану в нових умовах. Прикладом може бути ситуація, за якої підприємство втрачає конкурентні позиції на ринку, в подальшому застосовуючи інструменти традиційного маркетингу, коли його конкуренти здійснюють цифровізацію, зокрема щодо реалізації цифрового маркетингу. Зменшення обсягів реалізованої продукції, перехід основних клієнтів до конкурентів, збитки за результатами фінансового періоду тощо є результатами реалізації загрози, яка пов'язана із пасивністю, тобто нездатністю адаптуватися до тенденції ЦТЕ.

Ретельно розглянута сутність ВРЗ із уточненням їх основних параметрів стосовно забезпечення ЕБП та у взаємозв'язку із загальним характером ЦТЕ доводить кілька важливих фактів: ЦТ на макро- та мікрорівні спричиняє зміни, які провокують виникнення нових викликів, ризиків та загроз; ігнорування або ж реалізація ЦТ впливає на рівень безпеки, а відтак повинна здійснюватися під пильним контролем суб'єктів безпеки; динамічність змін вимагає розвитку СЕБП задля збереження та підтримання темпів ЦТП. Ці факти є основою для подальшого уточнення засад ЦТП, сутність яких було коротко з'ясовано у попередньому підрозділі.

Відповідно до розглянутих вище методичних аспектів виникнення й впливу деструктивних факторів, ці галузеві відмінності впливають на активізацію змін у СЕБП, зокрема розвитку її окремих складових, із відповідним паралельним упровадженням цифрових технологій та удосконаленням методів управління. Зазначений аспект є особливо важливим, з огляду на хибне уявлення про те, що ЦТ передбачає виключно інвестування у нові технології. В публікації Н. Іванченко, Ж. Кудрицької та К. Рекачинської на основі аналітичних даних доводиться, що «...прибуток фірми зростає в середньому на 26%, якщо використовувати технології і нові методи управління, але у випадку інвестування лише у менеджмент – 9%, а якщо лише в технології – прибуток падає на 11%» [60, с. 186]. Для прикладу, дедалі ширша автоматизація процесів взаємодії із споживачами дозволяє оперувати значними

обсягами інформації, що сприяє переходу від орієнтації на задоволення масових потреб до виявлення індивідуального інтересу та формування особистої пропозиції. Дані про клієнтів, активність конкурентів, прогнози можливої зміни ринку тощо формують інформаційне підґрунтя, яке, будучи використано суб'єктами безпеки, уможливорює виявлення змін у складі та темпах впливу основних деструктивних факторів. Безперечно, такі аргументи заслуговують на увагу та доводять необхідність у процесі розвитку СЕБП ширше застосовувати нові цифрові технології, підвищувати кваліфікаційний рівень співробітників служби безпеки та удосконалювати методичну базу управління відповідно до галузевої специфіки ЦТП.

Наступним, не менш важливим, параметром є швидкість технологічних змін. Якщо раніше періодичність широкого впровадження нових технологій становила 7–10 років, то сьогодні йдеться про суттєве пришвидшення і стрибкоподібність, що ускладнює процес забезпечення ЕБП через потребу не лише слідування за темпами розвитку, але й врахування значно більшої кількості деструктивних факторів. У межах кожного окремого українського підприємства відмінними є темпи ЦТ, але в більшості цей процес характеризується етапністю. На першому етапі, внаслідок усвідомлення менеджментом необхідності ЦТ, виникає інвестування в цифрові інструменти, що провокує нові ризики й загрози через зміни в діяльності певного підрозділу чи коригування окремих бізнес-процесів. Із набуттям досвіду відбувається перехід до наступного етапу, коли інвестування відбувається в межах окремого проекту, що провокує збільшення кількості й характеру деструктивних факторів й посилення спротиву з боку персоналу, кваліфікаційний рівень яких є недостатнім для ефективного використання цифрових технологій. Ці обставини спричиняють зміну в кадровій політиці, зокрема в підборі персоналу й оптимізації штату окремих підрозділів через вищий рівень автоматизації й роботизації. Третій етап характеризується розробленням стратегії ЦТ, яка пов'язана із упровадженням нової моделі бізнесу, змін ринків збуту та рівня взаємодії із контрагентами. Швидкість проходження кожного етапу є

відмінною і пов'язана зф специфікою сфери господарської діяльності, рівнем конкуренції та розвитку цифрової інфраструктури, але загалом увесь процес вимагає високої динамічності у розвитку СЕБП для своєчасного уникнення реалізації деструктивних факторів та уможливлення переходу до наступного етапу.

Цифровізація підприємства вносить корективи у пріоритетність забезпечення ЕБП за структурними складовими. Так, широке застосування «розумного» обладнання, зростання інформаційних потоків та формування центрів обробки інформації в межах кожного підрозділу поступово знижує потребу у приділенні уваги фізичному захисту, але вимагає посилення інформаційної й кадрової безпеки. В межах кіберфізичних систем основним джерелом загроз виступає саме людина. Автоматизація дозволяє знизити вплив людського фактору у великих масштабах, але конфлікти інтересів сприяють отриманню доступу до інформаційних ресурсів через зраду одного із відповідальних виконавців. Цей аспект є доволі складним, адже намагання інвестувати у дедалі досконаліші системи захисту від хакерських атак можуть бути нівельовані передачею ключів доступу або ж непрофесійним виконанням обов'язків одним із виконавців, що ще раз підкреслює важливість розвитку СЕБП і неможливість заміни роботи фахівців служби безпеки певною кількістю високопродуктивних машин.

Г. Ткачук [143, с. 28] висуває ідею концепції безпечності трансформаційних перетворень, в основі якої лежить здатність СЕБП розпізнати нові деструктивні фактори. На нашу думку, зважаючи на вищерозглянуті параметри ЦТП, без розвитку СЕБП, який повинен також включати і цифровізацію такої системи, виявлення новітніх ВРЗ є фактично неможливим. Окрім того, для уникнення негативного впливу деструктивних факторів, які будуть виникати в процесі цифровізації підприємства, розвиток СЕБП повинен випереджати швидкість змін загалом у масштабах підприємства. Ці аргументи створюють логічний перехід до виконання наступного завдання в

межах цього підрозділу, яке полягає в ретельному розгляді концептуального підґрунтя розвитку СЕБП.

В підрозділі 1.1 нами шляхом вивчення різних підходів до процесу розвитку підприємства (процес, рух, зміна системи) і ключових функцій служби безпеки, сформульовано власне тлумачення терміна «розвиток СЕБП», де наголошується на необхідності здійснення кількісних й якісних змін. Спираючись на зміст цього загального спрямування, конкретизуємо ключові аспекти цього процесу. Відповідно до зазначеного, найперше уточнимо питання зміни щодо парадигми розвитку підприємства. О. Тур висловлює міркування, що «...кожне підприємство має два стимули – бажання вижити і самовдосконалюватися (розвиватися)» [145, с. 39]. В. Занора розглядає етапність переходу в межах таких поєднань як «...функціонування – розвиток ...розвиток – функціонування ...розвиток – розвиток» [53, с. 71]. Загалом погоджуємося із тим, що в сучасних умовах ЦТЕ лише шляхом концентрації уваги на процесі розвитку можна втримувати конкурентні позиції бізнесу. Водночас зазначені автори не беруть до уваги безпекові аспекти, тобто здійсненню кількісно-якісних змін у межах усього підприємства повинен передувати розвиток СЕБП, адже в іншому випадку знижується ймовірність досягнення поставлених цілей через виникнення й негативний вплив деструктивних факторів, які пов'язані із ЦТЕ та тією цифровізацією, що буде проводитися в межах самого суб'єкта господарювання. Відповідно нова парадигма, яка враховує безпекові аспекти та ЦТЕ, може бути представлена так (рис. 1.12).

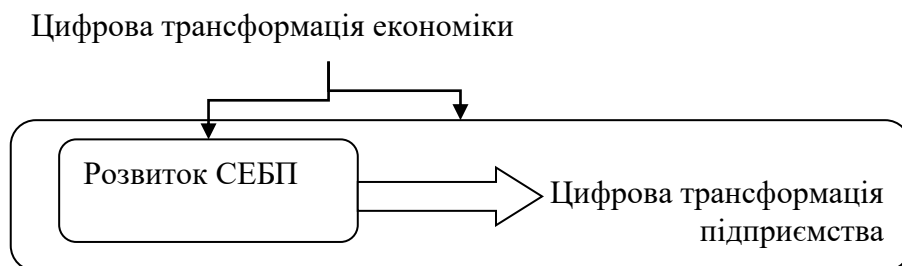


Рис. 1.12. Зміна парадигми розвитку підприємства та його СЕБП, *сформовано автором*

Графічно нами демонструється, що ЦТЕ задає параметри для відповідних процесів у масштабах підприємства, але першочергові зміни повинні відбутися в СЕБП для формування безпечних умов розвитку суб'єкта господарювання загалом. Цей момент покладено нами в основу концептуального підґрунтя розвитку СЕБП.

У наукових публікаціях доволі ретельно розглядається питання класифікації розвитку підприємства, водночас ці ж параметри стосовно розвитку СЕБП залишаються поза увагою. Відповідно, нами пропонується класифікація, яка враховує специфіку безпекової діяльності та є оптимізованою для більш чіткого розуміння суті цього процесу (рис. 1.13).

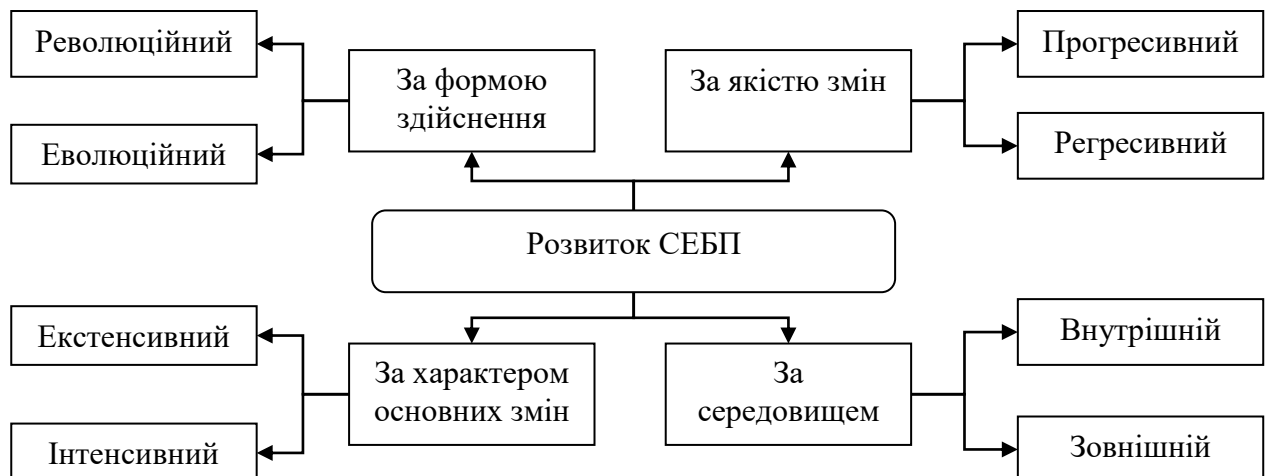


Рис. 1.13. Класифікація видів розвитку СЕБП, *сформовано автором*

За першою класифікаційною ознакою пропонується розрізнити революційний та еволюційний розвиток. Революційний розвиток СЕБП полягає в стрибкоподібних, радикальних змінах із переглядом базових засад функціонування служби безпеки, формуванням нових зв'язків з іншими структурними підрозділами підприємства, коригуванням ресурсного й організаційного забезпечення тощо. Еволюційний розвиток передбачає поступову й поетапну адаптацію якісних і кількісних параметрів СЕБП до зміни зовнішнього середовища й внутрішньогосподарських процесів.

Прогресивний розвиток СЕБП передбачає перехід від менш досконалої форми до більш досконалої, із покращенням якісних і кількісних параметрів, що дозволяє ефективно виконувати поставлені завдання. Регресивний розвиток пов'язаний із деградацією, зниженням якості виконуваних завдань та скороченням кадрового складу служби безпеки, попри це в умовах вимушеного згортання господарської діяльності, що відбулося через COVID-19 та військові дії, такий крок є виправданий.

Екстенсивний розвиток вимагає першочергового збільшення обсягів ресурсного забезпечення, зокрема й кадрового, що полягає у розширенні штатного розпису, створення окремих груп за основними сферами діяльності СЕБП (конкурентна розвідка, контррозвідка, фінансова, силова, кадрова, інформаційна, техніко-технологічна та інші складові ЕБП). Інтенсивний розвиток передбачає орієнтацію на досягнення завдань не за рахунок збільшення виконавців, а у результаті підвищення їх кваліфікаційного рівня, технічного озброєння, кращого використання резервів та пошуку нових можливостей.

Окремо нами виділено ще внутрішній й зовнішній розвиток. Перший із названих видів орієнтований на кількісні й якісні зміни служби безпеки, а другий – на покращення взаємодії із зовнішніми суб'єктами безпеки і насамперед із правоохоронними органами. Безперечно, оптимальним є варіант поєднання цих видів, що повинно суттєво посилити оборонні редути підприємства та забезпечити необхідну стійкість в умовах обмеженості внутрішніх ресурсів та зростаючої агресивності в діях суб'єктів зовнішнього середовища.

Сформована класифікація дозволяє розробити альтернативні варіанти програми розвитку СЕБП відповідно до змін зовнішнього середовища функціонування та інтенсивності внутрішніх процесів.

Проблематиці розвитку СЕБП сьогодні приділяється критично мало уваги. Певним позитивним винятком є напрацювання О. Вовк, яка, розглядаючи стратегічні аспекти управління ЕБП, доводить, що розвиток СЕБП становить

«...процес реагування на нові загрози та нарощування рівня захисту за підвищення ефективності застосування необхідних ресурсів» [22, с. 126]. Порівняння власного визначення із процитованим дозволяє ще раз акцентувати увагу на відмінностях, які конкретизують концептуальні засади розвитку СЕБП:

– авторське розуміння не обмежується розглядом лише загроз, а стосується усіх деструктивних факторів, тобто ще й викликів і ризиків. Зазначене є важливим моментом, оскільки, як було обґрунтовано вище, саме виклики й ризики дозволяють застосувати превентивні заходи захисту, коли реакція на загрози можлива за фактом виявлення втрат;

– розвиток СЕБП має пріоритет перед розвитком підприємства, оскільки без формування безпечних передумов не можна досягнути корпоративних цілей;

– нами акцентовано увагу, що розвиток СЕБП передбачає здійснення кількісно-якісних змін, які лежать у площині досягнення стратегічних цілей розвитку підприємства;

– в межах цього підрозділу нами доводилося, що основою розвитку СЕБП є зовнішні зміни, які в сучасних умовах найбільше пов'язані із ЦТЕ, та внутрішні процеси, що відбуваються переважно під впливом цифровізації.

Викладені уточнення також сприяють більш чіткому формулюванню концептуального підґрунтя розвитку СЕБП, які подано на рис. 1.14.

У графічному вигляді нами узагальнено авторське розуміння взаємозв'язку між ЦТЕ й підприємства та розвитком СЕБП. Додаткового розгляду потребує лише такий важливий параметр як оцінювання й ефективне застосування безпекового потенціалу. В основі наших міркувань були покладені результати узагальнення наукового доробку щодо потенціалу, його значення для розвитку підприємства та суті безпекового потенціалу. Так, В. Занора, Д. Куценко та Н. Одородько обґрунтовують важливість ролі потенціалу, Зважаючи на те, що його рівень «...є підґрунтям розвитку підприємства, обов'язковим елементом планування його діяльності» [53, с. 45]. Оскільки загалом науковці є

одностайними щодо значення потенціалу для розвитку підприємства, то зосередимо увагу на безпековому потенціалі. Потрібно визнати, що проблематика формування й ефективного застосування безпекового потенціалу в більшості не розглядається, тобто ця складова не виділяється в межах економічного потенціалу підприємства, що переважно пов'язано із невирішеністю загалом проблеми ресурсного забезпечення безпекової діяльності в умовах українських підприємств. Необхідність посилення захисту спонукає до створення СЕБП, але обмежене розуміння його ролі у функціонуванні й розвитку ускладнює розроблення механізмів управління, а відтак належного ресурсного забезпечення.

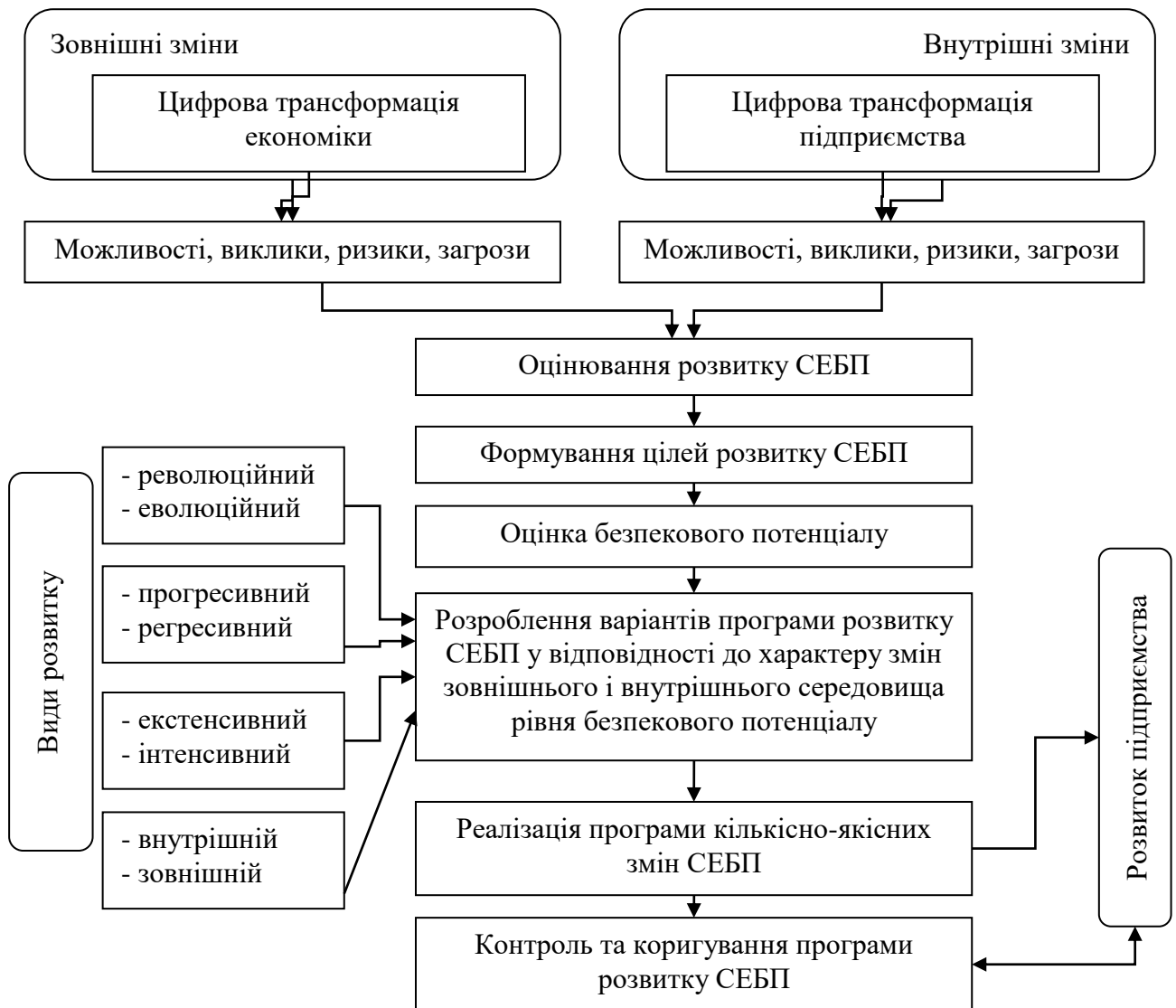


Рис. 1.14. Концептуальне підґрунтя розвитку СЕБП, сформовано автором

У межах наукової активності Львівської безпекової школи зроблено кілька важливих кроків щодо ліквідації вакууму на цій ділянці безпекознавства. В. Франчуком задані орієнтири щодо уточнення безпекової діяльності, а В. Фостяком визначено безпековий потенціал як «...сукупну здатність використати наявні ресурси і можливості для формування безпечних умов розвитку через зниження ризиків та протидію внутрішнім та зовнішнім загрозам» [153, с. 116]. Вважаємо, що безпековий потенціал має застосовуватися більш активно стосовно усіх деструктивних факторів, а його формування повинно здійснюватися через поєднання цифровізації та покращення кваліфікаційного рівня співробітників служби безпеки.

Підводячи підсумки, доцільно ще раз наголосити на окремих ключових аспектах, які доповнюють концептуальне підґрунтя розвитку СЕБП:

- доволі складний процес, оскільки реалізація відбувається, зважаючи на динамічність ЦТЕ і з випереджаючими темпами щодо цифровізації підприємства загалом задля формування безпечних умов його подальшого функціонування й розвитку;

- розвиток СЕБП вимагає покращення спроможності співробітників служби безпеки визначати, протидіяти та адаптуватися до нових дестабілізуючих факторів, зокрема і через цифровізацію безпекової діяльності;

- полягає в підконтрольному здійсненні кількісно-якісних змін, що можливе завдяки завчасному формуванню й розвитку безпекового потенціалу;

- узгоджується із стратегією розвитку підприємства, характеризуючись відмінними параметрами реалізації відповідно до специфіки господарської діяльності й динамічності середовища функціонування;

- за різної інтенсивності реалізації не обмежений часовими рамками внаслідок необхідності систематичного створення безпечних умов розвитку підприємства в умовах високої ймовірності виникнення й негативного впливу внутрішніх і зовнішніх деструктивних факторів.

Концептуальне підґрунтя сформоване на основі попереднього ретельного розгляду теоретичних засад створення СЕБП та характеру змін, які пов'язані із ЦТ, яка виникає на рівні економіки та в умовах кожного окремого підприємства. Своєю чергою, отримані результати будуть використані для удосконалення теоретико-методичних засад і розроблення практичних рекомендацій розвитку СЕБП.

ВИСНОВОК ДО РОЗДІЛУ 1

1. Простежено зміни у розумінні безпеки та ЕБ під час посилення інтенсивності економічної, політичної та соціальної взаємодії від часів Стародавньої Греції і до сьогодні, що послуговуючись підґрунтям для розгляду, окреслення змісту та критичного порівняння відмінних підходів у тлумаченні ЕБП. Виділено шість базових підходів («ресурсно-функціональний», «захисний», «дієвий», «гармонізаційний», «стійкість і стабільність функціонування», «комбінаційний»), які сформовані в розвідках українських науковців. Отримані результати становлять основу конкретизації мети й ключових цілей ЕБП.

2. На основі встановлення параметрів системи, які відповідають засадам безпекової діяльності, розглянуто відомі сьогодні три підходи до формування СЕБП, що дало змогу запропонувати власний підхід, згідно з яким така система становить поєднання суб'єктів та об'єктів безпеки, в межах безпекозабезпечувальних процесів, шляхом реалізації механізму забезпечення та дотримання політики безпеки, задля досягнення мети й визначених цілей в сфері ЕБ відповідно до специфіки й умов функціонування підприємства. Обумовлено умови формування СЕБП, які відповідають реаліям функціонування українських підприємств. За результатами критичного аналізу наукового доробку безпекознавців визначено функції, принципи, перелік ключових завдань та обґрунтовано етапність побудови СЕБП, у межах якої виокремлено такий етап як «розвиток СЕБП».

3. Досліджено, шляхом виділення трьох базових підходів («процесний», «системний» та «кардинальний») та встановлення наслідків реалізації, безпекові аспекти трансформації системи, що було використано як основу для з'ясування характеру змін у СЕС, що виникли через здійснення ПР, третя і четверта з яких характеризуються цифровою трансформацією. Доведена життєва важливість для існування бізнесу слідування за ЦТ, яка сьогодні визначає параметри конкурентного середовища. З'ясовано характер ЦТ підприємств, що провокує виникнення нових викликів і ризиків, а також можливостей, які повинні обов'язково стати об'єктом безпекової діяльності на рівні окремого підприємства. Простежено видозміну в розумінні поняття «цифрова економіка» із подальшим установленням сутності основних факторів, що виникають при збільшенні частки цифрової економіки, які безпосередньо впливають на процес забезпечення ЕБП. Доведено, що ЦТП повинна здійснюватися синхронно із розвитком СЕБП задля створення можливості суб'єктам безпеки здійснювати результативні дії, стосовно ВРЗ, які виникають під час таких процесів. Проведено систематизацію передумов розвитку СЕБП, зокрема під тиском ЦТ.

4. Сформовано концептуальне підґрунтя розвитку СЕБП, в основу якого покладено авторське розуміння того, що в поточних умовах ЦТЕ задає параметри для відповідних процесів у масштабах підприємства, але першочергові зміни повинні відбутися в СЕБП для формування безпечних умов розвитку суб'єкта господарювання загалом. Концептуальне підґрунтя враховує відому видову відмінність розвитку та містить цілісне поєднання складових безпекової діяльності, зокрема в частині оцінювання розвитку СЕБП, розроблення варіантів програми розвитку та її реалізації, з огляду на безпековий потенціал і необхідність забезпечення безпечних умов для розвитку підприємства.

Основні наукові результати опубліковані в працях: [176; 178–179; 184; 186; 188]

РОЗДІЛ 2

КОМПЛЕКСНЕ АНАЛІТИЧНЕ ПІДґРУНТЯ РОЗВИТКУ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

2.1. Дослідження умов розвитку системи економічної безпеки підприємств видавничо-поліграфічної галузі

ЦТЕ не є одномоментним фактом, а тривалим постійно активним процесом, що характеризує інтенсивність створення, надання доступу, набуття необхідних цифрових навичок і використання цифрових технологій в усіх сферах людської діяльності. Поглиблення глобалізаційних процесів вимагає здійснення оцінювання не в межах певної національної економіки, а шляхом порівняння з іншими учасниками світового економічного простору. Зважаючи не лише на ініціативу й обсяги інвестицій бізнесу у створенні й застосуванні, інформаційних ресурсів, інформаційно-комунікаційного обладнання й цифрових технологій для покращення конкурентних позицій і задоволення попиту в цифрових продуктах, а на готовність відповідної інфраструктури, результати дій органів державної влади, наявність у населення й спроможність використовувати відповідні технічні засоби й програмне забезпечення, поступ загалом та порівняно із лідерами. Сьогодні відомі та використовуються більше 20 індексів, які в різних ракурсах характеризують ЦТ на рівні національних економік. Дослідження здійснюються за ініціативи міжнародних інституцій, зокрема таких як Всесвітній банк, ОЕСР, ЮНКТАД ООН, ЮНЕСКО та інших. Об'єктом оцінювання виступає максимально широке коло країн, щодо яких, аналізуючи думку експертів та фактичні статистичні дані, розраховується значна кількість первинних показників, що в подальшому об'єднуються у групи із рейтингуванням або ж визначенням інтегрального індексу, спираючись на вагу кожного показника та групи. Більшість індикаторів розраховується щорічно із систематичним уточненням критеріїв, які застосовуються для

оцінювання, зважаючи на загальну динамічність поширення й змісту цифрових технологій. Необхідним зауваженням повинно бути те, що Україна не завжди є об'єктом дослідження при визначенні таких індексів. Зокрема, у 2022 р. це пов'язано із неможливістю отримання достовірних даних через військові дії. Водночас Державна служба статистики, хоча і порівняно недавно, тобто з 2018 р., розпочала власні дослідження, які характеризують активність підприємств у використанні сучасних цифрових технологій. Такі початкові умови дозволяють у межах цього підрозділу зосередитися на узагальненні й ретельному розгляді результатів оцінювання ЦТЕ на основі індексів, що розраховуються міжнародними організаціями та Державною службою статистики України, а також конкретизації параметрів ЦТ видавничих структур та поліграфічних підприємств для визначення інформаційного підґрунтя розвитку в їх умовах СЕБП.

Українським інститутом майбутнього розроблений «Прогноз розвитку світової економіки до 2030Е» [125], де, на основі ретельного вивчення аналітичних матеріалів низки міжнародних інституцій, зокрема McKinsey та IDC, констатується факт частки цифрової економіки у ВВП станом на 2016 р. у США на рівні 11%, Китаю – 10%, Індії – 6% та України – 4%, із подальшим прогнозом до збільшення у 2030Е у США до 60%, Китаю – 50% та Індії 50%, але без відповідних окреслень стосовно України. Цікавими можна також вважати матеріали «Проекту Плану відновлення України» [126], які створені уже із врахуванням стану національної економіки під час військових дій. Учасники робочої групи «Відновлення та розвиток економіки» констатують, що частка цифрової економіки у ВВП становила у 2019 р. – 4,3%, 2020 р. – 5,3% і 2021 р. – 5,2%, та прогнозують її зростання у 2022 р. до 5,5%, 2023 р. – 6% та 2024 р. – до 7,7%. Можна вважати такі прогнози доволі оптимістичними, зважаючи, що дослідники вказують темп зміни обсягу ВВП у 2022 р. на рівні 69,7% і фактичне продовження військових дій на території України у 2023 р., що значно впливає на темпи ЦТЕ.

Всесвітній центр конкурентоспроможності (IMD) щорічно розраховує рейтинг за назвою «World Digital Competitiveness Ranking» (WDC) [212], який комплексно характеризує спроможність кожної країни створювати й впроваджувати цифрові технології. Рейтинг країн створюється на підставі розрахунку 50 показників на основі фактичних даних, а також результату опитувань. Початкові показники об'єднані у три ключові групи, тобто «знання» (до уваги беруться витрати на освіту та НДДКР, частка науковців у загальній кількості населення, якісний склад здобувачів освіти та викладацького складу, результати наукових розробок у вигляді патентів й публікацій тощо), «технології» (положення чинної нормативної бази щодо започаткування бізнесу, створення й розробки технологій, захисту інтелектуальної власності, інвестування в технологічний поступ тощо) та «готовність до майбутнього» (стан Інтернет-торгівлі, наявність та інтенсивність використання засобами обміну інформацією, активність бізнесу в питаннях створення й застосування цифрових технологій, забезпечення кібербезпеки, ефективність реалізації публічно-приватного партнерства тощо). Нами було узагальнено звіти IMD з 2016 до 2021 рр. та графічно подано дані стосовно України (рис. 2.1). У звіті за 2022 р. даних щодо України немає, що пояснюється складністю отримання достовірної інформації під час активної фази військових дій.

Графічне зображення дозволяє зробити кілька узагальнень для подальшої деталізації: загальний рейтинг України в межах 2017–2021 рр. характеризується незначним, але поступовим покращенням місця нашої країни серед інших 63, стосовно яких здійснювалися розрахунки; стабільністю відзначається група показників «готовність до майбутнього», коли значення інших двох, тобто «знання» й «технології», змінюється із протилежною динамікою; у 2021-му позитивно високе значення було визначено у групі «знання» стосовно таких показників як «загальні державні витрати на освіту» (11), «співвідношення учень/викладач» (11) та «жінки-дослідники» (17); стосовно групи «технології» Україна зайняла лідируючі позиції за показником «Інвестиції в телекомунікації» (2); в межах групи «готовність до майбутнього» найвищий

рівень фіксувався щодо показника «використання великих даних та аналітики» (19). Серед трьох груп показників найвищими є рейтингові позиції, що характеризують можливість і якість здобуття освіти населенням, зокрема у 2021-му було зайнято 37 позицію, тобто умовну середину в межах усієї сукупності. Суттєво гірші позиції фіксуються стосовно наявності й спроможності створювати цифрові технології (у 2021-му – 58 місце) та готовності їх широкого використання (відповідно, 58 місце), що є свідченням глибокого відставання від країн-лідерів.

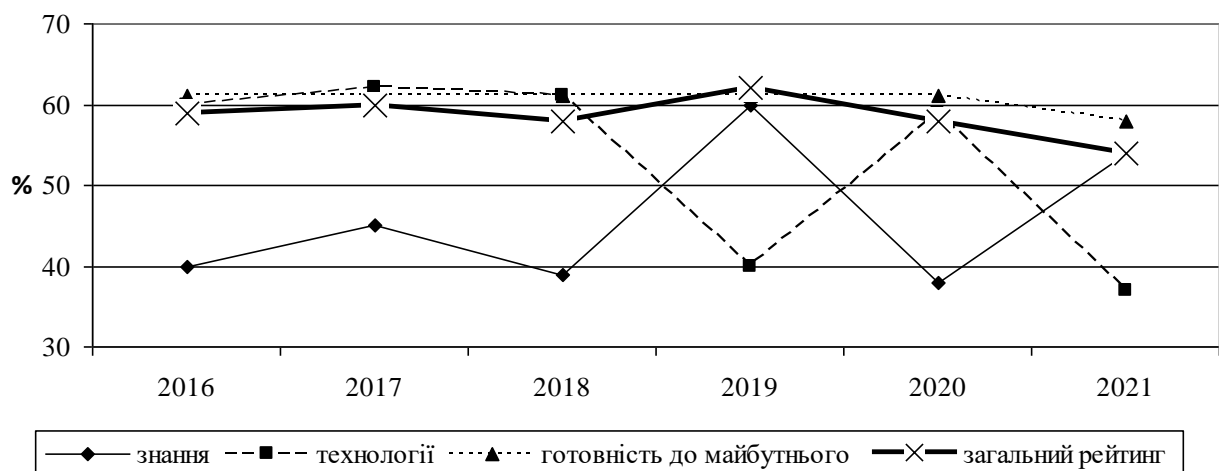


Рис. 2.1. Показники України за складовими рейтингу цифрової конкурентоспроможності, сформовано на основі [212]

Загалом 54 місце в рейтингу 63 країн із мінімальним покращенням до 24 лютого 2022 р. є скоріше негативним результатом, оскільки вказує на низьку швидкість цифровізації національної економіки. І. Саух, В. Шиманська й Т. Момот вбачають в основі такої ситуації загалом поточну неготовність суспільства й бізнесу до створення й застосування цифрових технологій, адже «...освоєння цифрових технологій потребує особливих адаптаційних підходів, включаючи готовність суспільства долучатись до процесів, пов'язаних з цифровими технологіями, наприклад, здійснювати покупки в мережі Інтернет..., а також гнучкості бізнесу через здатність трансформувати свої бізнес-моделі, щоб скористатися новими можливостями» [132, с. 230]. Додатково потрібно врахувати й те, що військові дії будуть мати виключно

негативні наслідки в формі посилення економічної нестабільності, руйнування технологічної інфраструктури й втрати людських ресурсів, що загалом знизить позиції України в рейтингу цифрової конкурентоспроможності, тобто пригальмує і так невисокі темпи цифровізації економіки та ускладнить конкуренту позицію країни.

Іншим показником, який слугує інформаційною основою для розуміння інтенсивності цифровізації національної економіки на фоні таких процесів в інших країнах, виступає Глобальний Індекс інновацій (Global Innovation Index (GII)). В основі розрахунку цього показника покладено визначення 80 індикаторів із відповідним групуванням для чіткості сприйняття результатів та можливості розроблення в подальшому відповідних стратегічних програм для покращення ситуації. На основі опрацювання щорічних звітів [211; 198] нами визначено рейтингове місце України за цим індексом: 2015 р. – 64; 2016 р. – 56; 2017 р. – 50; 2018 р. – 43; 2019 р. – 47; 2020 р. – 45; 2021 р. – 49; 2022 р. – 57; 2023 р. – 55. У межах 2018–2023 рр. явним є послаблення позицій, хоча при загальній кількості країн (131) Україна залишається у верхній половині рейтингу. Відповідно до даних звіту про ГІІ за 2023 р., результати рейтингу України у розрізі основних груп були визначені так: «результати знань і технологій» – 45; «ділова витонченість» – 48 (високий результат за індикатором «працевлаштування жінок з науковим ступенем» – 2); «людський капітал і дослідження» – 47 (найкращий результат за індикатором «середнє співвідношення учень/вчитель» – 14); «творчі результати» – 37; «інфраструктура» – 77; «інституції» – 100 (критичний рівень за індикатором «політична та операційна стабільність» – 130); «досконалість ринку» – 104. В цілому ГІІ, як і попередньо розглянутий Індекс цифрової конкурентоспроможності, дозволяє констатувати поточну пасивність у цифровізації національної економіки, що провокує погіршення ситуації через динамічність змін в інших країнах, які вбачають в інноваціях основу для технологічного поступу за рахунок більш раціонального використання наявних

природних ресурсів та нарощування обсягів створення й удосконалення цифрових продуктів.

Ще одним показником цифровізації економіки був ICT Development Index (IDI), тобто індекс розвитку інформаційно-комунікаційних технологій, який розраховувався з 2009 до 2017 рр. Проблеми із отриманням достовірних даних не дозволили продовжити його використання у 2018 р., але уже наявні результату все-таки дають певне уявлення про хід процесів і стосовно України. За традиційною для такого типу показників послідовністю, розрахунок інтегрального індексу вимагав визначення низки первинних показників, які в подальшому об'єднувалися у три групи, тобто «використання ІКТ» (вагомість – 40%; 5 складових, серед яких наявність у домогосподарствах персональних комп'ютерів, доступ до фіксованого Інтернету, пропускна здатність Інтернету), «доступність до ІКТ» (вагомість – 40%; 3 складові, які визначають інтенсивність використання Інтернету) та «навички ІКТ» (вагомість – 20%; 3 складові, що покликані охарактеризувати рівень володіння населенням цифровими навичками). Дослідження охоплювали 167 країн, серед яких Україна посідала такі рейтингові місця за величиною IDI: 2002 р. – 59; 2007 р. – 51; 2008 р. – 59; 2009 р. – 62; 2010 р. – 65; 2011 р. – 69; 2012 р. – 68; 2013 р. – 73; 2014 р. – 76; 2015 р. – 79; 2016 р. – 78; 2017 р. – 79. У 2012–2017 рр. відбулася певна стабілізація, але потрібно врахувати, що цей індекс також характеризує інтенсивність поширення ІКТ у світі, тобто стабільність у другій частині загального рейтингу демонструє фактичну нездатність надолужити уже наявне відставання від лідерів. Зроблені узагальнення ґрунтуються й на тому, що у 2017 р. Україна розміщувалася в рейтингу нижче за усі сусідні країни, зокрема Польщу (49), Угорщину (48), Румунію (58), Молдову (59). Загалом, як і стосовно вище розглянутих індексів, IDI вказував не лише на незадовільний рівень застосування ІКТ, але й нездатність здійснити рішучі кроки щодо покращення ситуації через нижчі темпи змін порівняно з тими тенденціями, що характерні для світової економіки.

Державна служба статистики України розпочала приділяти належну увагу відстеженням тенденцій цифровізації економіки порівняно недавно, тобто з 2018 р., зосередившись лише на окремих аспектах, зокрема на наявності підключення підприємств до Інтернету. В подальшому перелік параметрів був змінений й розширений за рахунок кількісної характеристики інтенсивності здійснення електронної торгівлі, активності підприємств у соціальних мережах та застосування ними інших цифрових технологій. Відтак сьогодні такі дані необхідно сприймати як вагоме доповнення до індикаторів, що визначаються міжнародними інституціями. Нами були вибрані лише окремі показники, які дозволяють сформулювати цілісне уявлення про стан і тенденції цифровізації національної економіки, першим з яких можна вважати рівень підключення підприємств до Інтернету (рис. 2.2).

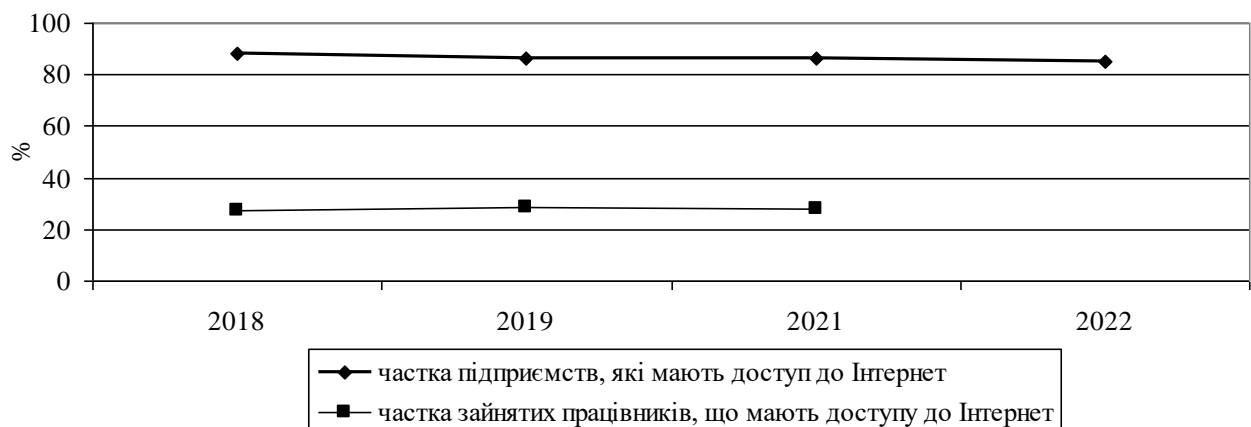


Рис. 2.2. Динаміка частки підприємств та зайнятих в їх умовах працівників стосовно підключення до Інтернету, сформовано на основі [139]

Певне зменшення частки підприємств, що мають доступ до Інтернету у 2019–2021 рр. пояснюється збільшенням таких суб'єктів в абсолютному вираженні, що й спровокувало певні структурні зміни. Спад у 2022 р. викликаний початком нової фази військової агресії із порушенням господарської діяльності більшості українських підприємств та ускладненням процесу отримання статистичних даних. У розрізі окремих видів економічної діяльності проявляється специфіка національної економіки, коли у 2022 р.

максимальна частка була притаманна не торгівлі чи виробникам інформаційного продукту, а операціям з нерухомістю (99,7%), виробництву коксу, продуктів нафтопереробки (98,7%) та постачанню електроенергії, газу й пари (96,9%). Аналітичні дані стосовно масштабів діяльності вказують, що лідерами у підключенні до Інтернету залишаються середні підприємства, зокрема у 2022 р. таких було 91,6%, коли серед малих цей показник становив 83,4%, а великих – 88,3%.

В аналітичних матеріалах (за винятком 2022 р.) міститься також інформація про кількість робочих місць, що забезпечені доступом до Інтернету. Хоча середній рівень в економіці і не є високим, зазначене пояснюється специфікою функціональних завдань, адже не усі роботи вимагають активного обміну інформацією. Відтак максимальне значення у 2021 р. фіксувалося стосовно діяльності туристичних агентств (91,1%), створення інформаційно-комунікаційних технологій (86,5%) та комп'ютерного програмування (85,2%), коли в переробній промисловості загалом 20,6%.

Основою для характеристик фактичного стану технічної інфраструктури, що забезпечує обмін інформацією, можуть бути дані про частку підприємств, які мають фіксований доступ до Інтернету. Такі показники не лише суттєво нижчі порівняно із загальним доступом до мережі (2018 р. – 62,1%, 2019 р. – 60,9% та 2021 р. – 61,8%), але також вказують на обмеженість у швидкості обміну інформацією. У 2021 р. більшість підприємств, тобто 40%, мали змогу використовувати мережі, швидкість на яких обмежена 100 Мбіт/с, що скоріше є недоліком у конкурентній боротьбі, де прихильність споживача визначається швидкістю відкриття веб-сторінки та завантаженням цікавого й корисного контенту. Наявні недоліки в розвитку мереж передачі інформації гальмують активність українських підприємств в інформаційному просторі. Частка підприємств, що використовує соціальні медіа для двостороннього зв'язку із споживачами й просування свого продукту, є критично низькою порівняно із кращими світовими практиками. Не лише іноземні споживачі, але й більшість української молоді надають перевагу, при здійсненні купівлі більшості товарів

тривалого використання, онлайн формату, тобто через віртуальне відвідування крамниць із можливістю ознайомлення з відгуками, здійсненням порівняння за ключовими параметрами та відстеженням зміни попиту й ціни на певний товар. У 2018–2022 рр. фактично відсутні позитивні зміни у частці таких підприємств, що використовували в своїй діяльності соціальні медіа: 2018 р. – 29,7%, 2019 р. – 30,1%, 2022 р. – 29,1%, що вказує на застій у цифровізації на мікро- й мікрорівні, а також реалізується у недостатній комунікації із споживачами, що не сприяє досягненню поставлених корпоративних цілей. У розрізі окремих видів економічної діяльності (станом на 2022 р.) лідируючі позиції займають туристичні агенції (60,1%), видавничі структури й виробники відеопродукції (59,4%) та торговельні підприємства (45,2%). Цікавою є структура соціальних медіа, що активно використовуються українськими підприємствами (рис. 2.3).

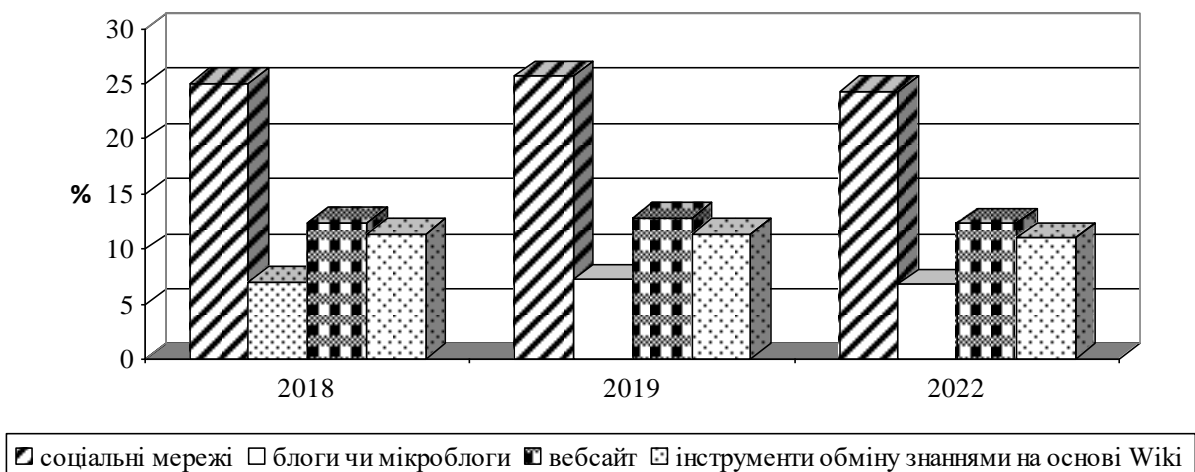


Рис. 2.3. Динаміка структури основних видів соціальних медіа, що використовуються українськими підприємствами, сформовано на основі [139]

Приділення уваги соціальним мережам можна трактувати не лише з позиції намагання покращити двосторонній зв'язок і пришвидшення донесення необхідної інформації до споживачів, об'єднаних у цільові аудиторії, але й через менші витрати й простоту реалізації. Водночас у стратегічному значенні лише активність у застосуванні усіх видів соціальних медіа уможливіє досягнення синергетичного ефекту, тобто покращення конкурентної позиції в умовах зростаючих темпів цифровізації економіки.

Основними причинами невеликої частки підприємств, що використовують вебсайт, пояснюється значними витратами на його створення, потребою постійного оновлення, тобто наповнення корисним контентом, котре вимагає залучення креативних фахівців, а також необхідністю застосування таких інструментів цифрового маркетингу як SEO та SEM для покращення позиції у видачі пошукових систем, що неможливо без команди висококваліфікованих ІТ-спеціалістів. Зроблене узагальнення набуває підтвердження в даних щодо активності застосування вебсайту підприємствами за масштабами діяльності, коли на такий крок зважувалися великі суб'єкти (у 2021 р. – 69,0%), проявляли інтерес середні (47,8%) та були пасивними малі (30,5%). Можна погодитися із позицією Д. Котелевець стосовно того, що «...з фінансових (і частково – кадрових) причин малі підприємства зазвичай неспроможні повною мірою забезпечувати технічну, комерційну, інформаційну та маркетингову сторони перманентної підтримку вебсайту» [78]. Аналітичні дані опосередковано вказують ще й на те, що для більшості українських підприємств вебсайт не став ефективним інструментом у конкурентній боротьбі за прихильність споживачів. Так, у 2021 р. 31,0% підприємств-власників вебсайту використовували його для інформування про асортиментний ряд, 0,4% створили налаштування для здійснення споживачем онлайн-замовлення, 4,5% передбачили можливість унесення змін у типове замовлення, 9,3% уможливили підконтрольність процесу виконання операції, 9,3% підтримували особливий профіль покупця, 16,9% містили посилання на профілі у соціальних мережах. Такі результати засвідчують обмеженість у використанні усіх можливостей вебсайту, що не сприяє отриманню очікуваного результату.

COVID-19 надав поштовх для більш активного розвитку електронної торгівлі через можливість уникнення фізичного контакту, а відтак зниження ризику захворювання. Одна із найбільших переваг електронної торгівлі полягає у спроможності реалізовувати продукцію без посередників і будь-яких географічних обмежень, що створює важливу конкурентну перевагу в умовах обмеженої купівельної спроможності населення. Аналітичні дані стосовно

України вказують на фактичну пасивність українських підприємств, тобто неспроможність використати нові можливості, які не зникли після завершення пандемії, а забезпечили виникнення нової культури у задоволенні потреб. Кількість підприємств в Україні, що використовували електронну торгівлю, залишалася незмінною: 2018 р. – 5,0%, 2019 р. – 4,8%, 2020 р. – 4,9%, 2021 р. – 5,0%, як і реалізованої продукції (% до загального обсягу): 2018 р. – 3,5%, 2019 р. – 4,5%, 2020 р. – 5,0%, 2021 р. – 5,3%. Схожа пасивність українських підприємств проявляється і у застосуванні інших інформаційно-комунікаційних технологій (частка у загальній кількості підприємств), зокрема у 2021 р. чат-сервіс мали 9,1%, купували послуги хмарних обчислень – 10,2%; проводили аналіз «великих даних» – 12,7%, використовували 3D-друк – 2,3%.

Певну складність становить неоднорідність часових періодів у визначенні рівня кожного показника, але динаміка з 2018 р., тобто початку досліджень аналітиками Державної служби статистики, є незначною, тобто немає суттєвих як позитивних, так і негативних змін, що дозволяє сприймати представлені вище дані як констатацію факту. Загалом ситуацію із використанням сучасних інформаційно-комунікаційних технологій, що становлять основу третьої Пр, можна вважати критичною, адже йдеться про поодинокую активність, а не цілеспрямовану реалізацію програми стосовно подолання наявного технологічного відставання від економічно розвинутих країн. Підтвердженням поточної неспроможності реалізувати третю промислову революцію є те, що у 2021 р. лише 2,9% підприємств використовували у своїй діяльності роботів.

Зосередження уваги при характеристиці цифровізації національної економіки лише на технологічних аспектах можна розширити через розгляд й людського фактору. За результатами аналітичних досліджень у 2021 р. 21,7% підприємств звітувалися про наявність у штаті фахівців з інформаційно-комунікаційних технологій. Водночас питанням навчання в цій сфері у 2020 р. приділили увагу лише 4,5% підприємств. Враховуючи вище розглянутий низький рівень активності в застосуванні цифрових технологій й недостатню увагу до покращення професійних здібностей відповідних фахівців, можна

дійти висновку про наявність проблеми в кадровому забезпеченні, джерелом якої є пасивність керуючої ланки, яка не враховує високі темпи технологічного поступу, що вимагає постійної уваги до розвитку людського капіталу.

Аналітичні матеріали Державної служби статистики дозволили виявити та більш глибоко пізнати проблеми українських підприємств у сфері застосування ІКТ, які становлять основу цифровізації національної економіки та кожного підприємства. Поточний рівень цифровізації є критичним і не може бути компенсований імпортом цифрових продуктів та устаткування, оскільки поглиблюється технологічний розрив, що негативно впливає на конкурентні позиції кожного українського підприємства та країни загалом. Не сприяють вирішенню цієї складної проблеми й законодавчі ініціативи, які в межах останнього десятиліття набули прояву у вигляді не нормативних законодавчих документів, що повинні спиратися на реальні базові показники із чітко визначеним планом поетапного виконання заходів на основі координації дій органів державної влади, бізнесу та місцевого самоврядування, а концепцій із декларуванням намірів щодо досягнення необхідного рівня цифровізації відповідно до світових тенденцій розвитку цифрової економіки. В цьому контексті доцільно згадати два документи, тобто «Концепцію розвитку цифрової економіки та суспільства на 2018–2020 роки» [124] та «Національну стратегію економічного розвитку України на період до 2030 року» [123]. І. Яненкова доволі критично характеризує зміст цих документів, доводячи, що вони розроблялися «...не спираючись на законодавчі документи щодо їх розробки, ...не регламентуються з точки зору обов'язковості їх виконання, не враховують попередні стратегії та концепції уряду, ... недостатньо враховують особливості інституційного середовища і механізми господарювання в Україні» [191, с. 14]. Тобто, на відміну від економічно розвинутих країн, де ініціатива цифровізації належить державі, стимулюється й фінансово підтримується задля покращення конкурентних позицій країни, в Україні ці процеси відбуваються завдяки ситуаційній ініціативі частини бізнесу під тиском транснаціональних корпорацій.

Підводячи підсумки, доцільно констатувати, що результати багаторічних досліджень міжнародних й українських інституцій переконливо доводять про поточну орієнтацію України на розвиток сервісів як можливого шляху посилення цифровізації національної економіки, ігноруючи кращі практики країн-лідерів, які приділяють максимальну увагу інвестиціям у розвиток високотехнологічного промислового виробництва, створення цифрових технологій, покращення інформаційної інфраструктури. Відтак стосовно України фіксуються суттєво нижчі темпи поступу у цифровізації економіки, що поглиблює «технологічний розрив». Фактично за результатами більшості індексів наша країна перебуває у нижній частині рейтингів, суттєво поступаючись не лише країнам-лідерам, але й найближчим сусідам за наявності суттєво вищого людського капіталу. Аналітичні матеріали Державної служби статистики вказують на інноваційну пасивність основної частини українських підприємств, що ставить під сумнів можливість реалізації не четвертої, а хоча б третьої ПР, що уже у короткостроковій перспективі буде посилювати загрози для ЕБ кожного виробника через відкритість внутрішнього ринку й послаблення його конкурентних позицій.

Згідно з визначеними у цьому підрозділі завданнями, в подальшому увага буде зосереджена на питаннях оцінювання діяльності підприємств ВПГ, тобто видавничих структур і поліграфічних підприємств, продукція яких значною мірою пов'язана із задоволенням інформаційних потреб населення, а також характеризується трансформацією, тобто йдеться про дедалі частіше представлення в цифровому варіанті на заміну традиційному у вигляді надрукованих на папері книг, брошур, газет і журналів.

Першочергово було визначено динаміку кількості підприємств за двома ключовими видами економічної діяльності, тобто «поліграфічна діяльність» (код за КВЕД-2010 – 18) та «видавнича діяльність» (відповідно – 58), що в графічному вигляді подано на рис. 2.4.

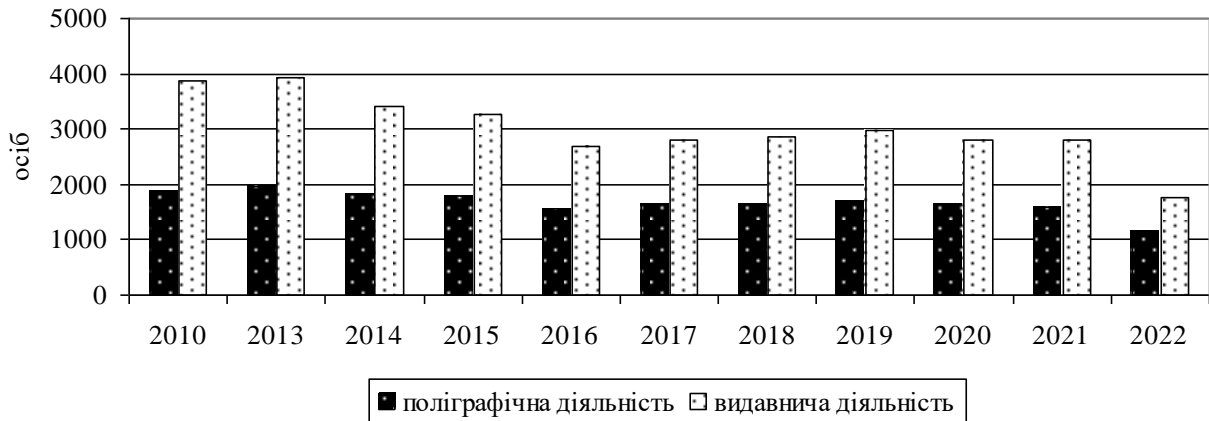


Рис. 2.4. Динаміка кількості діючих підприємств ВПП, сформовано на основі [140, с. 147]

Стосовно діяльності поліграфічних підприємств можна говорити скоріше про певну відносну стабільність щодо учасників ринку, адже у 2010 р. на ринку працювали 1892 суб'єкти із подальшим суттєвим зниженням у 2016-му до 1568 одиниць і наступним частковим відновленням до 1700 у 2019-му. Більш цікавим є те, що в Україні в межах 2017–2022 рр. здійснювало діяльність лише одне велике поліграфічне підприємство і критично мала кількість середніх, зокрема у 2022-му – 46 одиниці. Це також вказує, що поточні потреби у видавничій та невидавничій (етикетна, пакувальна, канцелярські й білові товари тощо) продукції задовольняються за рахунок роботи малих підприємств. Цей факт частково узгоджується зі світовими трендами, зокрема в частині «...більш швидкого розвитку цифрових невеликих друкарень, що спеціалізуються на випуску дрібних накладів і друці змінних даних» [29, с. 865]. Переваги малих підприємств дають змогу максимально повно врахувати інтереси невеликих груп споживачів, оперативно реагувати на зміну попиту й здійснювати діяльність географічно близько до клієнтів. Інший аспект полягає в тому, що виробнича база малих підприємств уможливорює виготовлення продукції дрібними партіями, тобто із обмеженою присутністю на ринку без можливості впливу на його розширення й розвиток. З позиції забезпечення інформаційної безпеки держави це є проблемним моментом, оскільки фактично

ліквідується один із каналів поширення інформації, що відповідає національним інтересам та заповнює інформаційний простір країни.

Діяльність видавничих структур характеризується більш негативними аспектами, що проявляється у значному зменшенні кількості учасників ринку. Якщо у 2010 р. налічувалося 3865 видавництв, то до у 2022-му їх кількість скоротилася до 1755 одиниць, тобто 54,59%. Із 2012 р. в Україні не функціонує жодне велике видавництво, а кількість середніх щорічно зменшується, тобто із 106 одиниць у 2010-му до 38 у 2022-му. Фактично зазначене суттєве скорочення відбувалося за рахунок малого бізнесу, що опосередковано вказує на недоліки адаптації видавничих структур до зміни інтересів споживачів щодо отримання інформації.

Певна сталість у кількості учасників поліграфічного ринку не відповідає динаміці чисельності зайнятих працівників (рис. 2.5). У 2010 р. на поліграфічних підприємствах було зайнято 20966 осіб, але в подальшому спостерігається скорочення персоналу до 13307 осіб у 2022-му, тобто на 36,53%. Такі процеси є негативним фактом, оскільки вказують на втрату кадрового потенціалу, а відтак – погіршення конкретних позицій. Зроблений висновок також спирається на порівняння середньої чисельності поліграфічних підприємств, коли в Німеччині «...в середньому на одному підприємстві зайнято не більше 16 осіб, а в штаті 80% друкарень значиться менше 20 працівників» [29, с. 866], але в Україні такий показник становить лише 10 осіб, тобто наявними є проблеми в кадровій безпеці.

Порівняно із поліграфічними підприємствами, кадрові втрати видавничих структур є більш вагомими, тобто в межах 2010–2022 рр. вони сягнули 69,94%. Тут причинами є незадовільний рівень оплати праці, але в межах країни, тобто на телебаченні, в офісах великих корпорацій, при створенні інформаційного продукту, що використовується в рекламних цілях, тощо.

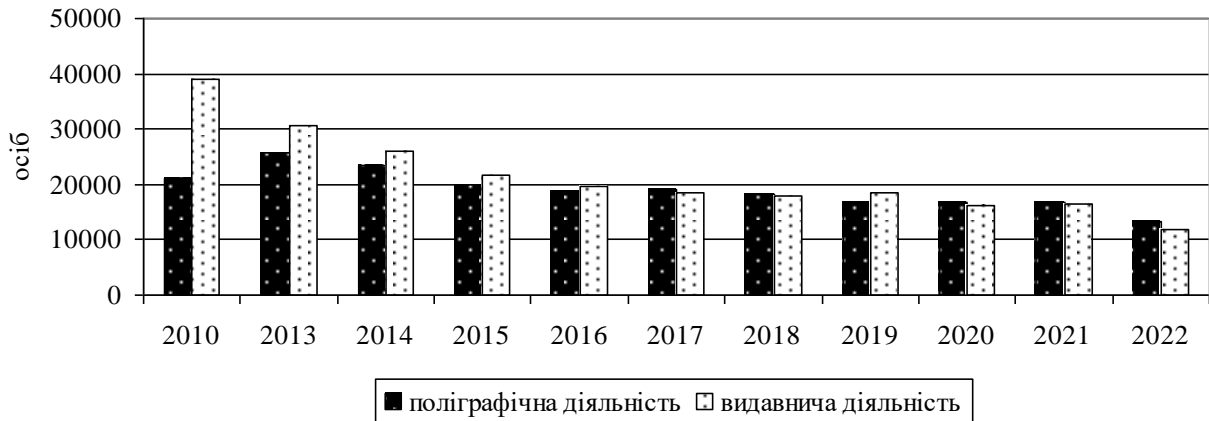


Рис. 2.5. Динаміка чисельності зайнятих працівників на підприємствах ВПП, сформовано на основі [140, с. 147]

Оминаючи ретельний розгляд усіх аспектів діяльності підприємств ВПП, вважаємо за необхідне проаналізувати рівень і динаміку фінансових результатів, зокрема чистого прибутку (збитку) та рентабельності операційної діяльності (рис. 2.6–2.7).

Величина кінцевого фінансового результату діяльності поліграфічних підприємств та видавничих структур змінювалася у 2010–2022 рр. синхронно, тобто формувалися збитки у 2014–2015 рр. та 2017-му, що можна пов'язати із початком агресії Російської Федерації та складністю стабілізації господарської діяльності в подальшому. Наступний етап, тобто 2018–2020 рр., характеризується відмінністю у величині отриманого чистого прибутку, який суттєво вищий у поліграфічних підприємств. Такі зміни частково відповідають світовим тенденціям, коли «...зростання обсягу друку книг та журналів в світі склало 0,6%, упаковок – 2,5%, комерційної друкарської продукції – 0,8%» [40, с. 78]. Поступовий зсув асортименту продукції поліграфічних підприємств на користь невидавничої продукції прослідковується в більшості економічно розвинутих країн, зокрема в Німеччині «...книги, журнали, газети в загальному обсязі виробництва становлять відповідно 6,6%, 11,3% та 11,4%. Частка друкованої продукції, пов'язаної з рекламою, досягає в загальному вартісному обсязі виконаних поліграфічних робіт більше 60%» [29, с. 865]. Такі дані є

свідченням трансформації в діяльності поліграфічних підприємств, що проявилася у зміні асортименту продукції на користь тієї, що потребує переробна промисловість.

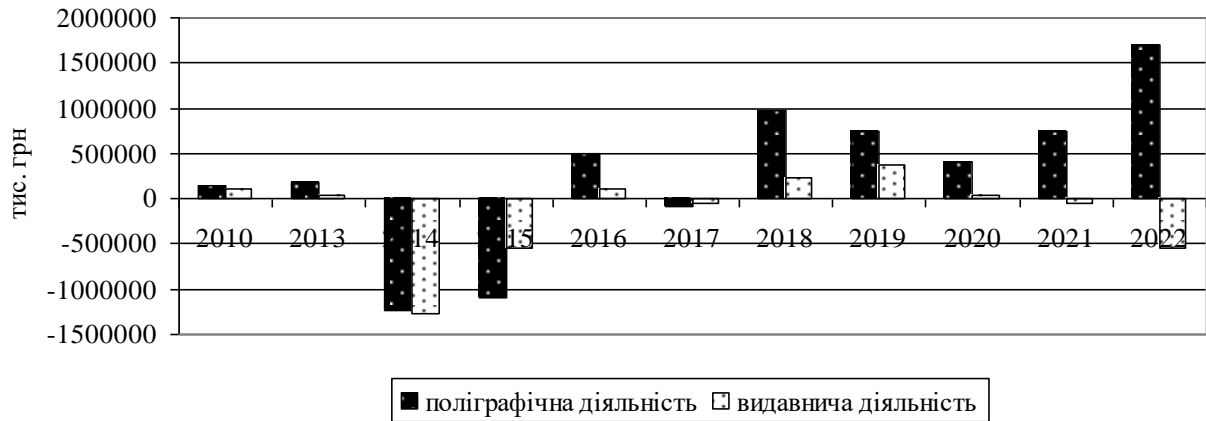


Рис. 2.6. Динаміка кінцевого результату діяльності підприємств ВПП, сформовано на основі [140, с. 147]

Попри позитивний сумарний результат діяльності поліграфічних підприємств у 2018–2022 рр., в аналітичних матеріалах Державної служби статистики містяться дані про значну частку збиткових суб'єктів. У 2010 р. збитковими були 37,7% діючих поліграфічних підприємств, коли в іншій крайній часовій точці частка таких скоротилася до 31,0%, що є свідченням необхідності приділення більше уваги забезпеченню фінансової безпеки. Стосовно видавничих структур спостерігається значно гірша ситуація, оскільки, крім збитковості у 2022 р., що можна пов'язати із військовими діями, простежується більша частка – 38,1%.

Незадовільний рівень фінансових результатів підприємств ВПП можна пояснити низькою рентабельністю операційної діяльності (рис. 2.7). Для порівняння доцільно взяти рівень цього показника загалом в економіці, зокрема у 2010 р. – 4,0%, 2014 р. – (-4,1%), 2015 р. – 1,0%, 2019 р. – 10,2%, 2021 р. – 12,6% та 2022 р. – 3,3%.

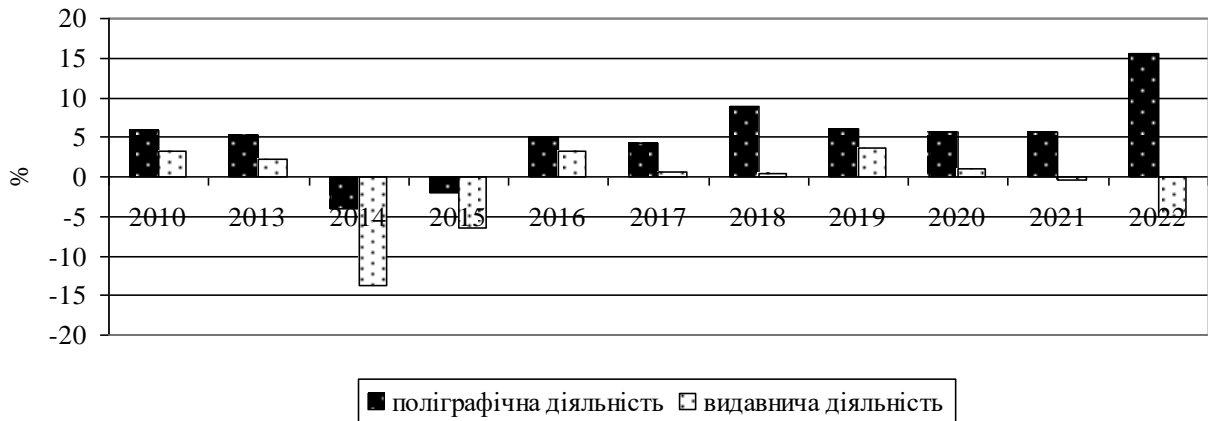


Рис. 2.7. Динаміка рентабельності операційної діяльності підприємств ВПГ, сформовано на основі [140 с. 147]

Якщо для поліграфічних підприємств у 2014 р ситуація загалом відповідала тій, що спостерігалася в економіці, то відновлення відбувалося суттєво нижчими темпами, а COVID-19 спричинив чергове погіршення, зокрема у 2021-му зазначений показник становив 5,7%, але у 2022 р. різко зріс до 15,6%. Значно складніша ситуація була у видавничій діяльності, де, окрім збитковості у 2014–2015 рр., яка сягнула у 2014-му 13,7%, спостерігалася подальша мінімальна рентабельність у 2016–2018 рр. із незначним зростанням у 2019-му до 3,7% та зниженням у 2021-му до (-0,5%) та у 2022-му до (-5,0%). Ці аналітичні дані переконливо доводять наявність недоліків у ЦТП ВПГ, коли їх продукція не повною мірою відповідає споживацьким запитам. Зроблене узагальнення спирається на результати відстеження динаміки обсягів виготовлення видавничої продукції за основними видами, тобто книг і брошур (рис. 2.8), журналів й інших періодичних видань (рис. 2.9) і газет (рис. 2.10).

Для наочності сприйняття процесів, що пов'язані із діяльністю підприємств ВПГ, досліджуваний період збільшений до 30 років, тобто з 1990 до 2021 рр. Такий формат вибрано не випадково, адже у 1990 р. тоді існуюча система управління країною передбачала виконання видавничими структурами й поліграфічними підприємствами функції ретранслятора комуністичної ідеології шляхом масового виробництва видавничої продукції. Загальний тираж

книг і брошур сягав рекордних 170 млн примірників. Для порівняння, у згаданому 1990 р. на одного мешканця України припадало 3,28 примірника книжкової продукції, коли у 2021-му – лише 1,09, що з позиції функціонування підприємств ВПП можна вважати катастрофічним спадом обсягів виробництва.

В графічному вигляді чітко простежуються дві тенденції: зменшення річного тиражу та зростання кількості назв, що можна пояснити поступовою втратою державою контролю над цією галуззю як через приватизаційні процеси, так і недоліки в управлінні великими підприємствами, контрольний пакет акцій яких залишався у Державному комітеті телебачення й радіомовлення. Тенденції в обсягах виготовлення книжкової продукції є протилежними до тих, що характеризують розвиток книговидання у світі, оскільки «...у 1960 р. вийшло 332 000 найменувань, у 1990 р. ця кількість становила 942 000 найменувань, а 2007 р. – 976 000 ...кількість щорічно виданих екземплярів (копій) нині оцінюють у 4 млрд» [164].



Рис. 2.8. Динаміка основних показників виробництва книжок і брошур, сформовано на основі [140, с. 112]

Низька купівельна спроможність населення також обмежила обсяги виробництва книжкової продукції, оскільки основну частинку у витратах домогосподарств займають продукти харчування, медичні препарати та комунальні послуги. Потрібно також врахувати, що українські поліграфічні

підприємства як технічно, технологічно, так і сировинно залежні від імпорту. Усе наявне устаткування іноземного виробництва, коли в кращому випадку йдеться про нові засоби, але стосовно друкарського обладнання, то поширеною є практика придбання того, що було уже у використанні на підприємствах Німеччини, Чехії та Польщі. Водночас такі обставини дозволяють зменшити потреби в інвестиційних ресурсах, підтримувати доволі високий технологічний рівень виготовлення продукції та конкурувати із європейськими виробниками.

Однією із причин зменшення попиту на книжкову продукцію, що виготовлена традиційним способом, можна вважати й поступове зростання інтересу до її електронного аналогу. Базовою конкурентною перевагою цифрового аналогу книги є активність читача, що проявляється у можливості сприймати інформацію у вигідному для себе форматі, взаємодіяти з машиною для отримання й покращення цифрових навичок, виконувати роль не лише споживача, але й учасника, тобто творчо розвиватися. Тимчасовою прогалиною є відсутність інтерактивних книг для дорослих читачів, що формує перспективи подальшої ЦТП ВПГ. Глобальною перешкодою можна вважати піратство, що повинно бути об'єктом протидії як на рівні держави, так і кожного виробника цифрового продукту шляхом розвитку СЕБП.

Низхідна хвиля стосовно річного тиражу й кількості назв журнальної продукції у 2010–2022 рр. стала наслідком часткової втрати інтересу споживачів до такого каналу надходження інформації під тиском розширення доступу до мережі Інтернет. Негативний вплив мало також зростання цін на крейдований папір, який не виготовляється в Україні, а імпортується, що при девальвації національної грошової одиниці спричинило значне збільшення собівартості продукції, а відтак журнали стали менш доступними для споживачів.

Доволі схожі тенденції помітні і стосовно газетної продукції, але їх початком став 2005 р. Втрата газетою двох ключових раніше існуючих переваг, тобто оперативність у поданні інформації та мінімальна ціна одного примірника, під тиском Інтернету спровокувало зменшення попиту споживачів

на цей вид видавничої продукції. Частина видавництв, використовуючи іноземну практику, створили цифрові аналоги традиційних газет, але їх популярність є нижчою порівняно із сайтами новин, блогами, соціальними мережами тощо. Лише особи старшого віку залишаються прихильниками газети у паперовому виконанні, коли середнє покоління та молодь більш активно використовують сучасні пристрої обміну інформацією, що забезпечують безперешкодний і вільний доступ до відомостей без часових і географічних обмежень.

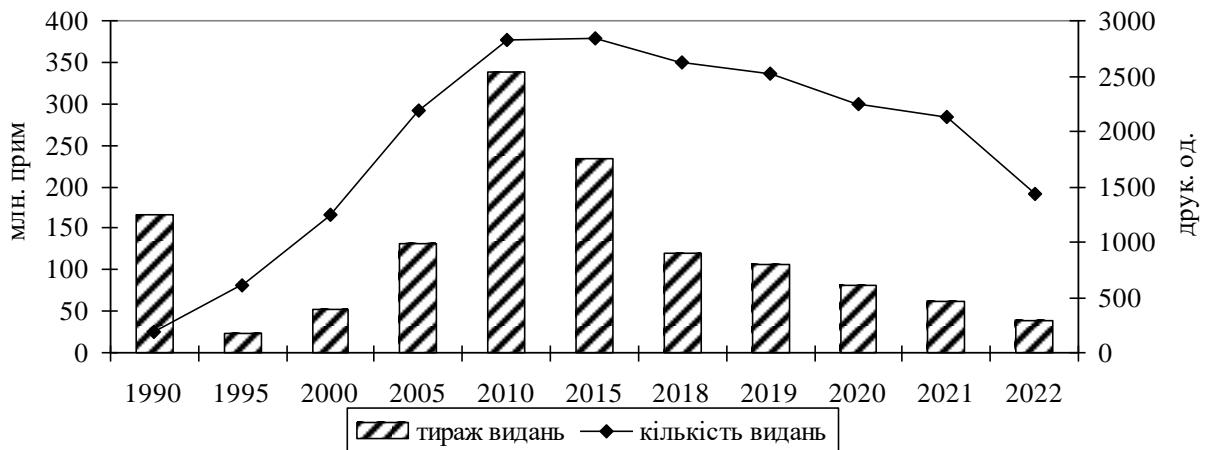


Рис. 2.9. Динаміка основних показників виробництва журналів та інших періодичних видань, сформовано на основі [140, с. 112]

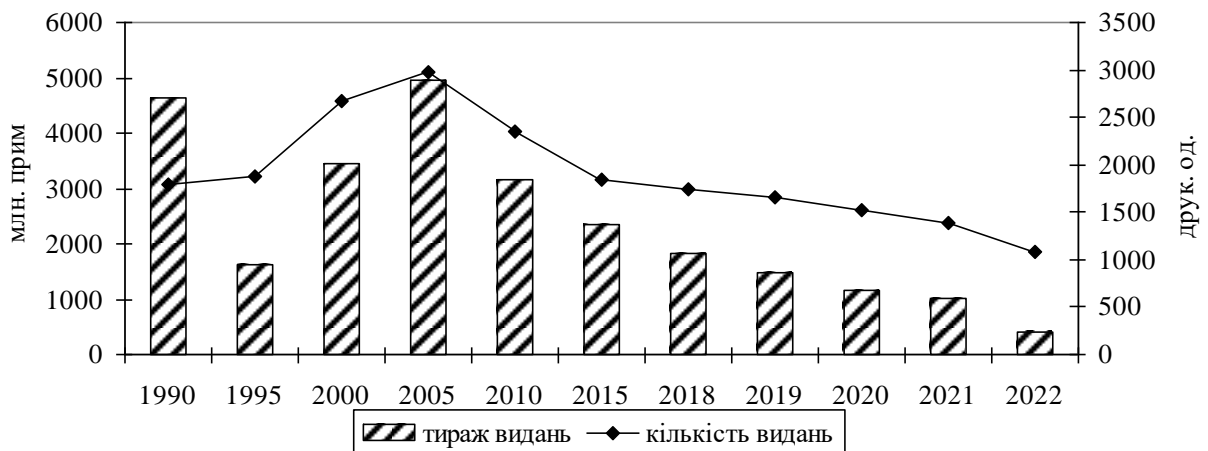


Рис. 2.10. Динаміка основних показників виробництва газет, сформовано на основі [140, с. 112]

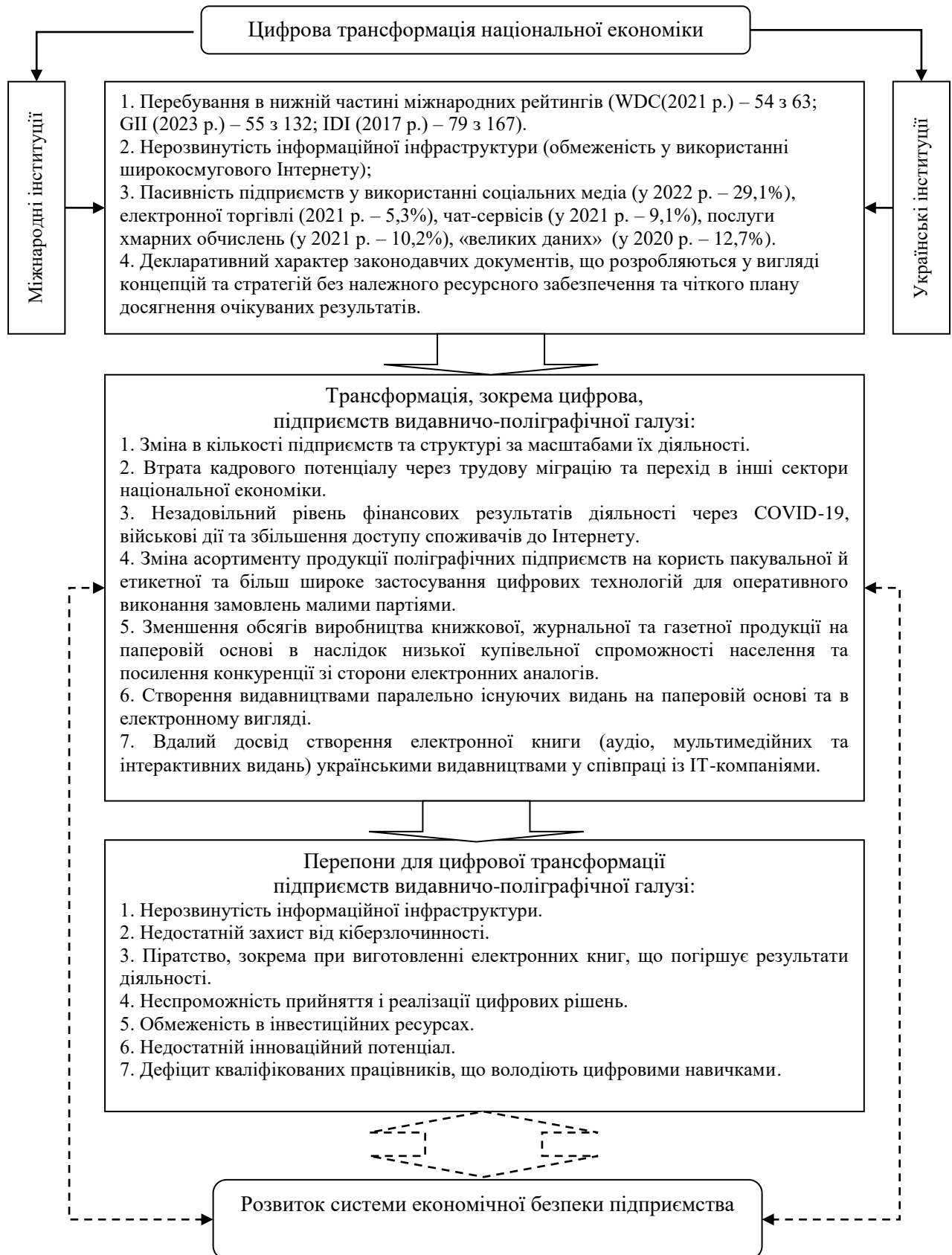


Рис. 2.11. Середовище розвитку системи ЕБП ВПГ, сформовано автором

Результати проведеного аналітичного дослідження, основою чого послуговували матеріали міжнародних та українських інститутів, нами узагальнено на рис. 2.11.

В графічному вигляді виділено кількісні ознаки ЦТ національної економіки, окреслено параметри змін у діяльності підприємств ВПП, зокрема в частині як утворення нових можливостей через більш активне використання цифрових технологій для поліграфічних підприємств при зміні асортименту продукції на користь пакувальної та етикетної та видавничих структур в умовах паралельної підготовки видань у паперовому й електронному виконанні, так і загроз, що переважно пов'язані із збільшенням у споживачів популярності новітніх потокових сервісів. Окремо виділено перепони, що гальмують цифрову трансформацію поліграфічних підприємств та видавничих структур, що повинно стати об'єктом уваги співробітників служби безпеки. Пунктиром підкреслено авторську позицію, що ЦТП повинна здійснюватися під контролем служби безпеки, а відтак передбачати її розвиток, з огляду на необхідність більш повного використання нових можливостей та ліквідації загроз.

2.2. Теоретико-методичний підхід до оцінювання розвитку системи економічної безпеки підприємства

Процес забезпечення ЕБП характеризується високою динамічністю змін базових параметрів, що вимагає швидкої реакції та активності в діях суб'єктів безпеки. Такими базовими параметрами виступають зміни зовнішнього середовища та корективи внутрішніх процесів, що провокує виникнення нових викликів, посилення ризиків та необхідності протидіяти загрозам. Окреслення фактичного рівня ЕБП традиційно пропонується проводити за рахунок практичного застосування однієї із відомих методик оцінювання. Нездатність застосувати іноземні розробки через суттєво відмінні умови безпекової діяльності актуалізувало потребу в посиленні власних наукових розвідок, що

забезпечило певний поступ. Водночас результатом застосування більшості відомих методик оцінювання є констатація факту про рівень безпеки, в окремих випадках – результативність дій суб'єктів безпеки, але питання розвитку СЕБП як таке не розглядається. Причиною цього можна вважати домінуюче сьогодні хибне уявлення, що таку систему необхідно, як обов'язкову складову в межах системи управління підприємством, одноразово створити і в подальшому зміни не потрібні, адже вона повинна виконувати поставлені завдання. В основі такого погляду лежить відносна стабільність економічних процесів планової економіки, але не максимальна невизначеність та висока швидкість зміни впливу внутрішніх і зовнішніх факторів ринкового середовища. СЕБП повинна не лише постійно змінюватися, але й формувати прийнятну основу для трансформації підприємства загалом відповідно до нових викликів як щодо ймовірного виникнення раніше неіснуючих або менш пріоритетних загроз, так і можливостей, використання яких дозволяє здобути конкурентні переваги. Відтак актуальним стає створення методичних засад оцінювання не лише ЕБП загалом, а й розвитку такої системи, що не може здійснюватися на основі існуючих підходів. У межах цього підрозділу нами поетапно буде проведено критичний огляд відомих підходів до оцінювання ЕБП із подальшим обґрунтуванням авторської позиції щодо оцінювання розвитку СЕБП та демонстрації можливості практичного застосування в умовах підприємств ВПГ.

Уникаючи розгляду кожного із відомих сьогодні підходів, можна підтвердити раніше висловлену тезу, що жоден із них не дозволяє відстежити процес розвитку СЕБП. Тобто можна спостерігати зміну окремих індикаторів, рівень безпеки стосовно функціональної складової чи загалом ЕБП, але стан і відповідність діючої СЕБП умовам функціонування підприємства та поставленим перед суб'єктами безпеки завданням – ні. Зазначене обумовило, враховуючи усі позитивні аспекти відомих підходів в оцінюванні ЕБП, формування авторського розуміння суті такого процесу задля інформаційної підтримки розвитку СЕБП, зокрема із врахуванням специфіки діяльності структур ВПГ. Складність виконання завдання полягає у відмінності стосовно

традиційного оцінювання ЕБП, коли дослідженню не підлягає певна кількість індикаторів, що визначають поточний стан фінансово-господарської діяльності, а воно повинно передбачати об'єктивне аналізування кількісних й якісних змін у самій СЕБП. Тобто ключовим є фіксування розвитку, класифікація якого була деталізована у підрозділі 1.3, а відтак може мати різний характер, тобто, для прикладу, як прогресивний, так і регресивний, або без чітких ознак ключового спрямування, але із обов'язковим врахуванням руху у зовнішньому й внутрішньому середовищі й стратегічних орієнтирів підприємства загалом. Відтак оцінювання повинно проводитися стосовно СЕБП як відкритої системи, тобто з постійною прив'язкою до змінних актуальних на певний момент часу умов. Зазначене ще раз доводить відмінність авторського підходу від розглянутих вище, стосовно яких такі початкові параметри не закладаються. Дотримуючись цих міркувань, нами в перелік індикаторів не були включені ті, що визначають рівень безпеки стосовно функціональних складових ЕБП, але деталізовані напрями цільового спрямування в розвитку СЕБП, зокрема, такі як економічне, адміністративно-правове, інформаційно-аналітичне, техніко-технологічне та кадрове. Іншим важливим моментом є спроба поєднати засади реалізації програмно-цільового та експертного підходів в оцінюванні. Тобто передбачено процедуру визначення початкових індикаторів за кожною складовою цільового спрямування, але на основі думок експертів із подальшою процедурою узагальнення й узгодження та розрахунком групових й інтегрального показників, чому повинна сприяти система коригуючих (вагових) коефіцієнтів, що визначають питому вагу кожного індикатора. Позиція експертів підлягає означенню в кількісному вимірі через застосування шкали, бали: «0,0-0,33» – негативні зміни; «0,34-0,66» – поєднання різноспрямованих незначних змін; «0,67-1,0» – покращення. З метою якісного оцінювання розвитку СЕБП для експертів було візуалізовано зазначену шкалу, як на рис. 2.12.

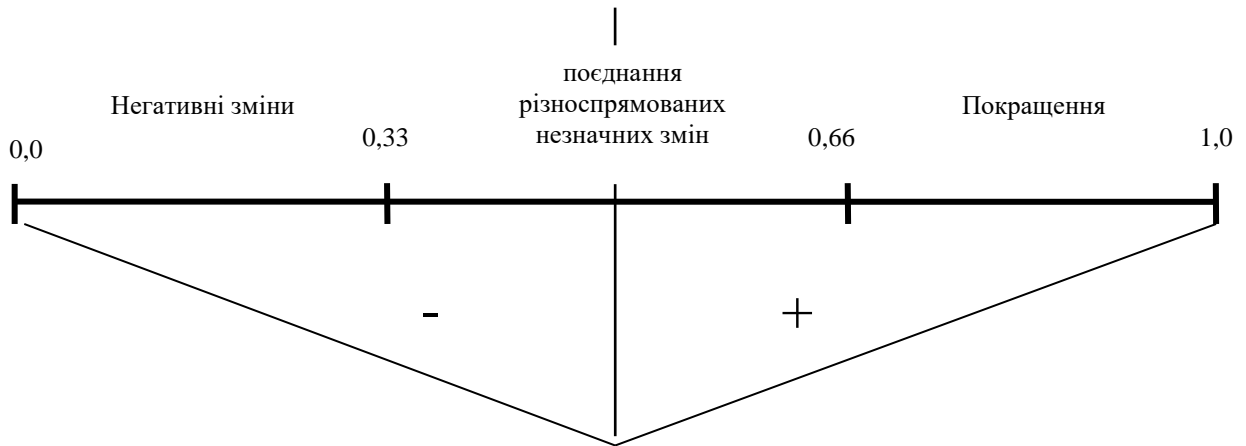


Рис. 2.12. Шкала оцінювання розвитку СЕБП, розроблено автором

Запропонована шкала дає змогу конкретизувати будь-які незначні зміни в СЕБП, тобто не крайні значення (близько до 0,0 – максимально негативні та до 1,0 – найбільш позитивні), а й усі проміжні за рахунок відповідного кількісного еквіваленту.

Уточнення потребує те, що «негативні зміни» або «поєднання різноспрямованих незначних змін» визначаються стосовно СЕБП щодо умов здійснення безпекової діяльності. Ті інструменти, що були результативними в минулому періоді, в умовах нових викликів і загроз можуть не забезпечити необхідний ефект через відсутність адаптаційних процедур і поступу в діях суб'єктів безпеки. Відтак акцентується не на констатації факту існування СЕБП із деталізацією її організаційної структури та матеріального забезпечення й результатах активності суб'єктів безпеки, а на її розвитку, тобто здійсненні кількісно-якісних змін, що дають змогу посилити захист підприємства відповідно до динаміки зовнішнього середовища та перемін внутрішніх процесів. Окреслені базові засади, що характеризуються суттєвою відмінністю від існуючих сьогодні підходів до оцінювання ЕБП, графічно, як модель, подано на рис. 2.13.

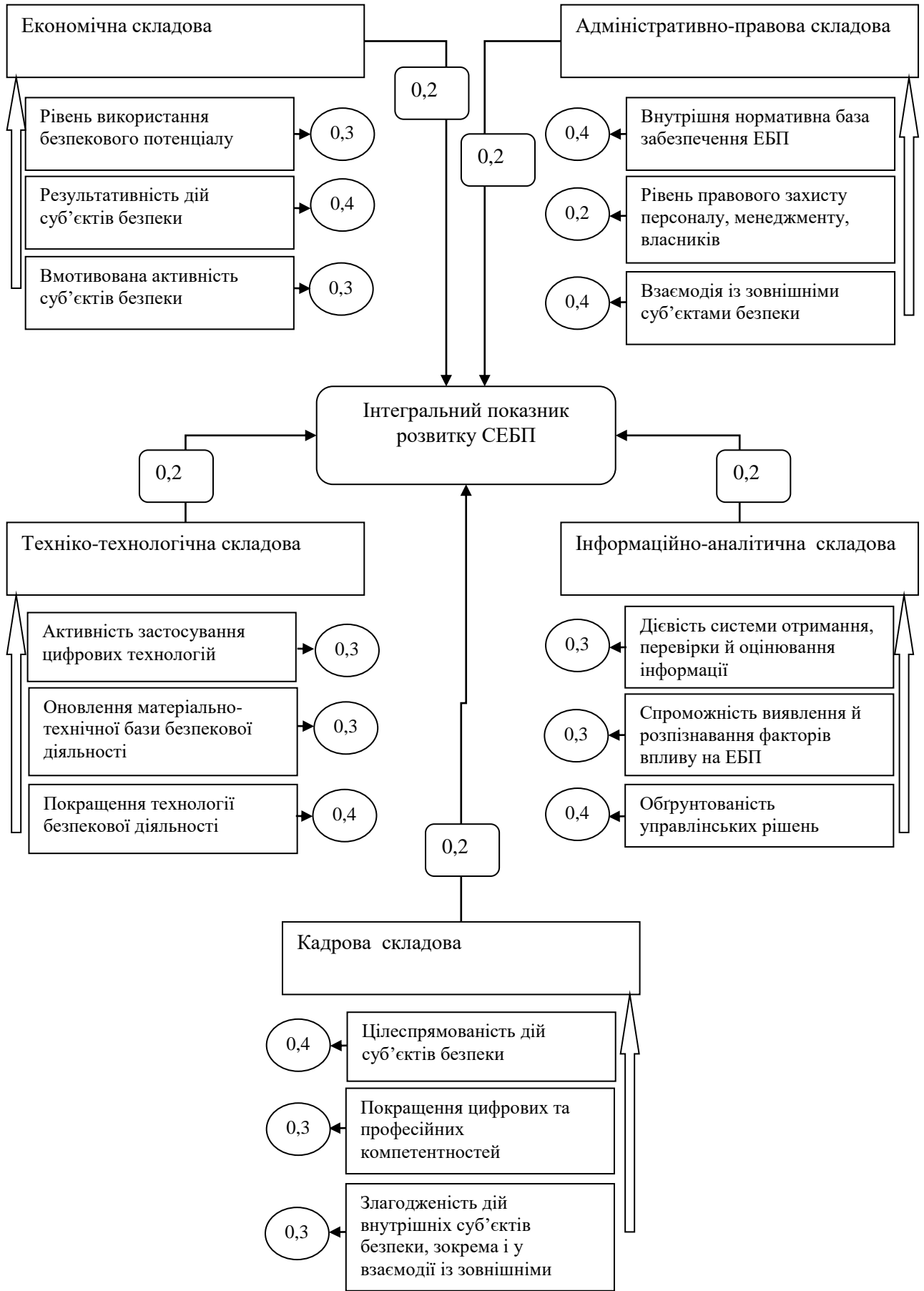


Рис. 2.13. Модель оцінювання розвитку СЕБП, сформовано автором

Початковий етап у застосуванні розробленої моделі полягає у визначенні стосовно певного підприємства ВПП п'ять груп індикаторів шляхом опитування експертів серед менеджерів різних рівнів управління, а також залучених фахівців. Установлення фактичного значення за кожним індикатором проводиться через узгодження крайніх відхилень у поглядах експертів і розрахунок середньої величини. В подальшому визначається груповий показник, з огляду на фактичне значення певного індикатора та вагового коефіцієнта. Третій етап полягає у визначенні інтегрального показника розвитку ЕБП на основі групових показників і відповідних вагових коефіцієнтів. Вагові коефіцієнти в межах груп і в подальшому для розрахунку інтегрального показниками нами розраховані, зважаючи на позицію експертів та враховуючи специфіку діяльності видавничих структур і поліграфічних підприємств.

Основною особливістю запропонованого підходу є те, що оцінювання може проводитися щоквартально та щорічно, відштовхуючись від розуміння тих змін, які відбулися в умовах діяльності певного підприємства, перетрубацій у внутрішніх процесах та активності суб'єктів безпеки. Динамічність змін вимагає постійної трансформації безпекової діяльності, відтак пасивність або низька швидкість у реагуванні сприймається як проблема, яка породжує загрозу нездатності захистити бізнес та забезпечити більш повне використання усіх нових можливостей для втримання й покращення конкурентних позицій. Результат оцінювання є основою розуміння поступу в безпековій діяльності, підґрунтям якого повинен бути розвиток СЕБП, темпи якого визначаються динамічністю перебігу подій за межами і стосовно самого підприємства. Фактично формується аналітичне підґрунтя для цілісного сприйняття усіх процесів у динаміці, коли основна увага приділяється не констатації фактів, що відбулися в минулому, та виправленню помилок, а відстеженню перебігу подій зі створенням основи для швидшого реагування в режимі реального часу. Безперечно, певна складність виникає через підбір і взаємодію із компетентними експертами, які повинні бути обізнаними не лише зі

специфікою діяльності певного підприємства, але володіти інформацією щодо розвитку галузі та трансформацій в національній економіці загалом. Водночас такі додаткові труднощі повинні бути ліквідовані за рахунок наукової організації системи оцінювання, зокрема шляхом ретельної роботи з підбору та підтримання постійного контакту з експертами. Наріжним каменем повинно стати усвідомлення, що пасивність у розвитку СЕБП еквівалентна втратам через нижчу результативність дій суб'єктів безпеки, а їх уникнення вимагає першочергового відповідного інформаційного забезпечення, зокрема за рахунок реалізації сформованого теоретико-методичного підходу.

Практичне застосування сформовано підходу нами здійснено в умовах активно діючих видавничих структур і поліграфічних підприємств. Це, зокрема:

– ТзОВ «Видавничий дім «Високий замок» (в подальшому ТзОВ «ВД «Високий Замок») (КВЕД 58.13) – спеціалізується на виготовленні газетної продукції, друкуванні рекламної та бланкової продукції;

– ТзОВ «Ельграф» (КВЕД 17.29) – виготовляє широкий асортимент пакувальної продукції;

– ТзОВ «Кліше» (КВЕД 17.29) – здійснює додрукарські процеси (виготовлення форм), а також друк етикетної та пакувальної продукції;

– видавничо-виробниче підприємство «Місіонер» (у подальшому ВВП «Місіонер») (КВЕД 58.11) – виконує видання книг, газетної та журнальної продукції;

– ТзОВ «Кольорове небо» (КВЕД 17.21) – здійснює друк рекламної та етикетної продукції.

Основою представлення результатів здійсненого оцінювання розвитку СЕБП можуть слугувати дані стосовно динаміки ключових показників діяльності визначеної групи підприємств. Розраховані темпи росту стосуються важливих індикаторів, що характеризують загалом рівень безпеки кожного підприємства, але нами вони застосовані для формування загального уявлення про безпекову діяльність. Тобто наше завдання полягає не в оцінюванні ЕБП, а

в розумінні суті змін у СЕБП під впливом зовнішніх і внутрішніх процесів як основи ЦТП загалом через формування безпечної для цього основи. Відтак таке цілісне уявлення буде вибудовуватися через виявлення тенденцій стосовно зміни чистого доходу від реалізації (рис. 2.14), середньоспискової чисельності працівників (рис. 2.15), середньорічної вартості активів (рис. 2.16), величини чистої рентабельності продажу (рис. 2.17). Попри те, що нами до уваги взяті видавничі структури та поліграфічні підприємства із схожими параметрами фінансово-господарської діяльності, але відносні величини, на відміну від абсолютних, більш якісно дозволяють відстежити загальні тенденції й охарактеризувати можливий вплив основних факторів. Такий підхід ще виправданий через можливість спостереження змін у діяльності кожного підприємства під впливом двох важливих зовнішніх факторів, тобто у 2019–2021 рр. – COVID-19, а в подальшому з 2022 року – нової хвилі військової агресії з боку Російської Федерації. Зазначене доволі чітко відображається уже стосовно першого показника, тобто величини чистого доходу від реалізації (рис. 2.14).

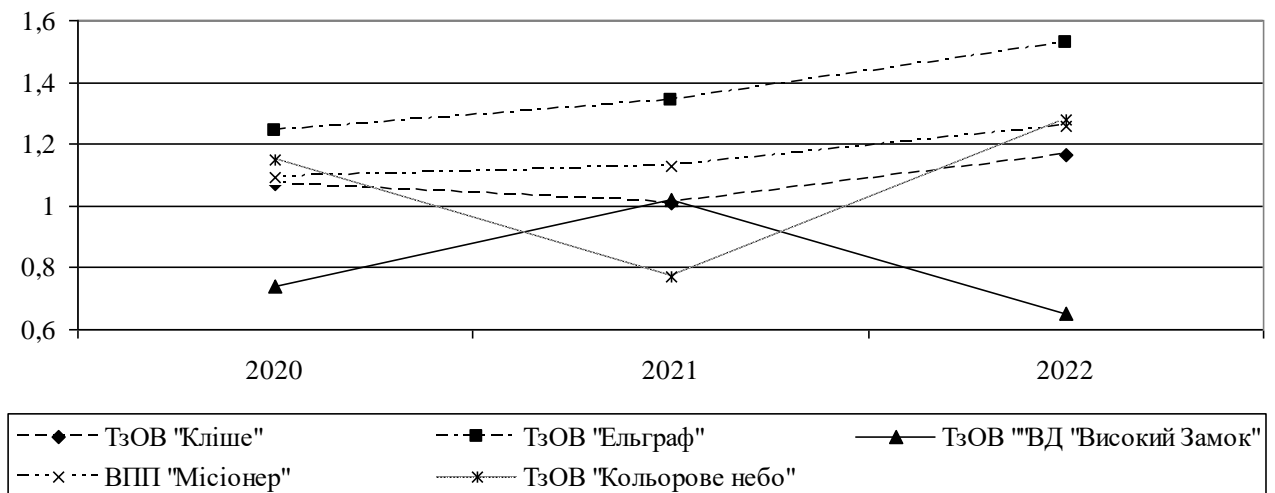


Рис. 2.14. Динаміка чистого доходу від реалізації стосовно сформованої вибірки підприємств ВПГ, 2019–2022 рр., розраховано автором

Розраховані темпи росту вказують на дещо відмінні тенденції в зміні виручки від реалізації продукції та послуг досліджуваної групи видавничих

структур та поліграфічних підприємств. Як уже підкреслювалося у підрозділі 2.1, COVID-19 частково пригальмував економічні процеси загалом у національній економіці, що змусило підприємства адаптовуватися. Менш швидка реакція щодо стабілізації ситуації відбулася в умовах ТзОВ «ВД «Високий замок», адже у 2020-му тут фіксувався спад на рівні 26%, коли усі інші підприємства відзначилися, хоча і не значним, але приростом чистого доходу. Важливо, що у 2021 р. ситуація змінилася на користь згаданого підприємства, коли приріст сягнув 2%. Кардинально відмінна динаміка спостерігається стосовно ТзОВ «Кольорове небо», адже спад у 2021-му у 23% змінився наступним різким приростом на 28%. Загалом такі суттєві перепади у величині чистого доходу засвідчують критично високу нестабільність через послідовну дію COVID-19 та військове протистояння стосовно кожного підприємства, що вимагало від суб'єктів безпеки приділення максимальної уваги питанням відновлення стабільності у функціонуванні уже в суттєво відмінних нових умовах. Також потрібно врахувати й ту обставину, що найбільш позитивні результати демонстрували ті підприємства, які виготовляють етикетну й пакувальну продукцію, яка є необхідною й обов'язковою складовою продукції переробної промисловості, попит на яку стабільно високий попри вплив будь-яких факторів. Відтак суб'єкти безпеки повинні були в процесі реалізації адаптаційних процедур зважаючи на необхідність максимального використання нових можливостей.

Трудові ресурси мають визначальний вплив на діяльність підприємств ВПП через необхідність володіння знаннями щодо специфічного й складного технологічного процесу, систематичного набуття нових компетенцій, покращення своєї майстерності, креативного підходу до виконання кожного замовлення. В рамках сформованої групи підприємств негативна динаміка в межах 2019–2022 рр. була характерна лише для ТзОВ «ВД «Високий замок». Аналізуючи розраховані темпи росту стосовно середньоспискової чисельності працівників (рис. 2.15), доцільно зважати ще й на такі факти: по-перше, згідно з наведеними даними у підрозділі 2.1, в межах ВПП триває подальше скорочення

кадрового потенціалу, коли ситуація в умовах усіх проаналізованих підприємств, окрім ТзОВ «ВД «Високий Замок», відрізняється позитивним, хоча і незначним, зростанням чисельності залучених працівників, що вказує на результативну роботу в сфері кадрової безпеки; по-друге, падіння середньоспискової чисельності працівників в умовах ТзОВ «ВД «Високий Замок» у 2020 р. на 5%, 2021 р. – 10% та у 2022 р. – на 49% вказує на ознаки реалізації загрози, вплив якої виходить за межі кадрової безпеки.

Зменшення чисельності працівників з 178 осіб у 2019 р. до 73 у 2022-му вимагає першочергового застосування комплексної програми ліквідації загрози для ЕБП стосовно ТзОВ «ВД «Високий замок». Користь такого трактування доводить синхронність змін у величині чистого доходу від реалізації, коли скорочення у 2022 р. відносно 2021-го сягнуло 35%. Попереднім твердженням може бути таке, що вказує на нездатність суб'єктів безпеки діяти в постпандемічному періоді в поєднанні із активною фазою військового протистояння. Тобто незадовільні темпи росту СЕБП унеможливають ефективну реакцію на високу динаміку зовнішнього середовища та внутрішніх процесів, що у сукупності негативно впливає на рівень ЕБП загалом.

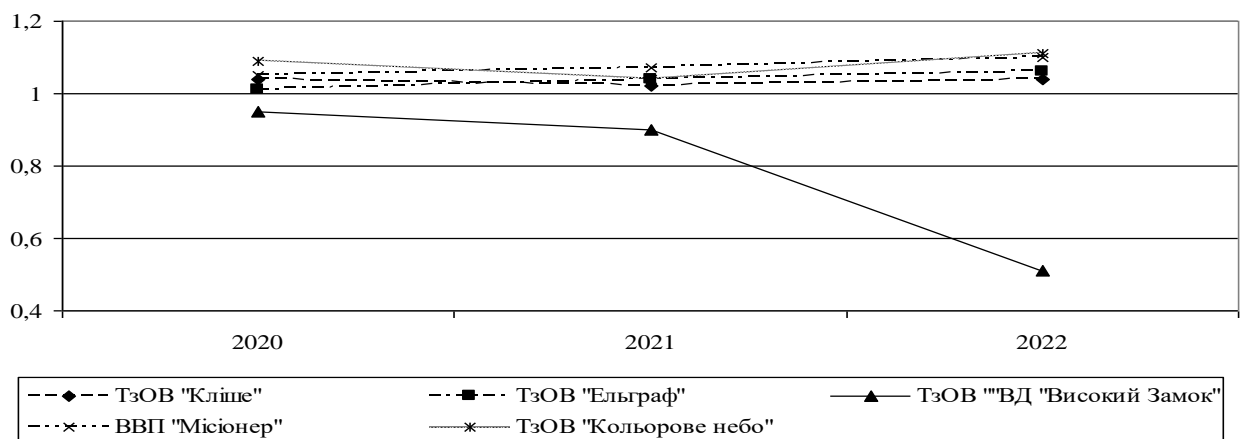


Рис. 2.15. Динаміка середньоспискової чисельності працівників стосовно сформованої вибірки підприємств ВПГ, 2019–2022 рр., розраховано автором

Зроблені узагальнення актуальні і стосовно наступного важливого показника – середньорічної вартості активів (рис. 2.16).

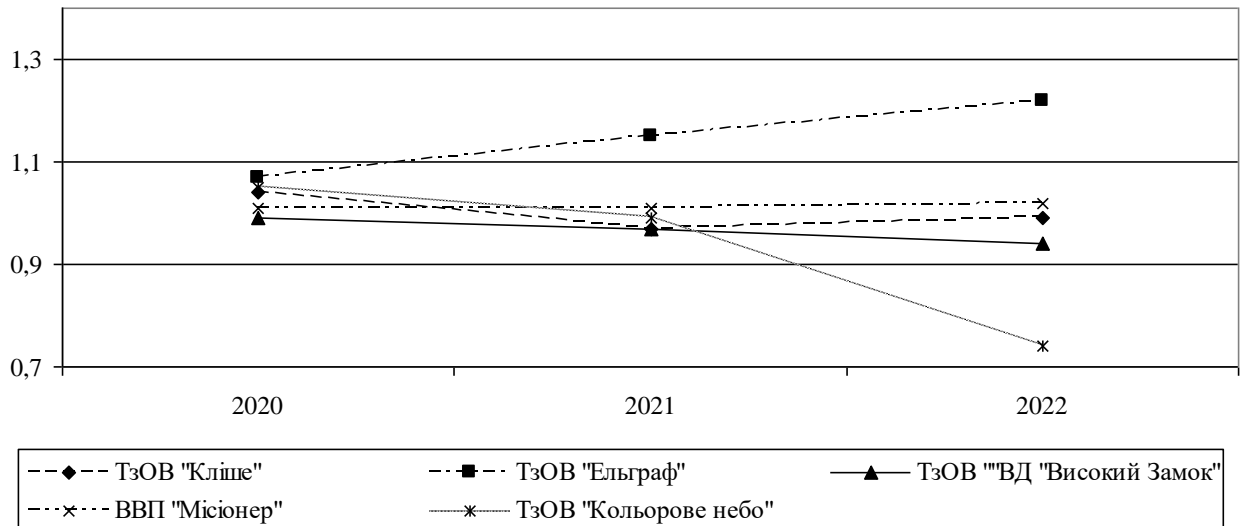


Рис. 2.16. Динаміка середньорічної вартості активів стосовно сформованої вибірки підприємств ВПГ, 2019-2022 рр., *розраховано автором*

Найвищий темп приросту середньорічної вартості активів був зафіксований стосовно ТЗОВ «Ельграф» у 2022 р. на рівні 22%, що зумовлено реалізацією програми глибокої модернізації друкарських процесів з придбанням й уведенням в експлуатацію нових машин з вищим рівнем цифрового управління. Більш важливим моментом є те, що простежується довготривала позитивна тенденція, яка вказує на здійснення комплексної програми розвитку технічної бази підприємства задля покращення конкурентної позиції в секторі виробництва пакувальної продукції. Вагоме зменшення досліджуваного показника стосовно ТЗОВ «Кольорове небо» у 2022 р. на 26% викликано переглядом кредитної політики, що забезпечило посилення контролю за надходженням виручки від реалізації, ефективність використання оборотних коштів та зниження ризиків невиконання зобов'язань перед кредиторами.

У підрозділі 2.1 нами наголошувалося на невисокому рівні рентабельності у ВПГ. Зроблені узагальнення набувають підтвердження і у величині й динаміці чистої рентабельності продажу, яка була розрахована стосовно сформованої сукупності підприємств (рис. 2.17).

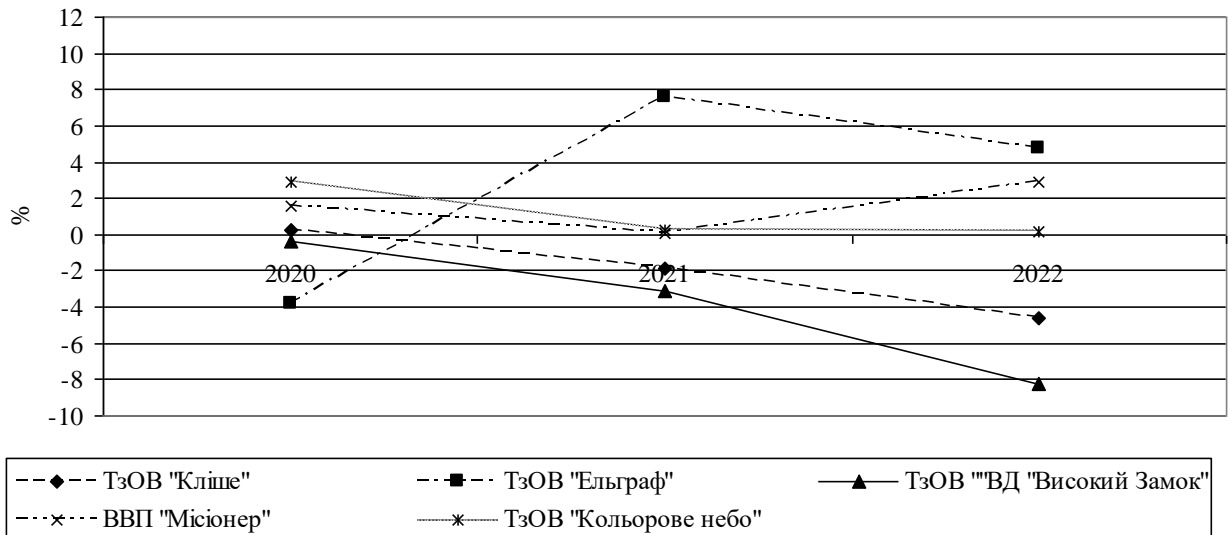


Рис. 2.17. Динаміка рівня чистої рентабельності продажів (%) стосовно сформованої вибірки підприємств ВПГ, 2019–2022 рр., розраховано автором

Поруч із катастрофічним зменшенням чистого доходу і втратою людських ресурсів, діяльність ТзОВ «ВД «Високий замок» у 2019–2022 рр. характеризується й негативною динамікою фінансових результатів, зокрема чиста рентабельність на кінець вказаного періоду визначена як збитковість у розмірі 8,25%. У сукупності усі зазначені індикатори вказують на погіршення рівня ЕБП, що потребує вжиття термінових заходів з боку суб'єктів безпеки для припинення руйнування підприємства як системи, відновлення стабільності та продовження існування. Стосовно інших підприємств, то фіксується динамічна зміна рівня зазначеного показника, що демонструє максимальну флуктуацію, яка не може залишатися без уваги суб'єктів безпеки задля збереження руху в поточному аттракторі, або переході до нового, який більшою мірою відповідає поточній етапності функціонування під час військового стану для національної економіки.

Резюмуючи, можна стверджувати, що в 2019–2022 рр. через різкі зміни умов функціонування внаслідок COVID-19 та військових дій діяльність відібраних підприємств, як і загалом тих, які працюють у межах ВПГ, характеризується дисбалансом, коли ключовим завданням суб'єктів безпеки

стала швидка реакція з розробленням й реалізацією стабілізуючих та адаптаційних програм. Потрібно визнати, що складність дій суб'єктів безпеки також обумовлена відсутністю досвіду впливу схожих за масштабами та непередбачуваністю наслідків факторів. Фактично в межах кожного підприємства індивідуально генеруються нові ідеї щодо вирішення кожної дрібної та загальної проблеми задля захисту та розвитку бізнесу. Такі моменти стали як необхідним підґрунтям для розвитку СЕБП, так і критерієм, що визначає подальше існування кожного підприємства через спроможність суб'єктів безпеки творчо вирішувати проблеми, яких раніше не виникало.

Проведений розгляд основних показників діяльності сформованої групи підприємств ВПГ вибудовує необхідне підґрунтя для реалізації авторського підходу до оцінювання СЕБП, зважаючи на життєву важливість своєчасного внесення змін в активність суб'єктів безпеки задля протидії й ліквідації раніше неіснуючих загроз та більш повного використання новітніх можливостей.

Співпраця з експертами дозволила визначити рівень кожного із п'ятнадцяти індикаторів стосовно виокремленої групи підприємств ВПГ та в подальшому провести усі необхідні розрахунки стосовно групових та інтегрального показника розвитку СЕБП. Усі проміжні розрахунки нами представлено в Додатку А (табл. А.1-А.5). На рис. 2.18 подано кінцевий результат, тобто інтегральний показник, рівень і динаміка якого суттєво відрізняються щодо кожного досліджуваного підприємства.

Розвиток СЕБП в умовах ТзОВ «Кліше» можна охарактеризувати як поступальний, але з мінімальною динамікою, що визначається значенням розрахованого інтегрального показника: 2019 р. – 0,54; 2020 р. – 0,54; 2021 р. – 0,57; 2022 р. – 0,58. Згідно з розробленою шкалою, виокремлюється поєднання поступальних дій із подальшою нездатністю своєчасно реагувати на вплив ключових факторів. На нашу думку, поступ наявний, зокрема стосовно кадрової та інформаційно-аналітичної складових, але відставання змін в адміністративно-правовому й техніко-технологічному елементах частково

нівелює їх, тим самим позбавляючи підприємство загалом можливості швидшими темпами адаптуватися до нових умов ведення бізнесу.

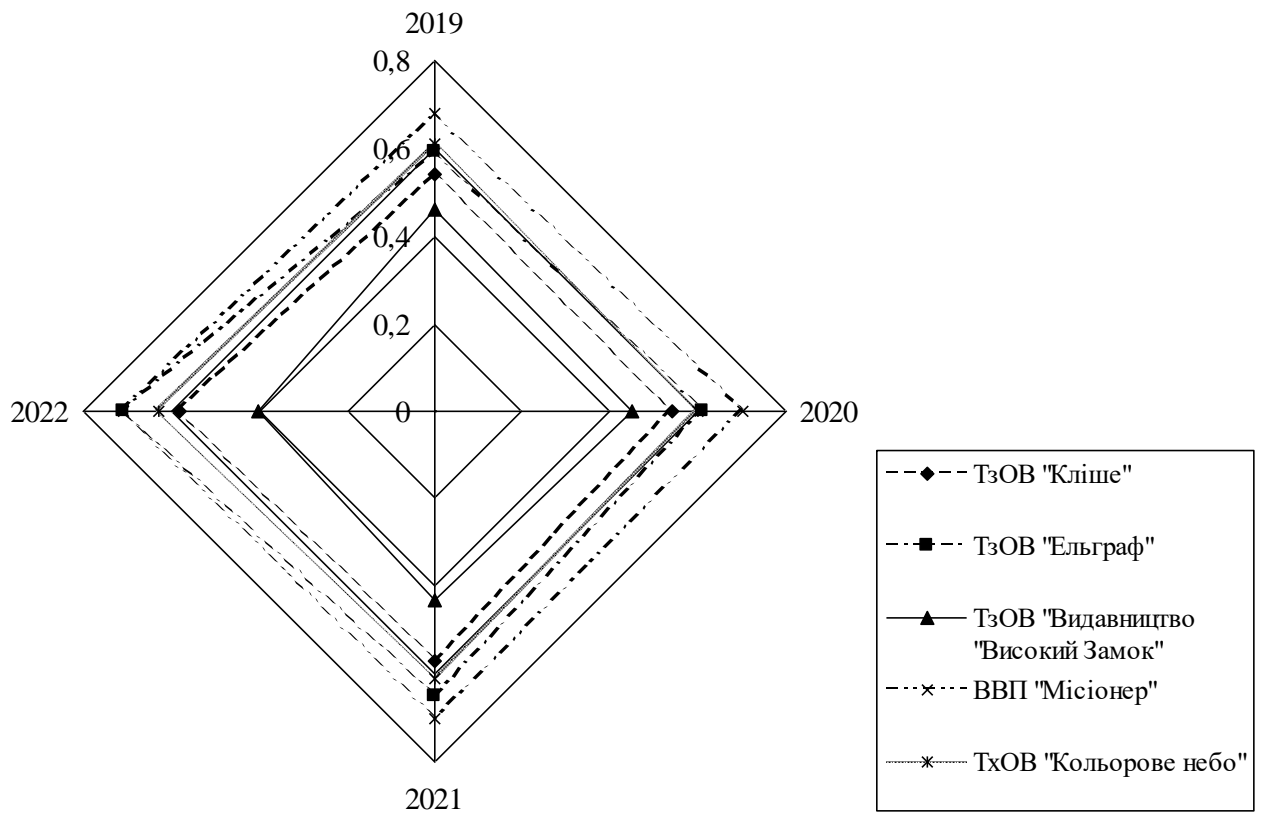


Рис. 2.18. Інтегральний показник розвитку СЕБП, *розраховано автором*

Схожа динаміка в розвитку СЕБП була визначена щодо ТзОВ «Ельграф» (2019 р. – 0,59; 2020 р. – 0,61; 2021 р. – 0,65; 2022 р. – 0,71) та ВВП «Місіонер» (2019 р. – 0,68; 2020 р. – 0,7; 2021 р. – 0,7; 2022 р. – 0,71). Із врахуванням незначних відмінностей можна все-таки говорити про реальний поступ у реалізації безпекового потенціалу й систематичній роботі стосовно використання нових можливостей, зокрема завдяки поглибленню співпраці із зовнішніми суб'єктами безпеки.

Якщо стосовн ТзОВ «Кольорове небо» фіксується динамічне коливання (2019 р. – 0,61; 2020 р. – 0,6; 2021 р. – 0,61; 2022 р. – 0,63), то стосовно ТзОВ «ВД «Високий замок» йдеться про погіршення ситуації (2019 р. – 0,46; 2020 р. – 0,45; 2021 р. – 0,43; 2022 р. – 0,4), тобто деградацію, яка уже в

короткостроковій перспективі унеможливилює реалізацію захисних заходів, а відтак вплив загроз стає результативним і провокує руйнування цього підприємства як системи. Підтвердженням висловленої тези можуть бути раніше розглянуті основні показники діяльності, де відзначалося зменшення обсягів чистого доходу, кадрового складу та погіршення фінансових результатів. Тобто відсутність поступу в розвитку СЕБП спричиняє нездатність адекватно і своєчасно реагувати на зміни в діяльності підприємства. Суб'єкти безпеки не спроможні створювати необхідні умови не лише для розвитку підприємства, але й продовження його функціонування. Якщо розгляд характеру впливу COVID-19 та військових дій вказав на складність швидкої адаптації до впливу цих тимчасових факторів усіх досліджуваних підприємств, то визначені у підрозділі 2.1 довготривалі тенденції у ВПП, які полягають у зменшенні інтересу до книжкової, журнальної та газетної продукції, не були враховані ТЗОВ «ВД «Високий замок», а відтак й стають основною причиною його занепаду. Тобто йдеться про посилення негативного впливу раніше існуючих загроз за рахунок нових факторів, що провокує основу реалізації ефекту «снігової лавини», яку суб'єкти безпеки нездатні зупинити, зокрема в межах застосування стандартного набору інструментів без необхідного поступу стосовно СЕБП. Зазначене ще раз доводить важливість формування засад розвитку СЕБП, зважаючи на цілісне бачення поточних і перспективних умов здійснення безпекової діяльності.

Підводячи підсумки, необхідно констатувати, що висунута ідея із подальшою її реалізацією у вигляді теоретико-методичного підходу до оцінювання розвитку СЕБП та апробацією в умовах п'яти поліграфічних підприємств і видавничих структур у поєднанні із формуванням цілісного уявлення про зміни в національній економіці та ВПП в цілому продемонстрували право на існування й практичну цінність отриманих результатів. Дані про тенденції в розвитку СЕБП засвідчили необхідність приділення особливої уваги в поступі такої системи для поточного функціонування й трансформації кожного підприємства через вибудовування

відповідної безпечної основи з боку суб'єктів безпеки. Одержані результати будуть використані в подальшому для обґрунтування змін у розвитку СЕБП і не лише через суттєвість впливу таких загроз як COVID-19 та військові дії.

2.3. Інформаційне забезпечення розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки

Забезпечення ЕБ в умовах українських підприємств відбувається під впливом значної кількості факторів, пріоритетність яких постійно змінюється. Попри це, безпекова діяльність має бути орієнтована не лише на ліквідацію поточних загроз, що виникають в умовах запровадженого воєнного стану й очікуваних змін під час післявоєнного відновлення національної економіки, але перспективного створення безпечного підґрунтя для трансформації діяльності підприємства відповідно до тенденцій в збільшенні частки цифрової економіки. Таке розширення спектру завдань вимагає перегляду засад формування й внесення коректив у підсистему ЕБП, яка відповідає за ІЗ, коли зміни повинні відстежуватися стосовно поточної ситуації у зовнішньому середовищі й внутрішніх процесів та стосуватися бачення тенденцій в зміні національної економіки й світових зрушень і в реалізації Індустрії 4.0. Йдеться не лише про можливість активнішого використання цифрових технологій для отримання й опрацювання більших обсягів інформаційних ресурсів, а перебудову засад роботи з інформацією як ресурсом, що дає змогу покращити результативність роботи суб'єктів безпеки. Відтак у межах цього підрозділу поставлено завдання щодо перегляду засад і розроблення моделі трансформації ІЗ як одного із важливих напрямів розвитку СЕБП. Визначене завдання та пошук варіантів його вирішення спирається на твердження Лі Якоккі стосовно того, що сучасний менеджер може прийняти обґрунтоване управлінське рішення лише за наявності 95% достовірної інформації, для чого попередньо потрібно приділити

належну увагу отриманню й опрацюванню відомостей з різних джерел, робота з якими займає до третини його робочого часу. Стосовно ж безпекової діяльності, зважаючи на потреби врахування ймовірності виникнення й впливу різного типу ризиків і загроз, то значення формування й застосування ІЗ зростає в рази. Такі аргументи нами використані для першочергового з'ясування суті поняття «інформація», яке лежить в основі ІЗ, як піл час безпекової діяльності, так і загалом управління на кожному рівні.

Сьогодні формується теоретична основа розвитку економіки знань, інформаційного суспільства та інших спрямувань, де інформація розглядається більше як один із найважливіших ресурсів, використання якого має дозволити подальше існування людства за зростаючої обмеженості природних багатств. Попри це, залишається й надалі актуальне сприйняття інформації, що походить від початкового латинського терміна «*informatio*», який окреслює будь-які відомості й дані, якими обмінюються члени спільноти. Аналіз напрацювань науковців дає змогу прослідкувати характер поступової зміни сприйняття інформації від повсякденних повідомлень до стратегічно важливого ресурсу, а також розглянути його нові якості, які актуальні і для суб'єктів безпеки. З позиції філософії важливим доповненням є визначення, згідно з яким інформація становить «...одну з трьох основних (поряд із матерією та енергією) субстанцій, що утворюють природній світ, у якому живе людина» [117, с. 241]. Таке тлумачення вагомо підвищує значення інформації, зважаючи і на специфіку її формування й застосування як ресурсу, який може бути використаний безмежну кількість разів у випадку відповідності заданим параметрам, тобто стосовно повноти, актуальності, цілісності, своєчасності тощо. Технологічний поступ сприяв трансформації у розумінні інформації, коли актуалізувалося її ототожнення зі знаннями, що формуються за результатами певних досліджень і практичної апробації та можуть бути поширені серед ширшого кола зацікавлених осіб. У подальшому такі якості інформації створили основу для перетворення її на продукт, що «...має певні якісні ознаки, собівартість і ціну, оскільки його виробляють так само, як і будь-

який інший продукт» [30, с. 66]. Створення засобів передачі й відтворення провокує й подальше розширення попиту на такий продукт, внаслідок чого виробництво зростає щорічно в геометричній прогресії. Разом із можливістю задовольнити інформаційні потреби дедалі більшої кількості споживачів виникає проблема інформаційного перенасичення зі збільшенням величини «інформаційного шуму», коли пошук необхідної інформації займає куди більше часу й вимагає систематичного оновлення технічних засобів і програмного забезпечення для слідування технічним вимогам. У безпекознавстві така ситуація є підставою для розвитку СЕБП, зокрема тієї її складової, що відповідає за ІЗ. У цьому контексті можна процитувати визначення терміна «інформація», що максимально наближене до сфери управління, в якому Г. Лучик пропонує його розглядати як «...відомості, одержані з різних джерел, які необхідно знайти чи одержати, вивчити чи дослідити, відкинути чи прийняти, перевірити і за необхідністю перевірити ще раз, перетворити на ресурс, прийняти рішення щодо його використання і спрогнозувати її загальну вигоду (економічну, соціальну, технологічну, політичну тощо)» [88, с. 188]. Науковець доводить, що інформація є основою управлінського процесу, вона дає змогу зменшити рівень невизначеності, а відтак знизити ризик. Водночас таке тлумачення повинно враховувати, що інформація в управлінні відрізняється від узагальненого її сприйняття як сукупності відомостей про усі процеси, які відбуваються в життєвому просторі певної людини. Інформація в управлінні повинна відповідати певним критеріям, серед яких основними можна вважати такі: своєчасність, достовірність, чіткість, відповідність фактичному стану й потребам певного користувача тощо. Додатково стосовно безпекового процесу ще й важливою є захищеність. Відтак можна стверджувати, що інформація набуває як властивості цінного ресурсу, адже вимагає значних витрат, так і потребує контролю за ефективністю використання. Сумарно усі розглянуті позиції дають змогу охарактеризувати сучасне сприйняття інформації як ресурсу, що використовується в безпековій діяльності (рис. 2.19).



Рис. 2.19. Сучасне трактування терміна «інформація», що актуальне для безпекової діяльності, *сформовано автором*

Певним доповненням до викладених графічно моментів може бути те, що для суб'єктів безпеки інформація виступає первинним поштовхом до дій. Тобто, йдеться не про факт реалізації певної загрози у вигляді втрат і збитків, а про ті відомості, що вказують на можливі зміни, що в подальшому призведуть до негативних наслідків, або можуть сформувавши можливості, використання яких сприятиме посиленню конкурентних позицій підприємства. Така позиція певною мірою відрізняється від традиційного спрямування дій суб'єктів безпеки виключно на ліквідацію проблемних моментів у діяльності підприємства, оскільки передбачає превентивне реагування, тобто більш ефективне, але можливе лише за наявності відповідного ІЗ.

Сприйняття ІЗ різняться серед представників наукових кіл і підприємців. Поширеним є його розуміння як наявності необхідної інформації для задоволення потреб у процесі прийняття управлінського рішення. Інші варіанти сприйняття відрізняються деталізацією окремих складових, не відкидаючи сутність первинного, де існує чіткий зв'язок між потребою та можливістю її задоволення, що вимагає виконання певних дій із залученням додаткових ресурсів, матеріального, технічного й кадрового характеру. Останнє

прослідковується у позиції Л. Лігоненко та М. Селезова, які вбачають ІЗ у «...сукупності структурних баз даних у вигляді документів, нормативної бази, реалізованих рішень, вербальної та невербальної, кількісної та якісної інформації, що виступають базисом для прийняття рішень» [86, с. 415]. Тобто в такому варіанті йдеться про структурування інформації, що дає змогу виявляти в ній потребу із подальшим наданням адресантам відповідно до встановлених якісних вимог. Більшою мірою на ресурсній основі наполягає С. Палагута звертаючи першочергову увагу на «...сукупність інформаційних ресурсів, засобів, методів і технологій, яка сприяє ефективній реалізації усього процесу управління, зокрема розробленню та реалізації управлінських рішень» [109, с. 419]. Така деталізація доводить, що фактично йдеться про доволі складний процес, який не поступається виробничому, а його реалізація повинна відбуватися відповідно до розробленої технології, тобто бути жорстко регламентованою, із наперед визначеними виконавцями та користувачами, коли результат пов'язаний із спроможністю останніх прийняти й проконтролювати за реалізацією управлінського рішення.

В позиції О. Кузьміна та Н. Георгіаді технічні параметри знаходяться на другому плані порівняно із цільовим призначенням ІЗ, зважаючи на те, що його пропонують сприймати як «...систему якісних і кількісних показників, що характеризують рівень задоволення суб'єктів управлінської діяльності управлінською інформацією та інформаційними технологіями для реалізації інформаційною системою встановлених цілей та завдань» [81, с. 15]. Ми також наголошуємо на потребі організації відповідної системи, яка повинна містити ряд пов'язаних елементів, коли через взаємодію, на основі вхідних ресурсів, уможлиблюється задоволення інформаційних потреб, що буде використано нами надалі стосовно ІЗ дій суб'єктів безпеки.

В. Іванова, з огляду на повсякчасну потребу кожного менеджера в інформації, наполягає на необхідності подання ІЗ як процесу, в межах якого відбуваються операції стосовно «...створення та постачання інформації, доступу до неї» [58, с. 62]. Вважаємо, що таке подання процесу дещо спрощене,

оскільки в сучасних умовах йдеться про суттєво більшу кількість обов'язкових операцій, які виконуються як людиною, так і машиною в автоматичному режимі. Відтак можна говорити про отримання, перевірку, узгодження, аналізування, надання, накопичування й зберігання тих відомостей й даних, які становлять інтерес для відповідних зацікавлених осіб і є предметом їх діяльності. В поточних умовах на перебіг перелічених етапів має вплив як мінімум оцифрування, що передбачає переведення інформації на друкованих носіях в їх електронний варіант. Більш «просунуті» варіанти полягають у широкому застосуванні цифрових технологій, тобто йдеться уже про цифровізацію зі створенням автоматичних систем ІЗ. Такий поступ створює чимало переваг, зокрема через здатність опрацьовувати більші обсяги інформації та на вищому якісному рівні задовольняти інформаційні потреби кожного адресанта, але й характеризується вищою ймовірністю реалізації інформаційних атак, що проявляється у спотворенні вхідної інформації. Змістовий аналіз розрізнених повідомлень можливий у поєднанні зусиль людини та відповідних цифрових технологій, зокрема штучного інтелекту, що є дорогим варіантом і малодоступним для більшості підприємницьких структур.

Аналогічно до раніше проведеного узагальнення стосовно змістового наповнення терміна «інформація», нами такі ж дії зроблені і щодо ІЗ з метою послідовного вибудовування теоретичних засад його формування для цілей розвитку СЕБП (рис. 2.20).

В цілому усі характеристики визначені, хоча окремо не наголошено на більш активному ІЗ як певній кровоносній системі у живих істот, коли у формі крові, яка забезпечує поширення необхідних для існування організму мікроелементів, виступає інформація. Такі міркування нами реалізовані через окреслення місця ІЗ у діяльності кожного підприємства (рис. 2.21).

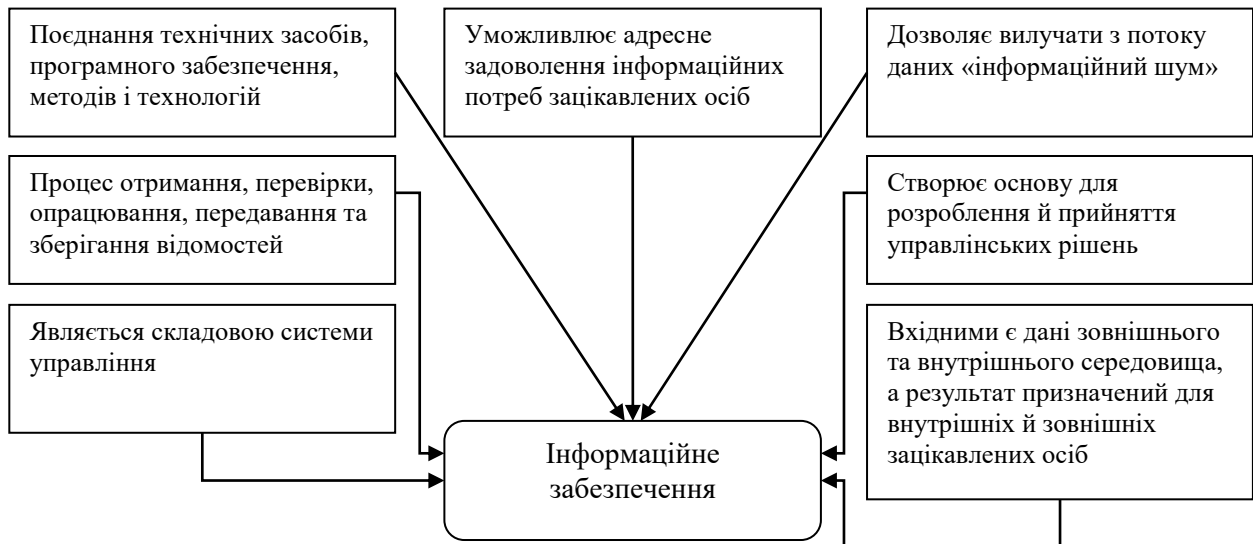


Рис. 2.20. Сучасне трактування терміна ІЗ, що актуальне для безпекової діяльності, сформовано автором



Рис. 2.21. Місце ІЗ у діяльності підприємства, сформовано автором

Підкреслений зв'язок між розвитком СЕБП, який в цьому випадку визначений у ракурсі покращення ІЗ, загалом відповідає авторській позиції, обґрунтованій у першому розділі. Водночас вказується, що таке покращення

провокується й ЦТ на рівні підприємства та загалом національної економіки. Дотримання засад системності актуалізує необхідність розгляду саме системи ІЗ, що функціонально пов'язана із системами вищого порядку, тобто ЕБП та ІЗ управління підприємством.

Система ІЗ, як окремий об'єкт пізнання, розглядається доволі обмеженим колом дослідників. Переважна ж кількість учених спирається у своїх міркуваннях на позицію, що інформація є обов'язковою складовою процесу управління, а відтак окремо розглядати систему ІЗ недоцільно. Поступ у розвитку інформаційного суспільства та цифрової трансформації економіки вносить корективи, які підсилюються тим значенням, яке отримує інформація як ресурс та окремий продукт, що здатний задовольняти потреби. Відтак питання формування й розвитку системи ІЗ набуває актуальності.

Функціональність системи ІЗ визначається її структурою. Обмежена позиція передбачає розгляд лише техніко-технологічної складової, коли розширена характеризується відмінністю поглядів дослідників. Так, С. Петренко виділяє «...інформаційну систему, інформаційний фонд та інформаційну діяльність» [111, с. 11]. Зважаючи на те, що складно погодитися із першою з виділених складових, варто розглянути структуризацію М. Денисенко, в якій виділені «...інформаційні ресурси, інформаційні технології та технічні засоби й програмне забезпечення» [32, с. 44]. Така структура вирізняється чіткістю, але дискусійним можна вважати визначення складовою системи інформаційних ресурсів, які більше повинні знаходитися на її вході, а операції стосовно них за рахунок умінь й навичок працівників, технічних засобів й програмного забезпечення мають сприяти задоволенню інформаційних запитів. Цінним доповненням до наявних уявлень про структуризацію системи ІЗ можуть слугувати аспекти, що виділив К. Линьов [85, с. 15], тобто організація (приналежність до системи вищого порядку через використання єдиної ресурсної бази та виконання завдань в її межах), управління (обов'язковий інструмент у процесі управління підприємством) та технологія (сформовані та постійно удосконалювані процедури роботи з

інформацією). На нашу думку, як стосовно системи ІЗ управління підприємством, підсистема СЕБП, повинна містити такі складові: технічні засоби й програмне забезпечення, технології (перелік внутрішніх інструкцій, норм, положень, вказівок, рекомендацій, що визначають порядок збору, отримання, реєстрації, перевірки та опрацювання інформаційних повідомлень із подальшим скеруванням аналітичних довідок певному адресанту) та кадри, що володіють необхідними компетенціями, коли організація та управління реалізуються відповідно до засад співіснування систем різного порядку.

Інший ракурс структуризації – ієрархічної – розглядає О. Орлик, виділяючи такі підсистеми рівнів управління як «...оперативний, функціональний та стратегічний» [107, с. 190], що, безперечно, є цікавим, з огляду на змістовне наповнення інформації, яка в подальшому застосовується для прийняття відповідних управлінських рішень. Водночас більш цінним є підхід науковців, які в розвідках порушують безпекову проблематику. Так, С. Шинкар [169] концентрує увагу на обліково-аналітичному забезпеченні управління ЕБП, виділяючи підсистеми обліку, аналізу і аудиту, що дозволяє відстежувати зміни у внутрішніх процесах, які відображаються в облікових документах. С. Мельник [97, с. 190] акцентує увагу на інформаційно-аналітичному забезпеченні в контексті управління фінансовою безпекою підприємства, що розширило сферу моніторингу і на зрушення у зовнішньому середовищі. О. Поліщук [118] приділила належну увагу питанню формування інформаційно-аналітичного забезпечення управління ЕБП, але її варіант передбачає відмінну ієрархію, коли інформаційно-аналітичне забезпечення охоплює обліково-аналітичне забезпечення, складовою якого є ІЗ. Наша позиція, ґрунтуючись на уточненій вище суті ІЗ, дещо відрізняється і представлена у графічному вигляді на рис. 2.22.

Авторська позиція може бути застосована на усіх рівнях, тобто як щодо управління підприємством, так й забезпечення ЕБП. Також такі акценти окреслюють параметри ІЗ розвитку СЕБП, оскільки передбачають узагальнення

інформації із внутрішніх та зовнішніх джерел як основу реалізації відповідних заходів.

Встановлений зв'язок слугує основою твердження, що формування інформаційної системи для цілей розвитку СЕБП не потребує «вибудовування з фундаменту» або радикальних змін у межах існуючої системи, а лише коригування базових засад реалізації та уточнення методичних параметрів.

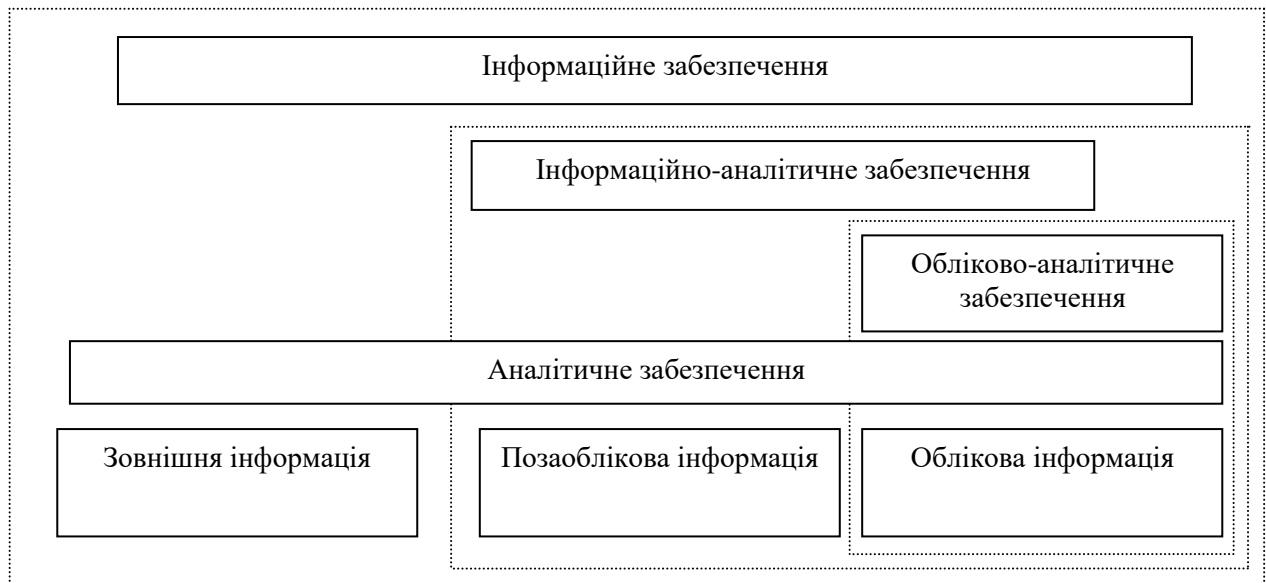


Рис. 2.22. Ієрархічне структурування ІЗ СЕБП, сформовано автором

Авторську позицію обґрунтуємо на основі характеристики змін, які потрібно здійснити в межах існуючої системи ІЗ:

- організаційні зміни в системі ІЗ, що полягають у коригуванні каналів надходження й опрацювання інформації з внутрішніх й зовнішніх джерел з подальшою переадресацією аналітичних звітів до суб'єктів, які відповідають за стан і розвиток СЕБП;

- технологічні зрушення, які потребують перегляду методів обробки інформації, змін у фільтрах для відсікання «інформаційного шуму», уточнення порогових значень та вагових коефіцієнтів для індикаторів оцінювання рівня розвитку СЕБП;

– технічне оновлення засобів отримання й опрацювання інформації, з огляду на посилення інформаційного потоку та необхідність застосування новіших версій програмного забезпечення;

– кадрове підсилення, що в умовах більшості підприємств, значна частка яких в умовах національної економіки належить до типу «малих», полягає в покращенні цифрових і професійних компетенцій працівників та додатковому залученні зовнішніх експертів;

– економічна підтримка, яка повинна формуватися не за «залишковим» принципом, а спираючись на обсяги фактично проведених робіт і подальшу спроможність системи ІЗ сприяти досягненню цілей розвитку СЕБП.

Окреслені зміни мають оперативний характер, але їх реалізація неможлива без попереднього переосмислення методичних засад, тобто уточнення мети, завдань, функцій, принципів тощо, що нами буде здійснено в подальшому.

Зважаючи на цільове спрямування, мету такої системи ІЗ потрібно визначити як встановлення підстав, які виникають у зв'язку із цифровою трансформацією економіки й підприємства та результатами безпекової діяльності, для розвитку СЕБП. Досягнення цієї мети полягає у виконанні таких пов'язаних завдань:

– визначення джерел інформації, що дозволяє отримувати й перекресно перевіряти повну та своєчасну інформацію;

– збір, отримання, узагальнення та накопичення первинної інформації щодо змін у середовищі функціонування, перебігу внутрішніх процесів та активності суб'єктів безпеки стосовно певного підприємства;

– перевірка якості первинної інформації, зокрема на достовірність, шляхом виконання запитів із інших джерел;

– установлення критеріїв правильності інтерпретації інформаційних повідомлень;

– аналізування й формування аналітичних довідок відповідно до інформаційних запитів адресантів і в зручній для них формі;

– формування інформаційних фондів для подальшого здійснення тенденційного аналізу.

Визначений перелік завдань є максимально широкий і слугує не лише досягненню визначеної вище мети, але загалом розвитку ІЗ у СЕБП, зокрема в частині застосування кількох незалежних джерел інформації, ретельної перевірки інформаційних повідомлень, їх опрацювання та надання аналітичних довідок відповідно до запитів адресантів.

Основні функції досліджуваної системи нами визначені як:

– описова, тобто задоволення інформаційних потреб адресантів задля формування у них чіткого цілісного уявлення про зміни в національній економіці, зокрема через її ЦТ, перебіг цифровізації підприємства та результативності дій суб'єктів безпеки, що є основою для розвитку СЕБП;

– аналітична – створення аналітичних довідок (записок), що містять достатній перелік якісних і кількісних показників, значення яких характеризує зміни, що потребують уваги для своєчасної реакції, а відтак більш ефективного використання ресурсної основи в питаннях забезпечення безпеки, зокрема шляхом розвитку СЕБП;

– прогностична – створення інформаційних фондів для відстеження тенденцій в зміні параметрів середовища функціонування, підприємства та безпекової діяльності зі створенням прогнозів як основи для розроблення програми розвитку СЕБП.

Цей перелік відрізняється від функцій СЕБП, оскільки стосується лише його складової – системи ІЗ із орієнтацією на вирішення важливих питань внесення змін у безпекову діяльність. Такі засади нами були застосовані і стосовно уточнення переліку основних принципів:

- об'єктивності, що вбачається у формуванні результатів, які реально відображають стан і характер змін стосовно основних об'єктів спостереження;

- узгодженості, тобто робота з різними джерелами інформації з метою перевірки даних і створення цілісного уявлення про певні явища і процеси, що впливають на безпеку підприємства;

- своєчасності, що виконується на основі автоматизації основних процесів роботи з інформацією й підвищення кваліфікаційного рівня залучених працівників з метою надання адресантам актуальних на певний момент часу даних, необхідних для прийняття управлінських рішень, зокрема стосовно розвитку СЕБП;

- раціональності – робота з тим обсягом інформації, який забезпечує необхідну основу для розроблення управлінського рішення, уникаючи надмірних витрат на отримання й опрацювання кожної наступної одиниці інформації за нездатності її вплинути на кінцевий результат.

Розглянуті принципи мають чітке цільове призначення, тобто стосуються процесів функціонування системи ІЗ і сприяють виконанню завдань щодо розвитку СЕБП.

У межах будь-якої системи обов'язковими складовими є об'єкти та суб'єкти. Стосовно першого елемента, то йому була приділена належна увага під час уточнення інформаційної бази, яка необхідна суб'єктам безпеки в питаннях вирішення проблеми розвитку СЕБП. Інший елемент – суб'єкти – є складнішим, що визначається хоча б тим, що поточні умови функціонування українських підприємств вимагають залучення усіх працівників до процесів роботи з інформацією. Г. Азаренкова та А. Майборода в питаннях створення ІЗ управління фінансовою безпекою підприємства розглядають класифікацію суб'єктів, що певною мірою дотичні до функціонування такої системи, за трьома класифікаційними ознаками, тобто залежно від «...етапу формування інформації; роботи в структурному підрозділі; рівня доступу до інформації підприємства» [2, с. 213]. Отримані результати є цікавими, але позбавляють системи розуміння цілісності, чіткої структуризації та надійності в систематичному виконанні наперед встановлених завдань. Варіативність є доречною, коли вона слугує доповненню основного інформаційного масиву. Відтак нами надається перевага формуванню жорсткої організаційної структури ІЗ, коли залучаються усі профільні підрозділи, тобто бухгалтерія, маркетинговий та аналітичний відділи, відділ кадрів, підрозділ

внутрішньогосподарського контролю тощо. Наперед доповнені посадові обов'язки окремих співробітників кожного профільного підрозділу дають змогу отримувати необхідну первинну інформацію, яку в подальшому узагальнюють й опрацьовують працівники служби безпеки, формуючи аналітичні довідки для адресантів.

Розглянуті вище методичні засади організації та функціонування системи ІЗ нами узагальнені і представлені у вигляді моделі на рис. 2.23.

Додаткового пояснення вимагають лише окремі моменти, зокрема те, що наша увага концентрується лише на одній із складових ІЗ, тобто тій, що відповідає за інформаційний супровід розвитку СЕБП. Практичною реалізацією такої підсистеми можна вважати представлені у підрозділі 2.1 результати аналізу процесів ЦТ економіки й підприємств ВПГ, а також у підрозділі 2.2 – приклад апробації розробленого теоретико-методичного підходу до оцінювання розвитку СЕБП в умовах видавничих структур та поліграфічних підприємств. Таке звуження дало змогу ретельніше розглядати питання характеристики кожного елементу та наочно продемонструвати важливість застосування не загальних засад організації ІЗ, а вибудовування, спираючись на цільове призначення.

У межах механізму роботи з інформацією повинні виконуватися усі поставлені завдання на основі вхідних інформаційних потоків та задіяння складових системи. Додатково виділено ті моменти, що пов'язані із ЦТЕ, що, на відміну від факторів короткочасної дії, тобто пандемії та військових дій, потребують постійної уваги для здобуття й збереження конкурентних позицій кожного підприємства, а також ЦТП, та тенденціями в розвитку СЕБП. Додатково не вказувалися процедури роботи з інформацією, оскільки вони можуть регламентуватися різними протоколами, відповідно до джерел походження та потреб адресантів. Загалом же йдеться про отримання, перевірку, доповнення, опрацювання, надсилання й збереження.

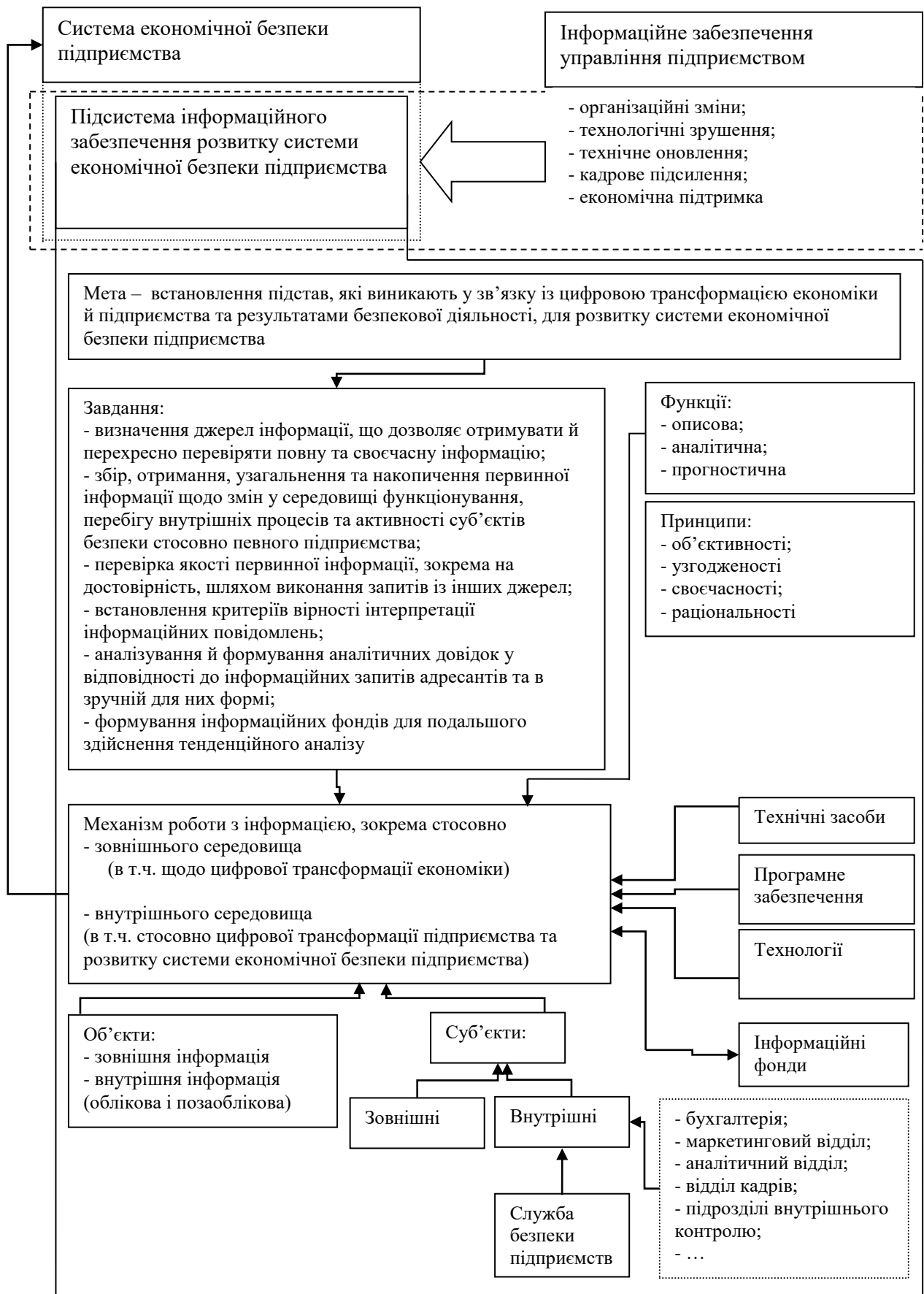


Рис. 2.23. Модель підсистеми ІЗ розвитку СЕБП, сформовано автором

Розроблена модель логічно об'єднує раніше отримані результати та слугує необхідною основою для роботи над теоретичними засадами розвитку СЕБП.

ВИСНОВОК ДО РОЗДІЛУ 2

1. Для об'єктивної оцінки тенденцій в ЦТ національної економіки узагальнено та ретельно проаналізовано аналітичні матеріали, які складаються із міжнародних рейтингів та офіційних статистичних даних щодо активності використання цифрових технологій в Україні. Відповідно до результатів рейтингування позицію України до 2022 р. було охарактеризовано як незадовільну внаслідок пасивності у цифровізації національної економіки через неготовність суспільства і бізнесу до створення й застосування цифрових технологій. Інші країни у цьому є більш активними, тобто їх поступ суттєвіший, що збільшує технологічний розрив.

2. З'ясовано основні аспекти діяльності підприємств ВПП, продукція яких значною мірою пов'язана із задоволенням інформаційних потреб населення, а також характеризується трансформацією, тобто йдеться про дедалі частіше представлення в цифровому варіанті, що замінює традиційний вигляд надрукованих на папері книг, брошур, газет і журналів. Виявлено, що упродовж останніх тридцяти років, за результатами здійснення приватизаційного процесу, видозмінення характеру видавничої та невидавничої продукції та можливості якісного задоволення потреб споживачів, основними суб'єктами стали малі підприємства, які мають низку конкурентних переваг, але не є достатньо ефективним інструментом у забезпеченні інформаційної безпеки з боку держави. Встановлено, що здійснено оцінювання основних показників діяльності поліграфічних підприємств та видавничих структур, динаміка яких вказує на поглиблення кризи у видавничій сфері, що проявляється у зменшенні кількості учасників, ринку, втраті кадрового потенціалу, зростанні збитків, як результату діяльності, коли поліграфічна діяльність дедалі більше переорієнтовується на задоволення потреб переробної галузі в етикетній та пакувальній продукції.

3. Обґрунтовано, що відомі сьогодні підходи до оцінювання ЕБП дозволяють охарактеризувати безпекову діяльність в умовах певного підприємства в минулому та поточному періоді, але обмежені в характеристиці розвитку СЕБП. Відмінність авторського підходу до оцінювання СЕБП полягає в тому, що акцент ставиться не на констатації факту існування СЕБП з деталізацією її організаційної структури та матеріального забезпечення й результатах активності суб'єктів безпеки, а на її розвитку, тобто здійсненні кількісно-якісних змін, що дозволяють посилити захист підприємства відповідно до динаміки зовнішнього середовища та перемін внутрішніх процесів. Проведена апробація розробленого теоретико-методичного підходу в умовах п'яти підприємств ВПГ засвідчила неоднозначність у розвитку їх СЕБП, коли існуючі засади здійснення безпекової діяльності не забезпечили адекватність і своєчасність реакції на виникнення нових загроз та можливостей в складних умовах пандемії та військових дій.

4. Доведено, що розвиток СЕБП визначається ІЗ, яке, згідно з системним підходом, повинно бути організованим у вигляді окремої підсистеми, яка має уможливлювати відстеження зміни у зовнішньому середовищі й внутрішніх процесах та стосуватися бачення тенденцій в ЦТЕ та перспектив ЦТП. Здійснено ієрархічне структурування ІЗ СЕБП, яке уточнює зв'язок між такими термінами як «зовнішня інформація», «позаоблікова інформація», «облікова інформація», «аналітичне забезпечення», «обліково-аналітичне забезпечення», «інформаційно-аналітичне забезпечення», що послугувало необхідною основою для розгляду змін, які потрібно здійснити в межах існуючої системи ІЗ, та розроблення методичних засад, які включають мету, завдання, функції, принципи, об'єкти, суб'єкти, забезпечення, що у сукупності формує основу дієвості підсистеми ІЗ розвитку СЕБП.

Основні наукові результати опубліковані в працях: [177; 183; 187; 189]

РОЗДІЛ 3

УДОСКОНАЛЕННЯ МЕТОДИЧНИХ ЗАСАД РОЗВИТКУ СИСТЕМИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

3.1. Механізм управління розвитком системи економічної безпеки підприємства в умовах цифрової трансформації економіки

ЦТЕ, яка спрямована на збільшення частки цифрової економіки, у поєднанні із змінами, що були спричинені пандемією COVID-19 та широкомасштабними військовими діями, спровокували максимальну нестабільність у функціонуванні усіх українських підприємств. Підтримання життєздатності такої СЕС як підприємство за таких умов неможливо без розвитку СЕБП як фундаменту його існування й розвитку. Зміни зовнішнього й внутрішнього середовища спричиняють зниження ефективності використання існуючих інструментів стосовно протидії дестабілізуючим факторам, тим самим стимулюючи удосконалення методичних засад забезпечення ЕБП, підґрунтям чого повинен стати механізм управління розвитком СЕБП. Ця теза спирається на закладені ще у підрозділі 1.1 міркування щодо змісту розвитку СЕБП як контрольованого і економічно обґрунтованого здійснення кількісно-якісних змін, які повинні бути реалізовані через попереднє створення й застосування відповідного механізму, адже йдеться про постійний процес. Якщо COVID-19 та військові дії актуальні в межах обмеженого часу, то ЦТЕ, з огляду на зміни в межах третьої й четвертої ПР та орієнтацію усіх економічно розвинутих країн на збільшення частки цифрової економіки задля збереження й покращення конкурентних позицій у світовому економічному просторі, має ознаки процесу, який впливатиме найсуттєвіше на діяльність суб'єктів господарювання і в довгостроковій перспективі. Відповідно до зазначеного, в межах цього підрозділу, спираючись на розуміння базових засад існування підприємства як системи, що визначаються її стійкістю, стабільністю,

здатністю досягати й підтримувати рівновагу в умовах посилення флуктуацій, наближення до точки біфуркації, що потребує вибору прийнятної атрактору через урахування актуальних домінантів ЦТЕ, будуть розглянуті теоретичні засади створення й застосування механізму управління розвитком СЕБП.

В основі встановлення сутності, визначення мети й окреслення цілей ЕБП нами акцентувалося на важливості забезпечення стабільності й досягненні стійкості у функціонуванні підприємства попри зміну впливу дестабілізуючих факторів. Відтак розроблення методичних засад формування й застосування механізму управління розвитком СЕБП повинно відштовхуватися від конкретизації суті понять «стійкість» і «стабільність». У підрозділі 1.1 нами вказувалося, що єдиний іноземний термін «stability» в українській науковій літературі має два відокремлені значення, тобто стійкість і стабільність, відмінність між якими доволі чітко проявляється саме в безпекознавстві.

Важливо підкреслити, що поняття «стійкість» є міждисциплінарним, а його застосуванню в економіці передувало окреслення суті у філософії, медицині, біології, математиці та механіці. Для прикладу, у філософії розглядається стійкість як форма, яка уможливорює існування певних об'єктів пізнання, коли нестійкі – руйнуються через внутрішні протиріччя і нездатність взаємодіяти із зовнішнім середовищем. Передумовами виявлення інтересу економістів до проблематики досягнення й підтримання стійкості стали напрацювання математиків, зокрема: О. Ляпунова (розглядав стійкість рівноваги певної системи), В. Попова (досліджував параметри абсолютної стійкості), А. Михайлова (визначив критерії досягнення стійкості замкненої системи) та інших. Перенесення теоретичних напрацювань у практичну площину дослідження економічних явищ і процесів відбулося у 1973 р., коли під час енергетичної кризи виникла потреба у встановленні параметрів підтримання стійкості національної економіки за певного рівня залежності від ситуації на світових ресурсних ринках й обмеженості природних ресурсів. Лише порівняно недавно проблематика забезпечення стійкості почала

розглядатися стосовно мікрорівня, при цьому в подальшому спираючись на напрацювання науковців в інших галузях науки.

Для чіткості сприйняття сучасного розуміння поняття «стійкість» стосовно діяльності підприємств доцільно звернути увагу на його тлумачення у довідниковій літературі. У довідниковій літературі стійкість визначається як «...здатність вистояти супроти чогось, встояти, успішно протистояти силі, витримати, не поступатися» [51, с. 115], тобто йдеться про здатність зберегти цілісність певної системи попри наростання впливу зовнішнього середовища. У першому розділі дисертаційної роботи нами наголошувалося, що дії суб'єктів безпеки повинні бути орієнтовані не лише на зміни зовнішнього середовища, але й на підконтрольність внутрішніх процесів, що певним чином видозмінює процес підтримання стійкості стосовно підприємства з позиції безпекознавства. Цікаві аспекти простежуються і у визначенні, що подається у тлумачному словнику української мови, де стійкість представлена як «...здатність зберігати, існувати в несприятливих умовах;...для нього характерні стабільність, постійність» [104, с. 704]. У цьому варіанті наголошується як на тому, що стійкість уможливорює продовження існування і в несприятливому середовищі, так і встановлюється зв'язок із терміном «стабільність». Загалом, можна стверджувати, що міждисциплінарність стійкості, яка доповнюється ще й рівнями визначення в економічному середовищі (підприємство, галузь, регіон, національна економіка), формує широке й багатоаспектне поле для подальшого поглиблення теоретичних засад забезпечення ЕБП.

Проведене узагальнення дало змогу виявити, що міждисциплінарність відображена у певних відмінностях сприйняття стійкості економістами. Нами конкретизовано суть чотирьох основних підходів у трактуванні цього поняття, які коротко розглянуті нижче із уточненням зв'язку з іншими галузями науки та з'ясуванням параметрів безпекової діяльності. В межах першого підходу дослідники відштовхуються від того розуміння, яке міститься у довідниковій літературі, тобто стосовно здатності зберегти цілісність попри зміну впливу зовнішнього середовища. Економісти певним чином уточнюють таке загальне

уявлення про стійкість системи, спираючись на природу існування підприємства. Так, В. Іванов доводить необхідність розуміти під стійкістю «...здатність економічної системи не відхилятися від свого стану (статистичного або динамічного) при різних внутрішніх і зовнішніх дестабілізуючих впливах на рахунок ефективного формування, використання фінансових та інших механізмів» [59, с. 26]. Попри наявність спільних ознак у розумінні стійкості через збереження поточного стану певної системи, відмінність поглядів економістів полягає у необхідності створення відповідних механізмів, які й уможливають підтримання стійкості системи. Ці ж моменти є підґрунтям для твердження, що стійкість підприємства потребує розроблення й застосування механізмів, які б не лише уможливлювали відстеження зміни внутрішнього й зовнішнього середовища, але й забезпечували перехід до нового стійкого стану, який характеризується кращими показниками діяльності. Тобто з позиції змін, які провокуються ЦТЕ, суб'єкти безпеки повинні забезпечити перехід до нового стійкого стану через недопущення виникнення й впливу дестабілізуючих факторів, які виникають у процесі ЦТП, що неможливо без розвитку самої СЕБП.

Представники другого підходу у своїх міркуваннях здійснюють як ототожнення стійкості із рівновагою, так і обґрунтовують зв'язок між цими термінами. Для прикладу, О. Колодізев та К. Нужний розуміють під стійкістю «...стан рівноваги або здатність повертатися в цей стан відкритої СЕС, після того як відбулося виведення з цього стану зовнішніми і внутрішніми впливами за рахунок ефективного використання всіх видів ресурсів з подальшою здатністю забезпечувати оптимальний процес їх поповнення» [73, с. 240]. На нашу думку, дискусійною є необхідність ототожнення стійкості й рівноваги, але безперечним є їх зв'язок. Стійкістю визначається здатність підтримувати максимально довго рівновагу системи, або ж повертати її до рівноважного стану після певного збурення. Своєю чергою, рівновага характеризує стійкість системи, її здатність протистояти змінам максимально довго. Водночас рівновага стримує розвиток, який спирається на необхідність здійснення змін.

Відповідно до цього, суб'єкти безпеки повинні реалізовувати заходи для забезпечення стійкості підприємства із можливістю розвитку за рахунок підтримання динамічної рівноваги, тобто такої, що уможлиблює відхилення задля реалізації трансформаційних процесів підприємства, зокрема у відповідь на ЦТЕ.

Доволі значна кількість науковців у трактуванні стійкості підприємства концентрують увагу на забезпеченні її ключової складової, тобто фінансової стійкості. Така позиція доволі чітко прослідковується у визначенні, що міститься у публікації Д. Ковальова й Т. Сухорукової, в якій вони подають стійкість як «...фінансовий стан..., господарська діяльність якого забезпечує в нормальних умовах виконання всіх його зобов'язань перед працівниками, іншими організаціями, державою завдяки достатнім доходам і відповідності доходів і витрат» [68, с. 48]. Загалом погоджуючись із ключовою роллю фінансової складової у структурі ЕБП, все-таки вважаємо, що акцент суто на фінансових показниках обмежує дієвість суб'єктів безпеки, зокрема в частині розпізнавання усіх дестабілізуючих факторів, а відтак і відстеження зміни стану системи загалом. Висока плинність кадрів, зокрема висококваліфікованих, набуде відображення у зміні фінансових показників лише за результатами формування квартальної або ж й річної звітності, коли буде порушена стійкість системи через втрату ключового в умовах цифрової економіки ресурсу – людського. Несвоєчасність реалізації захисних заходів суб'єктами безпеки знижує не лише кадрову стійкість, а й фінансову та стосовно інших складових ЕБП.

Окремо нами виділено підхід, прихильники якого фактично не розрізняють стійкість й стабільність. Зазначене прослідковується у міркуваннях Р. Єремейчука, який розглядає стійкість підприємства як «...таку організацію його виробничо-господарської діяльності, яка дає можливість забезпечити стабільні техніко-економічні показники з позитивною динамікою й ефективно адаптуватися до збурення навколишнього і внутрішнього середовища» [45, с. 58]. На нашу думку, стійкість створює необхідне підґрунтя для стабільного

функціонування підприємства із доволі високою ймовірністю досягнення попередньо визначених цілей. Стійкість залежить від контрольованості внутрішніх процесів та здатності адекватно реагувати на зміну зовнішнього середовища, що ще раз засвідчує важливість формування й розвитку СЕБП.

Узагальнюючи, можна стверджувати, що в межах розглянутих підходів чітко прослідковується діалектичний взаємозв'язок між стійкістю, стабільністю й рівновагою. Заслуговує на увагу і те, що стійкість системи найперше визначається її внутрішньою структурою, яка повинна бути гнучкою, тобто здатною удосконалюватися відповідно до впливу дестабілізуючих факторів, джерелом виникнення яких є: зміни в національній економіці, зокрема і щодо зростання частки цифрової економіки; рівень агресивності зовнішнього середовища підприємства; рівень менеджменту. Підтримання стійкості вимагає не лише формування СЕБП, а й її розвитку для постійного осучаснення теоретико-методичного базису безпекової діяльності.

Відповідно до підкресленої вище синтаксичної й змістової спорідненості понять «стійкість» і «стабільність», приділимо увагу й другому із названих для обґрунтування методичних засад розвитку СЕБП. Ретельне узагальнення наукових напрацювань щодо суті стійкості засвідчило, що його сучасне трактування економістами частково визначено у природничих науках, де під ним розуміють максимально тривале існування певного організму попри зміну навколишнього природнього середовища. Загалом таке сприйняття стабільності можна визначити як статичне, коли в економіці перевагу надають діям щодо забезпечення прийнятних умов функціонування й розвитку, тобто динамічному змісту цього поняття. Іншим визначальним моментом є те, що стабільність в економіці розглядається стосовно макрорівня, зокрема через оцінювання параметрів національної економіки, виробництва й споживання продуктів харчування, доходів і витрат домогосподарств тощо. Стосовно мікрорівня відзначається низька інтенсивність наукових розвідок із недостатньою чіткістю розгляду суті стабільності в діяльності певного підприємства. Нами умовно виокремлено основні три підходи у трактуванні стабільності, які слугують

додатковими аргументами на користь необхідності формування механізму розвитку СЕБП.

У межах першого підходу йдеться про розгляд стабільності у взаємозв'язку із стійкістю. Т. Поперляк доводить, що «...економічна стабільність є ширшим, бо це стан, коли економічна система функціонує в стані рівноваги, зберігаючи незмінною свою структуру, коли економічна стійкість – здатність зберігати показники на певному рівні, незважаючи на постійний вплив зовнішнього та внутрішнього середовища» [113, с. 27–29]. На нашу думку, дискусійним є визначене співвідношення між стабільністю й стійкістю, як і неврахування необхідності формування безпечних умов, які б дозволяли максимально довго досягати поставлених цілей. Зважаючи на високий динамізм у зміні середовища функціонування підприємств, зокрема в ракурсі ЦТЕ, прихильність статичного трактування стабільності містить додаткові ризики поглиблення технологічного відставання, що вчергове доводить необхідність розвитку СЕБП як основи контрольованої ЦТП, тобто в межах допустимих відхилень для підтримання динамічної стабільності.

Другий підхід передбачає фактичне ототожнення стабільності й рівноваги, що чітко прослідковується у визначенні В. Суміна: «...економічна стабільність (рівновага) – це стан економічної системи, яка має бути збалансованою» [141, с. 160]. Безперечно, стабільність передбачає знаходження й підтримання хоча б короткочасної рівноваги, що можливо завдяки реалізації комплексу заходів для врівноваження впливу різноспрямованих факторів, в чому ключову роль повинні виконувати суб'єкти безпеки завдяки наявності функціонуючої підсистеми ІЗ в складі СЕБП.

Н. Любченко в межах третього підходу доводить, що забезпечення економічної стабільності підприємства вимагає застосування «...економічних, технічних, організаційно-правових та інших заходів за допомогою фінансових, виробничих, інформаційних, технічних, людських тощо ресурсів з врахуванням місії та цілей підприємства» [89, с. 230]. Загалом погоджуючись із таким підходом, вважаємо, що Н. Любченко достатньою мірою не конкретизує

спрямування заходів. На нашу думку, комплексне застосування стабілізаційних заходів може передбачати, за умови несуттєвих впливів дестабілізуючих факторів, відновлення попередньої рівноваги або перехід до нового рівноважного стану, з огляду на необхідність більш радикальних змін, зокрема через ЦТЕ.

Підводячи підсумки цієї частини дослідження, можна стверджувати, що в умовах ЦТЕ пріоритетність отримує не статична стабільність, а динамічна, яка полягає в здійсненні комплексу заходів, які передбачають цілеспрямоване внесення змін у діяльність підприємства задля підтримання життєдіяльності, чому повинен сприяти розвиток СЕБП.

У процесі з'ясування суті й обґрунтування важливості досягнення стійкості й підтримання стабільності підприємства нами неодноразово згадувалося таке поняття як «рівновага», під яким загалом розуміють сталість основних параметрів системи. Ретельне вивчення наукового доробку дало змогу констатувати, що більшість економістів беруть за основу загальноприйняте розуміння цього терміна. Скажімо, рівновага розглядається як «...незмінність деяких показників системи (обсягу постачань, прибутку) з допустимими відхиленнями від їх заданих рівнів» [96, с. 122]. На противагу такому розумінню існують інші погляди, які спираються насамперед на сутність СЕС, ключовими складовими яких виступають люди, що характеризуються динамікою й невизначеністю поведінки. В цьому ракурсі доволі чіткою є позиція В. Веселовського, який доводить, що «...живі системи ніколи не бувають у рівновазі й виконують за рахунок своєї вільної енергії постійну роботу проти рівноваги» [20, с. 25]. Зазначене вказує на існування дилеми, коли система прагне за рахунок стійкості й стабільності встановити стан рівноваги, але людський фактор порушує її. Така протилежність спонукала науковців до розгляду можливих різновидів рівноваги. Якщо «абсолютна» рівновага неможлива стосовно відкритої СЕС, якою є підприємство, то розглядаються такі різновиди як «хитка» або ж «динамічна», які передбачають можливе контрольоване відхилення, зокрема спричинене й дестабілізуючими

факторами. Ідею «динамічної» рівноваги розвиває Т. Шира [171, с. 125] в контексті забезпечення корпоративної безпеки шляхом погашення відхилень через реалізацію компенсаційних заходів за ініціативою суб'єктів безпеки. На нашу думку, завданням суб'єктів безпеки повинно бути не лише відстеження рівня ЕБП, але й прогнозування впливу основних факторів, перелік яких нами був приведений вище (зокрема і спричинених ЦТЕ), що можуть спровокувати виникнення й посилення впливу дестабілізуючих факторів, що призведе до порушення рівноваги поза допустимий рівень. Тобто у нашому розумінні дії суб'єктів безпеки повинні бути зосереджені на підтримці динамічної рівноваги, яка уможливорює контрольований й цілеспрямований розвиток відповідно до зміни середовища функціонування. Встановлення граничних значень стосовно кожного індикатора із прогнозуванням можливих змін під впливом основних факторів потребує розвитку СЕБП хоча б щодо удосконалення ІЗ.

Попри те, що поняття «стійкість», «стабільність» і «рівновага» активно застосовуються безпекознавцями для розвитку теоретико-методологічних засад забезпечення ЕБП, отримані результати в більшості орієнтовані на ліквідацію наслідків негативного впливу дестабілізуючих факторів. З'ясовано, що в процесі забезпечення економічної безпеки на вищому рівні, тобто держави, активно застосовуються такі поняття як «флуктуація», «біфуркація», «атрактор» й «гомеостаз», що сприяє поглибленню розуміння змін, які впливають на рівень безпеки, із розробленням заходів не лише стосовно підтримання рівноважного стану національної економіки, але й створення безпечних умов для розвитку, зокрема шляхом збільшення частки цифрової економіки. Ці моменти підштовхнули до створення теоретичного підґрунтя формування механізму розвитку СЕБП шляхом уточнення змісту вказаних вище понять стосовно діяльності окремого підприємства.

Т. Нікітченко під флуктуаціями розуміє «...збурюючі дії, які сприяють відхиленню функціонування системи від її закономірного стану» [103, с. 59]. Продовжуючи ці міркування, спираючись на розглянуту сутність дестабілізуючих факторів, можна стверджувати, що флуктуації провокують,

внаслідок невідповідності стану системи й характеру змін, виникнення загроз, через вплив яких порушується рівновага із більшим за встановлений прийнятний рівень відхиленням. Ці міркування набувають часткового підтвердження у позиції В. Марченко, який вважає, що в «...ролі флуктуацій можуть виступати зміни кон'юнктури ринку, ціни ресурсу, відсоткових ставок, інноваційного потенціалу галузі, інвестиційних потоків тощо» [93, с. 158]. Вважаємо, що цей перелік доцільно доповнити тими процесами, які виникають внаслідок ЦТЕ. У випадку неготовності до таких флуктуацій виникають загрози для ЕБП, а в умовах своєчасно проведеної трансформації – з'являються додаткові конкурентні переваги. За будь-якого варіанту розвитку подій визначальною є ефективність СЕБП, що безпосередньо залежить від її розвитку.

Флуктуації спричиняють перехід системи в точку біфуркації, яку загалом розуміють як певний «переломний момент». Науковці у своїх міркуваннях доволі одностайні у трактуванні поняття «біфуркація», і окремі уточнення скоріше слугують необхідній деталізації. В. Шкуркіна розглядає зазначений термін як «...момент нестійкості, коли система вибирає подальший шлях еволюції, місце, в якому відбувається катастрофа» [173, с. 230]. Доречним буде пояснення, що авторка під «катастрофою» розуміє радикальні зміни, спричинені зовнішніми флуктуаціями. В інших визначеннях додатково наголошується, що точка біфуркації характеризується: зниженням стійкості, втратою стабільності, появою кількох альтернативних варіантів подальшого розвитку, високим рівнем невизначеності. Попри певну одностайність у розумінні біфуркації, на увагу заслуговує й певним чином відмінна позиція А. Гальчинського [23, с. 63], який вбачає в ній поштовх до інноваційної діяльності, яка забезпечує не лише виживання в умовах зміни зовнішнього середовища, а здобуття необхідних переваг над пасивними конкурентами. На нашу думку, можна погодитися із аргументами А. Гальчинського на користь позитивного результату перебування в точці біфуркації, але не можна залишати поза увагою й інші варіанти розвитку подій, тобто аттрактори, що можуть спровокувати

занепад із подальшим руйнуванням системи. Не менш важливим моментом є те, що перехід до точки біфуркації може бути наслідком не лише посилення флуктуацій, але й спровокований змінами в системі управління, тобто такими, що передбачають як розвиток підприємства, так і втрату контролю й хибні рішення. Зазначені моменти актуалізують необхідність систематичного здійснення суб'єктами безпеки заходів щодо:

- діагностування флуктуацій й наближення до точки біфуркації з метою розроблення й реалізації управлінських рішень для: переходу до бажаного варіанту розвитку й уникнення руйнування системи; подальшого відновлення стійкості й повернення до стабільного функціонування уже у післятрансформаційному періоді;

- відстеження характеру змін у точці біфуркації, тобто чи вони «поступові» (перехід до певного варіанту розвитку відбувається плавно), чи «радикальні» (спровоковані швидкоплинними флуктуаціями із високим рівнем невизначеності), що окреслює характер дій задля збалансування стану системи;

- недопущення виникнення кількох точок біфуркації в межах короткого проміжку часу, що може створити передумову для руйнування системи внаслідок неконтрольованого зниження життєздатності.

Активність суб'єктів безпеки стосовно відстеження флуктуацій й перебування в точці біфуркації слугує аргументом на користь розвитку СЕБП, адже лише у випадку високої надійності такої системи підприємство здатне впливати на подальший перебіг подій в його діяльності.

У точці біфуркації відбувається перехід за одним із атракторів і подальше встановлення тимчасової рівноваги в змінених зовнішніх умовах й коригування внутрішніх процесів. Потрібно визнати факт доволі відмінного трактування терміна «атрактор». Н. Бичкова доводить необхідність розуміти атрактор як «...ідею чи місію бізнес-діяльності, що спрямовує розрізнений колектив в єдину систему; це мета, яку організація ставить на певній стадії свого життєвого циклу» [7, с. 91]. З такою позицією можна погодитися частково, адже лише частина атракторів формується за ініціативи підприємства, інші –

утворюються, спираючись на результати зовнішніх і внутрішніх флуктуацій. О. Хитра розглядає сутність досліджуваного терміна як «...ступінь синтезу порядку та хаосу, який перевершує всі відомі на даному рівні розвитку системи ступені складності» [158, с. 104]. Якщо зважити на те, що система в точці біфуркації опиняється на розгалуженні, то будь-який напрям, тобто атрактор, суттєво відрізняється від попереднього стану, відповідно й набутий раніше досвід є недостатнім, що ще в одному ракурсі підкреслює необхідність розвитку СЕБП для подальшого встановлення динамічної рівноваги. Водночас, спираючись на з'ясовану сутність і параметри забезпечення стійкості й стабільності існування системи, можна стверджувати, що дії суб'єктів безпеки, за рахунок реалізації комплексу заходів, повинні бути спрямовані на підтримання динамічної рівноваги, зокрема й шляхом погашення зовнішніх і внутрішніх флуктуацій. У випадку наближення до точки біфуркації СЕБП повинна забезпечити перехід до бажаного атрактору, тобто такого, що відповідає інтересам підприємства, за умови ініціювання точки біфуркації – завчасне формування необхідного атрактору й контроль за процесом переходу. Останній варіант актуальний з позицій низької активності українських підприємств стосовно ЦТЕ, коли світові тенденції переконливо доводять необхідність пришвидшення змін для отримання конкурентних позицій на зовнішніх ринках і забезпечення лідерства серед вітчизняних товаровиробників.

Підтримання рівноваги в біології розглядається через максимально довге існування живих організмів попри вплив навколишнього середовища й внутрішні зміни та окреслюється таким поняттям як «гомеостаз». Одним із перших дослідників, який загалом охарактеризував існування гомеостазу і не лише в біології, став У. Кеннон. Як послідовник Н. Вінер, він сформував концепцію гомеостазу, а С. Бір обґрунтував його сутність як «...здатність системи підтримувати її критичні параметри у фізіологічно допустимих межах в умовах випадкових перешкод або збурень» [8, с. 52]. Застосування терміна «гомеостаз» доволі швидко поширилося за межі біології, оскільки створювалася необхідна теоретична база розуміння відносної незмінності

певних систем попри динамічність середовища функціонування. В довідниковій літературі гомеостаз подавався як «...модель організму, яка має здатність імітувати можливості підтримувати певні параметри у визначених межах і пристосовуватися до зовнішніх чинників» [51, с. 115]. Попри те, що в основі трактування лежала прив'язка до живого організму, коло об'єктів дослідження постійно розширювалося. Гомеостаз створював необхідне підґрунтя для окреслення границь можливого пристосування, тобто адаптації й повернення до стану рівноваги. Саме ці акценти були поглиблені в кібернетиці завдяки науковим розвідкам У. Ешбі, який першим сформував методологічний базис створення гомеостазу як механізму, що наочно встановлює межі надійності системи, тобто можливість повернення до попереднього стану, після впливу на неї різних зовнішніх факторів. У подальшому не лише в кібернетиці гомеостаз почав розглядатися як механізм саморегуляції, який, використовуючи зворотній зв'язок, уможлиблює підтримку функціонування системи в певних межах упродовж тривалого періоду.

З позиції удосконалення методичного забезпечення розвитку СЕБП цікавими є такі ключові параметри гомеостазу: в межах системи стабілізація ситуації, після зміни однієї складової під впливом зовнішніх та/або внутрішніх факторів, відбувається шляхом посилення взаємодії й формування компенсаційного впливу інших елементів; дієвість механізму саморегулювання визначається допустимими межами змін; кожна складова характеризується певною автономністю функціонування в межах системи, що створює передумови для децентралізації оперативного управління із одночасним посиленням інформаційної взаємодії на тактичному й стратегічному рівнях. Відповідно до зазначеного, формування такого механізму повинно сприяти підтриманню динамічної рівноваги при незначних змінах у середовищі функціонування за рахунок внутрішньої організації, тобто насамперед діяльності суб'єктів безпеки. Водночас гомеостаз уможлиблює внутрішнє удосконалення для підтримання стійкості системи, що повинно бути реалізовано найперше через розвиток СЕБП.

Здійснене узагальнення стосовно сутності таких понять як «стійкість», «стабільність», «рівновага», які активно використовуються безпекознавцями, у поєднанні із «флуктуацією», «біфуркацією», «атрактором» й «гомеостазом», що застосовуються економістами в більшості стосовно макроекономічних процесів, у сукупності дало змогу сформувати необхідне підґрунтя для розроблення механізму розвитку СЕБП через: ретельний розгляд взаємозв'язків між усіма поняттями; моделювання ситуації із різним ступенем зміни умов функціонування підприємства; послідовне доведення необхідності вносити зміни в діяльність суб'єктів безпеки; доведення можливості реагування на тенденції в ЦТЕ виключно за рахунок попереднього формування безпечних умов подальших змін у межах підприємства. Наступний етап повинен передбачати використання отриманих результатів для формування відповідного механізму, що неможливо без розгляду змісту поняття «механізм» та засад його створення й реалізації в межах СЕС та уточнення місця механізму розвитку СЕБП у механізмі забезпечення ЕБП.

Сьогодні механізм виступає обов'язковою складовою практично кожної ґрунтовної наукової публікації із подальшим уточненням змісту. Нами відібрано дві позиції, які доволі чітко відображають спрямування наукових розвідок. М. Дороніна інтерпретує механізм як «...складну систему, яка має параметри «входу» та «виходу», складається з необхідної кількості елементів, які забезпечують «...на виході бажані значення істотних параметрів за мінімальних втрат енергії» [38, с. 128]. Цінною відмінністю такого підходу є не лише сприйняття механізму як складної системи, але й орієнтація на досягнення поставлених завдань, дотримуючись принципу раціональності використання ресурсів. Комплексний варіант розуміння механізм пропонує Л. Фролова, подаючи його як «...сукупність (або систему) формальних і неформальних правил, процедур, методів, способів, форм, важелів, функцій управління економічними відносинами різного рівня» [157, с. 130]. Зміст цього визначення яскраво доводить не шаблонність, а можливість багатоваріантної

побудови механізму, реалізація якого уможлиблює конкретизацію елементів такої системи та процесу взаємодії між ними.

Проведене узагальнення створює необхідне підґрунтя для розгляду механізму забезпечення ЕБП у двох площинах, тобто дотримуючись внутрішньої побудови (складу елементів) та порядку реалізації безпекової діяльності, яка повинна уможливити функціонування й розвиток підприємств в умовах ЦТЕ шляхом розроблення й прийняття суб'єктами безпеки оперативних, тактичних і стратегічних рішень як стосовно об'єктів безпеки, так і суб'єктів зовнішнього середовища.

Поглиблене ознайомлення із напрацюваннями безпекознавців виявило, що ними актуалізується проблематика забезпечення ЕБП, але формування теоретико-методологічного забезпечення перебуває на стадії активного формування, де є ще ряд секторів, що потребують посилення наукових розвідок. Один із таких секторів представлений механізмом забезпечення ЕБП. Лише в окремих публікаціях розглядаються засади формування й реалізації такого механізму. Цікавою є позиція Н. Пойди-Носик, яка пропонує окремо розглядати «механізм управління як спосіб впливу суб'єкта на об'єкт за допомогою різних засобів та механізм забезпечення – сукупність заходів щодо створення надійних умов гарантування захисту від небезпеки» [116, с. 26]. Загалом погоджуючись із необхідністю розрізнення цих базових понять, вважаємо, що механізм забезпечення ЕБП повинен бути орієнтований на виконання мети СЕБП, тобто передбачати забезпечення стабільності функціонування підприємства шляхом адаптації та/або протидії дестабілізуючим факторам. Попри те, спираючись на здійснене уточнення таких базових понять як «стабільність», «стійкість», «рівновага», «флуктуація», «біфуркація, «атрактор» й «гомеостаз», вважаємо, що перелік локальних механізмів повинен бути дещо іншим, зокрема містити:

- механізм гомеостаз;
- механізму взаємодії внутрішніх та зовнішніх суб'єктів безпеки;
- механізму формування і реалізації безпекового потенціалу;

- механізм діагностики;
- механізм ідентифікації дестабілізуючих факторів;
- механізм прогнозування;
- механізм прийняття рішення;
- механізм управління розвитком СЕБП.

Наші міркування стосовно переліку локальних механізмів доповнені також структурними елементами та процесом реалізації, що графічно продемонстровано на рис. 3.1.

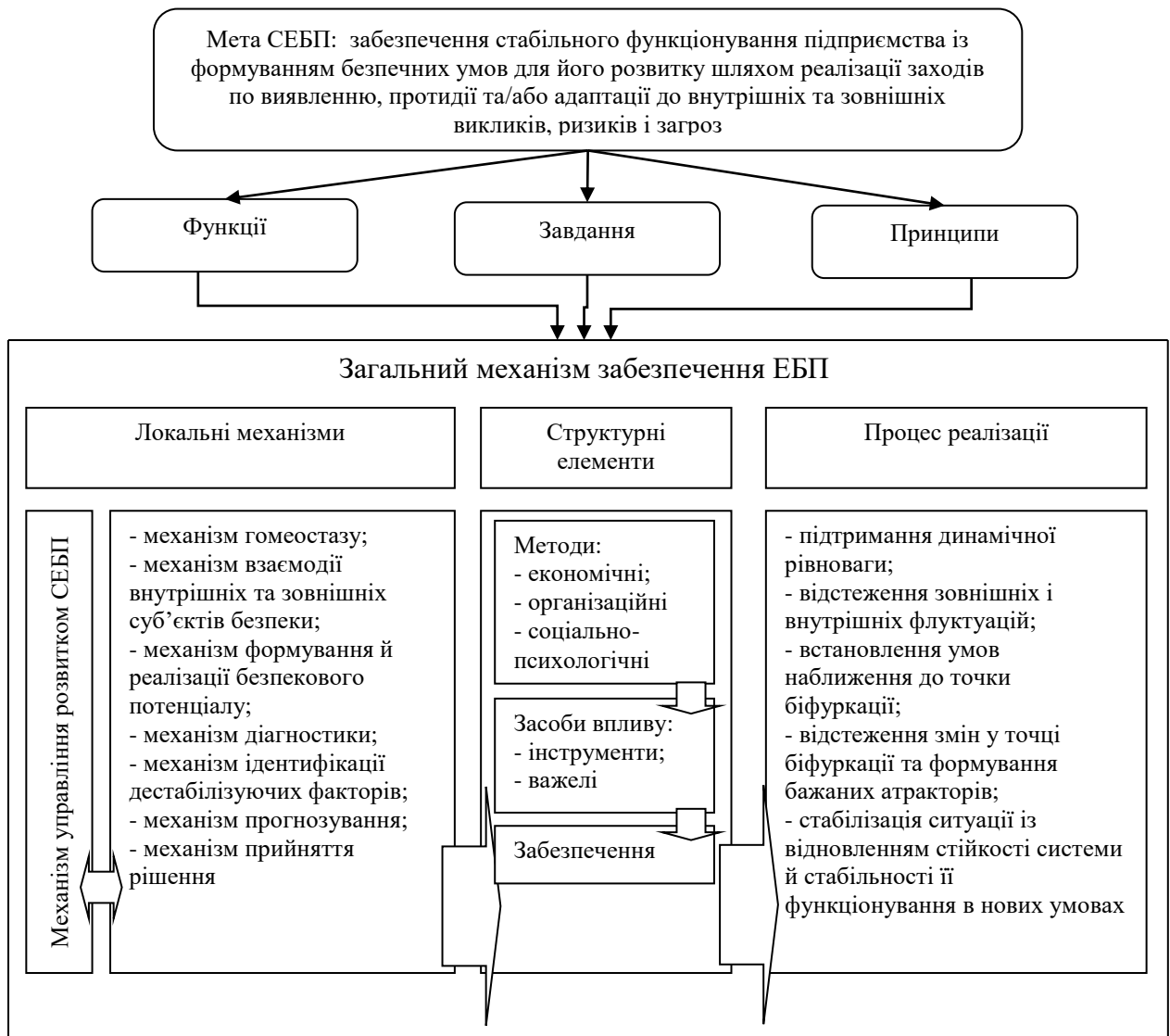


Рис. 3.1. Механізм забезпечення ЕБП, сформовано автором

Проведений огляд доробку безпекознавців засвідчив, що методичні засади формування й застосування механізму управління розвитком СЕБП сьогодні фактично не сформовані. Науковці зосереджують увагу на проблематиці розвитку, розгляді аспектів управління розвитком, розроблення механізму управління розвитком підприємства загалом. Зазначене стало підставою для лаконічного подання результатів доробку за кожним напрямом як підґрунтя для аргументованого подання власних міркувань щодо змісту механізму управління розвитком СЕБП. У цьому контексті за основу можна взяти твердження Ю. Шарова, згідно з яким «...розвиток має бути керованим і здійснюватися через цілеспрямоване управління» [166, с. 35], що засвідчує правильність створення саме механізму управління розвитком СЕБП як такого, реалізація якого повинна уможливити внесення змін у безпекову діяльність підприємства відповідно до тенденцій ЦТЕ та інших змін у середовищі функціонування.

Н. Боднар сформувала концепцію розвитку, яка «...передбачає здійснення змін у структурному та кадровому аспектах: в межах структурного – створюються сприятливі умови для досягнення підприємством поставлених цілей; у межах кадрового – проводяться заходи з підвищення кваліфікації працівників (розвиток персоналу) та їх стимулювання до впровадження інновацій, підвищення творчої активності» [11]. Така позиція актуальна і в умовах ЦТЕ, хоча саме групування аспектів не сприяє необхідній чіткості у розумінні спрямування змін в умовах підприємства, заважаючи хоча б на те, що кадрові трансформації становлять за змістом структурні. Без подальшого ретельного розгляду інших позицій стосовно управління розвитком можна стверджувати, що забезпечення відповідності параметрів функціонування підприємства у високодинамічному середовищі може бути досягнуто виключно за рахунок управління його розвитком, що, своєю чергою, актуалізує питання якості системи управління й СЕБП як такої, що повинна забезпечити безпечні умови для змін. Ця теза набуває підтвердження у висловлюваннях О. Раєвської, яка процес управління розвитком розуміє як «...усунення протиріч, що виникають на двох рівнях – між генетичною схильністю підприємства до

розвитку та стохастичними флуктуаціями зовнішнього або внутрішнього середовища» [128, с. 213–216]. На нашу думку, це твердження максимально чітко підкреслює як важливість СЕБП для уможливлення розвитку підприємства шляхом ліквідації протиріч, які провокують виникнення нових дестабілізуючих факторів, так і те, що такі дії вимагають розвитку самої СЕБП більш швидкими темпами. Зазначене може бути реалізовано через застосування певного механізму, тобто механізму управління. Оминаючи ретельний розгляд основних підходів до трактування суті поняття «механізм управління», зазначимо, що у вузькому ракурсі під ним розуміють систему, яка генерує управлінські рішення для внесення змін у діяльність підприємства, а у широкому – передбачає конкретизацію взаємодії організаційних ланок підприємства з метою отримання позитивних результатів. Зазначене дозволяє перейти до розгляду комплексного поняття «механізм управління розвитком», хоча на цьому етапі ще стосовно усього підприємства. О. Раєвська вважає такий механізм «...найбільш активною частиною системи управління, здатною забезпечити цілеспрямований розвиток підприємства» [128, с. 225], а також виділяючи в його структурі засоби та методи управління. Ми розглядаємо такі висловлювання з позиції підтвердження власних міркувань щодо необхідності посилення взаємодії внутрішніх і зовнішніх суб'єктів безпеки, на чому було акцентовано увагу у першому розділі. Окрім цього, доволі цікавою є блочна структура такого механізму, яка характеризує процес внесення змін на основі отриманих даних щодо динаміки середовища функціонування, що створює передумови актуальності й своєчасності розвитку. Відтак вважаємо, що механізм управління розвитком СЕБП повинен: містити перелік методів та інструментів здійснення керуючого впливу; характеризувати процес через виділення основних етапів; конкретизувати спрямування реалізації управлінських рішень. Зазначені базові засади були покладені в основу авторського варіанту механізму управління розвитком СЕБП (рис. 3.2).

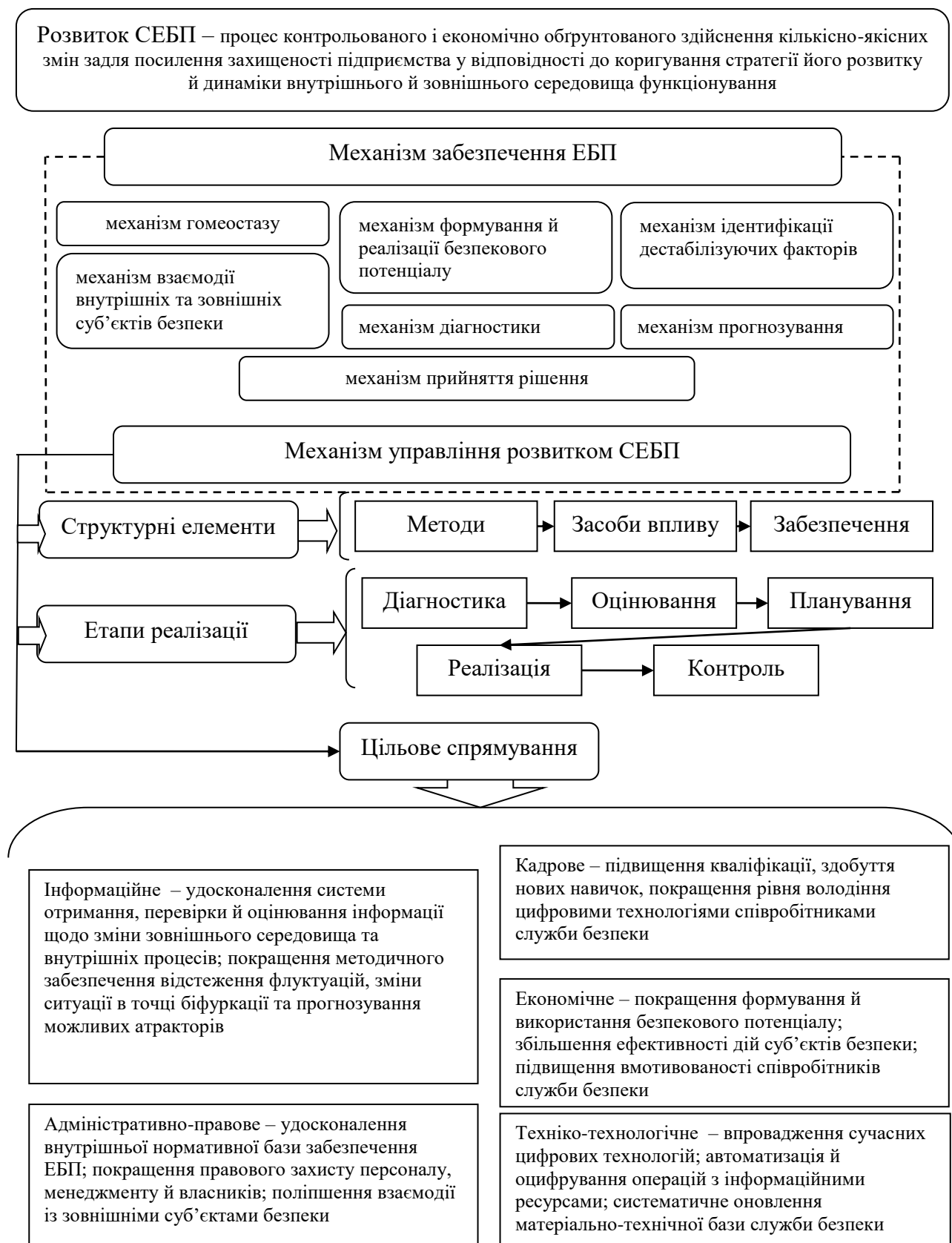


Рис. 3.2. Механізм управління розвитком СЕБП, сформовано автором

Структура розробленого механізму відповідає авторському розумінню розвитку СЕБП, яке було розглянуто у першому розділі дисертаційної роботи. Відмінністю запропонованого варіанту можна вважати комплексність підходу, коли чітко виділені структурні елементи, етапи реалізації та цільове спрямування. Останнє сформовано, зважаючи на зміни, які виникли під час ЦТЕ та покликані удосконалити СЕБП задля уможливлення формування нею безпечних умов розвитку підприємства загалом.

Підводячи підсумки, можна стверджувати, що завдяки узагальненню й послідовному формуванню авторського розуміння таких базових понять як «стійкість», «стабільність», «рівновага», «флуктуація», «біфуркація», «атрактор», «гомеостаз», а також «механізм», «механізм управління» й «механізм управління розвитком» було розроблено механізм управління розвитком СЕБП як складової загального механізму забезпечення ЕБП. Отримані результати стали продовженням сформованих теоретичних засад розвитку СЕБП та будуть використані як підґрунтя для розгляду теоретико-практичних аспектів створення й ефективного використання безпекового потенціалу.

3.2. Методичні засади розвитку системи економічної безпеки підприємства

ЦТЕ через високу інтенсивність і розширення сфер застосування цифрових технологій формує певну надбудову над реальною економікою, яка створює доволі значні переваги за рахунок доступу та можливості більш повного використання інформаційних ресурсів. Разом із новими можливостями виникає й не менша кількість проблем, які першочергово проявляються у потребі здобуття навичок і формування необхідних знань для використання новітніх ІКТ та створення відповідних систем захисту в інформаційному середовищі. Зазначене актуальне як для держави, підприємства, так і окремої особи. Якщо

зупинитися на рівні підприємства, то СЕБП, яка була здатна адекватно реагувати й забезпечувати необхідний рівень захисту в умовах традиційної економіки, потребує видозмінення через розвиток, з огляду на оновлений перелік загроз, зокрема й в інформаційному просторі, незважаючи на ступінь присутності в ньому певного підприємства. Сьогодні фактично жодне підприємство не може залишитися поза інформаційним простором, а відтак разом із використанням нових можливостей завдяки застосуванню цифрових технологій актуалізується й проблема перегляду засад забезпечення безпеки. Хибним є уявлення про такі зміни лише в ракурсі придбання новішого комп'ютерного обладнання й використання програмного забезпечення, що ускладнює несанкціонований доступ до інформаційних ресурсів підприємства. ЦТЕ більшою мірою стосується людини, тобто й як найманого працівника, зокрема й співробітника служби безпеки, що повинен бути здатним повною мірою використовувати досягнення технологічного поступ і в питаннях забезпечення безпеки не лише щодо загроз в інформаційному просторі, а стосовно усіх, що певним чином впливають на діяльність підприємства. Загалом у межах цього підрозділу нами порушується доволі складне завдання, що полягає в уточненні характеру змін у СЕБП під впливом зростаючої інтенсивності використання цифрових технологій, зокрема й щодо постійного покращення цифрових компетентностей співробітників служби безпеки підприємства.

Перш ніж сконцентрувати увагу на розгляді основних засад розвитку СЕБП, вважаємо за необхідне уточнити характер зв'язку між такими поняттями як «цифрова безпека», «інформаційна безпека» і «кібербезпека». Зазначений крок пов'язаний із тим, що, з огляду на зміст ЦТЕ, деякі науковці здійснюють спроби змінити базові параметри безпекознавства, зокрема на мікрорівні, подаючи їх як наступний етап розвитку. Зважаючи, що в подальшому нами будуть обґрунтовані медичні засади розвитку СЕБП, то попередньо важливо критично розглянути інші позиції.

Питання необхідності забезпечення цифрової безпеки порушено в публікації М. Саврук, де вона визначена як «...стан захищеності інформації, яка забезпечує життєво важливі інтереси підприємства та суспільства в цілому» [131, с. 78]. Доволі схожої позиції дотримується й Т. Ткачук визначаючи цифрову безпеку як «...безпеку об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією, та нерозголошення даних про той чи інший об'єкт, що є комерційною таємницею» [143, с. 148]. На нашу думку, таке розуміння цифрової безпеки доволі наближено до існуючого трактування інформаційної безпеки, в межах якої суб'єкти безпеки здійснюють кроки щодо захисту інформаційних ресурсів підприємства та забезпечення інформаційних потреб менеджменту, зокрема задля підтримання стійкості й контрольованої трансформації підприємства. Певним чином відмінної позиції щодо визначення суті терміна «цифрова безпека» дотримується Т. Передерій, вбачаючи в ній «...захищеність функціональних складових підприємства під час здійснення господарської діяльності в умовах цифровізації і конкуренції; заходи і методи, що спрямовані на мінімізацію зовнішніх і внутрішніх ризиків е-бізнесу, а також забезпечення безпеки функціональних складових» [110, с. 202]. Вважаємо, що доволі дискусійним є не лише саме визначення, але й те, що Т. Передерій формує функціональну структуру цифрової безпеки шляхом включення до її змісту таких складових як «фінансова», «інформаційна», «екотехнологічна», «правова» і «кадрово-інтелектуальна». Така функціональна структура вказує на бажання автора практично автоматично підмінити термін ЕБП на новий, тобто «цифрову безпеку», з чим доволі складно погодитися.

Узагальнюючи вважаємо, що розвідки у сфері розвитку безпекознавства шляхом введення в обіг поняття «цифрова економіка» стосовно окремого підприємства є сьогодні недостатньо глибинними. Науковці відгукуються на факт збільшення активності підприємницьких структур в інформаційному просторі на фоні карантинних обмежень та ускладнень, зумовлених військовими діями, але результатом стає дублювання або ж заміна

установлених засад безпекової діяльності без реального вирішення проблеми розвитку, зокрема СЕБП.

Ще один напрям розвитку безпекознавства сьогодні формується через намагання виділити й надати найбільшій важливості забезпеченню кібербезпеки не лише на державному рівні, але й стосовно кожного окремого підприємства. Підґрунтям такого спрямування, на чому буде наголошено в подальшому, стали зміни в складі загроз, де дедалі більшу частку та важливість стосовно необхідності реагування займають атаки на інформаційні ресурси підприємства. Як і стосовно цифрової безпеки, нами буде критично розглянуто сутність поняття «кібербезпека» на предмет можливості її виділення як окремої складової в межах функціональної структури ЕБП. Так, В. Бурячок обґрунтовує необхідність розуміти кібербезпеку як «...стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам» [12, с. 35]. Окрім певного поєднання двох відмінних рівнів, тобто держави та підприємства, дискусійним є те, що йдеться про захист кіберпростору. Сьогодні під терміном «кіберпростір» розуміють певне поєднання засобів і предметів цифрових процесів, які тривають і в діяльності кожного підприємства, тобто йдеться про: оцифровану інформацію, технічні засоби й програмне забезпечення, що дозволяють її отримувати, передавати, опрацьовувати, зберігати й використовувати за призначенням, та інформаційну взаємодію за допомогою технічної інфраструктури. Фактично прихильники необхідності організації кібербезпеки розглядають інформаційні ресурси та засоби роботи з ними, акцентуючи увагу на специфіці здійснення господарської діяльності в онлайн-форматі. Наші висновки ґрунтуються насамперед на утвердженому розумінні суті інформаційної безпеки, яка в безпекознавстві сприймається як одна із ключових функціональних складових ЕБП незалежно від масштабів і специфіки господарської діяльності. Для порівняння, серед

значної кількості відомих визначень інформаційної безпеки нами виділено авторства В. Кузьомко, де це поняття розглядається як «...стан інформаційних ресурсів і пов'язаних з ними інформаційних засобів і систем суб'єкта господарювання, який гарантує якісне і безперебійне забезпечення його діяльності необхідною інформацією за умови високого рівня її захищеності від внутрішніх і зовнішніх загроз» [82, с. 208]. Порівнюючи раніше процитовані визначення кібербезпеки й інформаційної безпеки, можна дійти таких висновків: інформаційна безпека є ширшим поняттям, адже передбачає не лише захист, але й задоволення інформаційних потреб; кібербезпека є складовою інформаційної безпеки із виконанням окремих вузькоспеціалізованих завдань. Окрім цього, вважаємо за необхідне наголосити ще на одному важливому моменті, який полягає у неготовності українських підприємств протистояти загрозам для інформаційної безпеки, що спричинені ЦТЕ. За твердженням аналітиків, лише «...кожна третя організація в Україні (31%) має повністю функціонуючу програму кібербезпеки для захисту від кібератак» [138, с. 82]. На перешкоді покращення захисту українських підприємств стоїть не лише технічне відставання через нижчі темпи ЦТЕ, але й людський фактор. Йдеться як про найманих працівників як основного джерела загроз, так і незадовільний рівень володіння цифровими компетентностями, що знижують ефективність дій суб'єктів безпеки, чому буде приділено більше увагу в подальшому.

Проведені узагальнення й критичний огляд слугують основою для твердження, що розвиток СЕБП полягає в переосмисленні змісту безпекової діяльності в масштабах кожного окремого підприємств відповідно до реального рівня активності використання цифрових технологій й змісту стратегічних цілей. Зміни в СЕБП повинні синхронізуватися із ЦТП, на чому наголошувалося в першому розділі дисертаційної роботи. Відштовхуючись саме від цього базового параметру, вважаємо за доцільне дещо модифікувати позицію А. Ковальчука стосовно етапності ЦТП, яка в його розумінні повинна передбачати «...аналіз бізнес-процесів та стратегічних можливостей; формування персоналу; оцінка результатів» [69, с. 154]. Вважаємо, що: аналіз

бізнес-процесів на предмет їх реалізації із вищим рівнем цифровізації повинен супроводжуватися оцінюванням можливих ризиків задля забезпечення покращення ефективності господарської діяльності загалом; формуванню персоналу, тобто підготовці найманих працівників до роботи із оновленими технічними засобами й програмним забезпеченням, повинен передувати розвиток цифрових компетенцій у суб'єктів безпеки задля більш повного використання переваг цифровізації та недопущення виникнення й впливу нових загроз; оцінка результатів має здійснюватися із врахуванням не лише наслідків реалізації окремих рішень, але й зважаючи на вплив на безпекову діяльність і зміну рівня ЕБП. Загалом ЦТ – набагато складніший процес порівняно із загальноочікуваною роботизацією й автоматизацією, адже стає можливою насамперед через переосмислення бізнес-процесів і здатність адаптуватися до цього працівників. Вважаємо за доцільне підкреслити, що науковці, попри їх відмінні погляди щодо значення цифрової й інформаційної безпеки та кібербезпеки, а також процесу ЦТП, єдині у своїх міркуваннях стосовно можливості досягнення поставлених цілей через покращення цифрової компетентності працівників і найперше співробітників служби безпеки. Відповідно, можна вважати, що розвиток СЕБП, спираючись на теоретичне підґрунтя, вимагає приділення уваги питанням рівня й здатності систематично покращувати цифрові компетентності через високу швидкість технологічного поступу суб'єктами безпеки. Такі міркування дещо відрізняються від загальноприйнятих, де домінують технологічні пріоритети, що спонукало до пошуку й практичного підґрунтя у вигляді проведення опитування представників бізнесу.

Для отримання об'єктивних результатів нами були запрошені до співпраці 45 експертів, які за професією пов'язані із підприємствами різних видів економічної діяльності, зокрема і ВПГ. До уваги були взяті не лише ПП, але й такі, що спеціалізуються на оптовій й роздрібній торгівлі. Зазначений крок здійснений, зважаючи на те, що ЦТ більш активно реалізується в умовах національної економіки саме в секторі послуг, зокрема задоволення

інформаційних потреб підприємствами ВПГ. Залучення експертів, що володіють інформацією стосовно широкого кола підприємницьких структур (Додаток А, рис. А.1), дозволило отримати дані, що об'єктивно характеризують процеси в національній економіці. В процесі підбору експертів, окрім галузевої специфіки, базовим критерієм виступив також масштаб діяльності певного підприємства (Додаток А, рис. А.2). Зазначене є особливо актуальним з огляду на відмінності у функціонуванні СЕБП на малих, середніх та великих підприємствах. Безперечно, як зазначалося у другому розділі, домінуючу частку в національній економіці займають малі форми організації бізнесу, але розроблені в подальшому методичні засади мають широке застосування, зокрема і через ретельний підбір експертів. Одне із завдань, що було визначено під час співпраці із експертами, передбачало розгляд поточної ситуації щодо організації забезпечення ЕБП (Додаток А, рис. А.3).

Доцільно наголосити на тому, що експерти у своїх відповідях стосовно організації забезпечення ЕБП послуговувалися сформованими типовими варіантами, які не враховували окремі специфічні моменти. Аналізувався стан справ на момент опитування, хоча стосовно забезпечення безпеки доцільно говорити про високу динаміку, що спровокована життєвою необхідністю постійного пошуку кращого варіанту задля виживання бізнесу. Потрібно також наголосити, що середній і великі підприємства тяжіють до комбінованого варіанту із різним рівнем співпраці з Поліцією охорони та приватними охоронними службами. Відзначається також зміна у пріоритетах залучення зовнішніх суб'єктів безпеки. Якщо порівняно недавно йшлося виключно про фізичний захист майна підприємства, то в межах останніх кількох років суттєвість втрат через кібератаки змушують бізнес укладати угоду стосовно організації безпечних умов функціонування в інформаційному просторі. Доволі значні витрати на постійне оновлення технічної бази та необхідність залучення висококваліфікованих фахівців через різноманітність кібератак спонукають бізнес до пошуку оптимального варіанту забезпечення безпеки.

У підрозділі 1.3 нами був визначений характер змін у діяльності підприємства за результатами ЦТ (рис. 1.12), основою чого стали кращі практики в економічно розвинутих країнах. В ході співпраці з експертами була отримана інформація про хід ЦТП, які потрапили у вибірку (рис. 3.3).

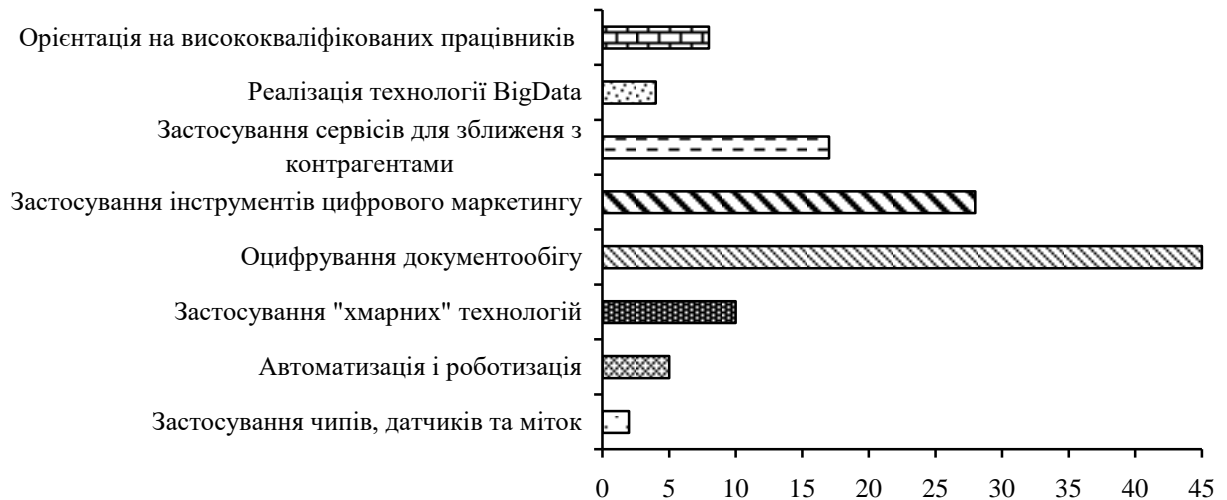


Рис. 3.3. Характеристика поточного рівня ЦТП, *сформовано автором*

Отримані результати фактично підтверджують те, що бізнес ЦТ здійснює через збільшення частки стосовно отримання, накопичення й використання інформації на цифрових носіях (усі 45 підприємств) та більш активне застосування інструментів цифрового маркетингу (28 із 45 підприємств). Останнє стало вирішальним фактором у конкурентній боротьбі під час карантинних обмежень через COVID-19. Зазначимо також, що створення автоматизованого виробництва на основі взаємозв'язку між окремими машинами через промисловий Інтернет сьогодні на певному початковому рівні відбувається лише в умовах окремих фармацевтичних компаній. Не йдеться про повну автоматизацію від замовлення матеріалів і сировини до реалізації готової продукції, але явними є ознаки поступового впровадження технології, де участь людини у виробничому процесі мінімізується до рівня загального контролю.

Наступний етап співпраці з експертами полягав у формуванні переліку найсуттєвіших загроз для ЕБП (рис. 3.4).

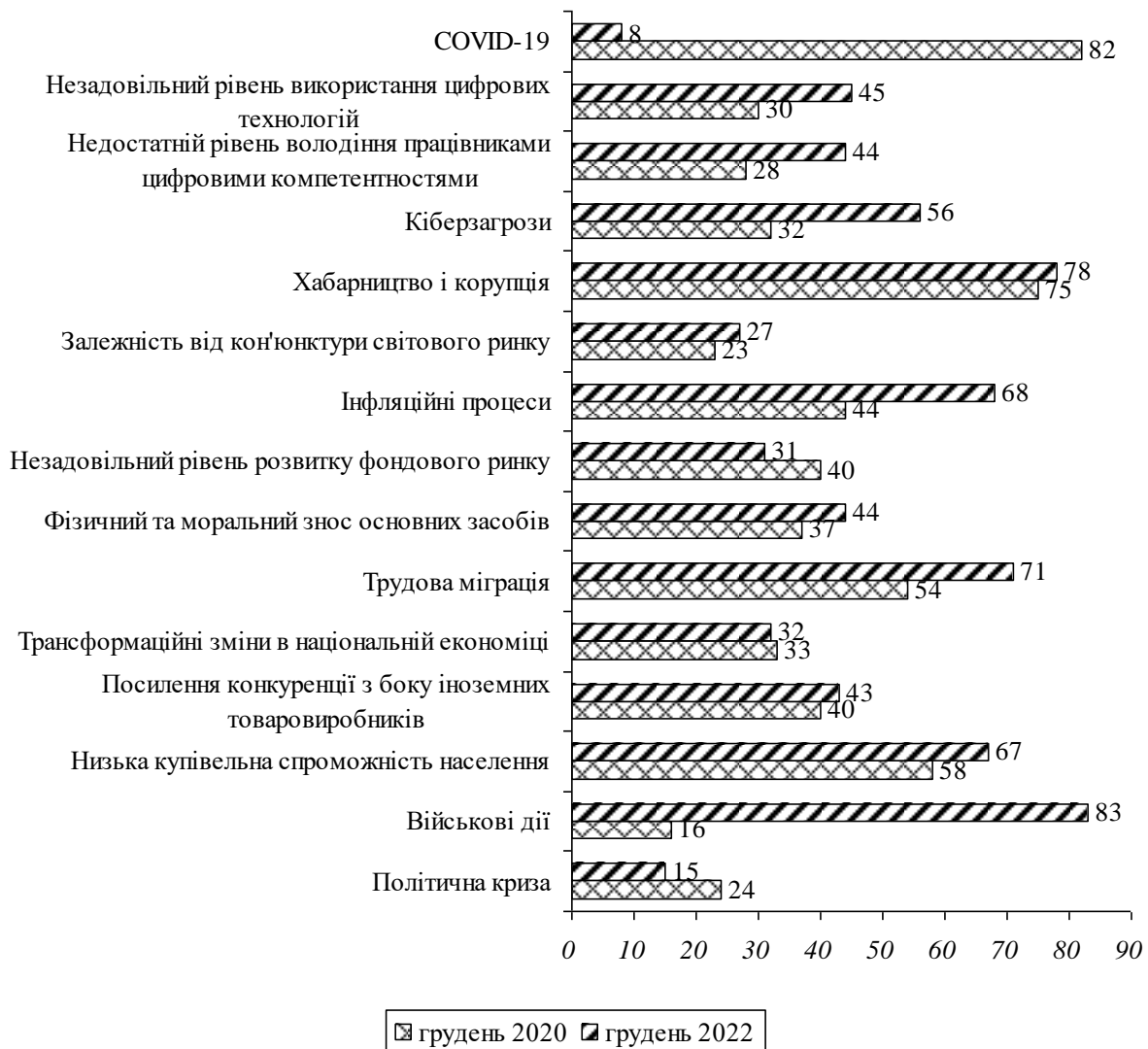


Рис. 3.4. Сукупність найсуттєвіших загроз для ЕБП (грудень 2020 р. та грудень 2022 р.), сформовано автором

Відмінністю цього етапу було те, що експерти повинні були вибрати із максимально широкого переліку загроз ті, які були актуальними для пов'язаних з ними підприємств у двох часових моментах: грудень 2020 р. і грудень 2022 р. Такий крок був здійснений задля відстеження зміни в переліку загроз, що потребували максимальної уваги з боку суб'єктів безпеки.

Отримані результати потрібно тлумачити із врахуванням кількох важливих моментів: 45 досліджуваних підприємств були прийняті за 100%, а результати характеризують частку тих підприємств для яких та чи інша загроза суттєво впливала на їх ЕБ; експерти були дотичні до діяльності підприємств різних видів економічної діяльності, стосовно яких перелік найвагоміших загроз певним чином відмінний, тому отримані результати є усереднені і позбавлені врахування глибокої галузевої специфіки; важливою є динаміка, яка доволі чітко прослідковується у втраті пріоритетності щодо загрози, пов'язаної із COVID-19 та посиленням негативного впливу військових дій; визначальним є зростання впливу загроз для інформаційної безпеки як в частині збільшення кількості кібератак, так й незадовільного рівня володіння персоналом, зокрема й співробітниками служби безпеки, цифровими компетентностями, що гальмують процеси більш активнішого використання цифрових технологій у господарській діяльності. Останній момент нами був розглянутий більш детально за рахунок додаткового розгляду загроз, що безпосередньо пов'язані із ЦТП (рис. 3.5).

В графічному вигляді продемонстровано частку підприємств для яких була актуальна кожна із визначених загроз. Основна частина загроз певним чином пов'язана між собою, адже в їх основі лежить нездатність працівників виконувати поставлені завдання через недостатній рівень цифрових компетентностей. Зазначене повною мірою стосується і співробітників служби безпеки, завдання яких не лише розширилися через необхідність протидії кібератакам та реагування на інші процеси, що протікають в інформаційному середовищі, але й вимагають перегляду підходів для досягнення цілей стосовно інших функціональних секторів ЕБП. Цей аспект є важливим зважаючи на зміни, що визначають подальший розвиток СЕБП, тому йому буде приділена належна увага.

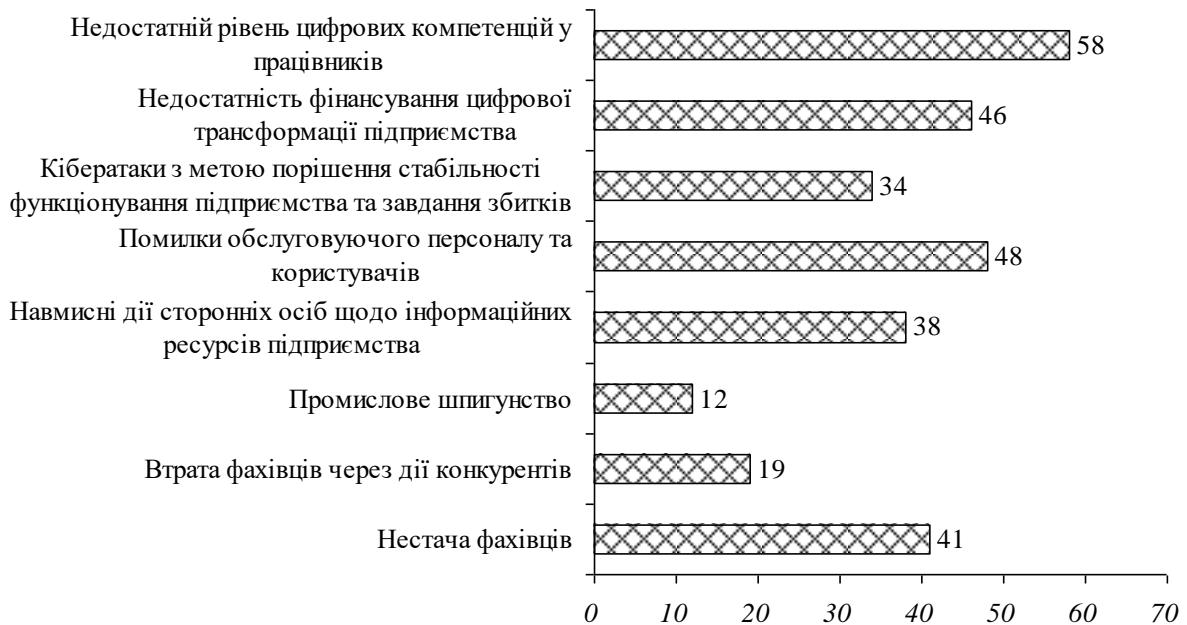


Рис. 3.5. Сукупність загроз для ЕБП, що пов'язані із ЦТ, сформовано автором

Фінансова безпека традиційно розглядається як ключова внаслідок реальної можливості відстежити за рахунок фінансових показників суттєвість впливу кожної загрози. ЦТП першочергово забезпечує покращення ІЗ управління через можливість отримання даних та розроблення на їх основі управлінських рішень, спрямованих на формування й покращення використання фінансових ресурсів, а також пришвидшує банківські операції. Водночас ця ж перевага створює підґрунтя для реалізації кібератак, які спрямовані на викрадення грошових коштів підприємства. Від співробітників служби безпеки вимагається недопущення реалізації нових загроз для фінансової безпеки, що потребує поглиблених знань у сфері фінансів та покращення цифрових компетенцій, зважаючи на характер процесів, які відбуваються в інформаційному просторі.

Не минули зміни й процесу забезпечення інтелектуально-кадрової безпеки через збільшення конкуренції за носіїв інтелектуального капіталу, що здатні генерувати нові знання, а відтак формувати конкурентні переваги певного підприємства. Автоматизація зменшує потребу у звичайній фізичній

праці, але провокує зростання попиту на висококваліфікованих фахівців, які в умовах посилення глобалізаційних й цифровізаційних процесів фактично не обмежені жодними кордонами. Людина традиційно вважається найбільшим джерелом загроз, а посилення інформаційного обміну суттєво збільшує вимоги до організації захисту об'єктів інтелектуальної власності. Загалом же завдання суб'єктів безпеки в сфері кадрової безпеки видозмінюються через наростання інтенсивності використання інформаційних технологій, зокрема і у відносинах між підприємством та найманим працівником.

Забезпечення інформаційної складової ЕБП внаслідок цифровізації трансформується найбільшою мірою через збільшення інформаційних потоків, що повинно залишатися підконтрольним через постійне оновлення технічної бази й покращення цифрових компетенцій обслуговуючого персоналу. Оскільки вище нами уже було акцентовано увагу на необхідності систематичного вдосконалення захисту інформаційних потоків, також наголосимо на збільшенні інформаційних потреб у межах підприємства та більш активного використання інформації як ключового ресурсу у господарській діяльності.

Складність забезпечення техніко-технологічної безпеки зростає через скорочення циклу активного використання устаткування. Не йдеться лише про комп'ютерне обладнання, а загалом про більшість тих засобів, що використовуються для створення суспільного продукту, адже простежується чітка тенденція до зниження матеріало- і енергомісткості засобів виробництва із дедалі більшим насиченням їх чипами для взаємодії між собою. Попри певний розрив у технічному розвитку, українські підприємства змушені дотримуватися високих темпів, що задають їх іноземні конкуренти, що, відповідно, не може залишатися поза увагою суб'єктів безпеки в значенні своєчасної ліквідації швидко змінного переліку актуальних загроз і стосовно цієї складової ЕБП.

Силова безпека, попри її уставлений акцент на фізичний захист майна підприємства, також зазначає змін під впливом ЦТП. Разом із зростанням

кількості рейдерських атак, що супроводжуються попереднім ретельним вивченням бізнесу та формуванням в інформаційному полі відповідного підґрунтя для проведення фізичного захоплення, збільшується кількість випадків шантажу менеджменту вищої ланки через виявлення фактів активності в соціальних мережах. Під час COVID-19 набула актуальності практика широкого застосування віддаленої організації праці, що суттєво змінює поле завдань для суб'єктів безпеки, адже потребує приділення особливої уваги питанням технічного забезпечення віртуальних і фактичних робочих місць, уможливлення безпечного обміну інформацією та підтримання контролю за діями кожного найманого працівника.

Узагальнюючи, можна констатувати, що активне впровадження цифрових технологій, яке є вимушеним кроком для українських підприємств у конкурентній боротьбі, вагомо впливає на функціонування СЕБП, надаючи поштовх до розвитку, який полягає не лише в технічному оновленні, але у поступі стосовно кожного співробітника служби безпеки в частині постійного покращення його цифрових компетентностей. Зазначене чітко прослідковується у висновках, які були зроблені стосовно кожної функціональної складової ЕБП та створює необхідне підґрунтя для більш ретельного розгляду таких понять як «компетенція», «компетентність» й «цифрові компетентності», що в подальшому стануть основою для формування методичних засад розвитку СЕБП.

На сторінках наукових видань триває доволі жвава дискусія стосовно суті та зв'язку між такими термінами як «компетентність» та «компетенція». Враховуючи те, що цей момент був визначений нами як одне із завдань у межах цього підрозділу, то обмежимося лише їх розглядом з позиції, максимально наближеної до проблематики розвитку СЕБП. Вважаємо, що доволі лаконічно сутність поняття «компетентність» подано у Великому тлумачному словнику як «...поінформованість, обізнаність, авторитетність» [19, с. 560]. Разом із чіткістю цього визначення, воно орієнтовано на максимально широке застосування, що є певним недоліком у конкретній ситуації. Серед відомих

позицій науковців заслуговує на увагу думка І. Зязюн, згідно з якою компетентність визначена як «...екзистенціональна властивість людини, що є продуктом її власної життєтворчої активності, ініційованої процесом освіти; як властивість індивіда вона існує в різних формах – як високий рівень умілості, як спосіб особистісної самореалізації (звички, спосіб життєдіяльності, захоплення), як деякий підсумок саморозвитку індивіда, форма вияву здібностей тощо» [56, с. 17]. Без розгляду інших точок зору, які, безперечно, заслуговують на увагу, можна констатувати, що компетентність характеризує процеси не одномоментні, а тривалі і пов'язані із постійним самовдосконаленням за рахунок систематичного здобуття нових знань із їх практичним застосуванням у будь-яких життєвих ситуаціях. Ці узагальнення є основою для твердження, що розвиток СЕБП безпосередньо пов'язаний із покращенням компетентностей у співробітників служби безпеки, який повинен здійснюватися на постійній основі для формування відповідних актуальних на певний момент компетенцій.

У згаданому вище Великому тлумачному словнику термін «компетенція» представлено як «...добра обізнаність із чим-небудь; коло повноважень якої-небудь організації, установи або особи» [19, с. 560]. Порівнюючи між собою трактування обох термінів, що розглядаються, можна дійти висновку, що компетентність є більш ширшим, оскільки характеризує процес генерування знань й їх практичного застосування, коли компетенція – обмежене коло питань, стосовно яких певна особа може вважатися експертом, тобто таким, що більш глибоко обізнаний із аспектами вирішення окремих проблем. В контексті розгляду засад розвитку СЕБП доцільно зосередитися саме на компетентностях, адже ЦТ виходить за рамки кола професійних питань співробітників служби безпеки.

Дотримуючись обраної позиції, що формує основу методичних засад розвитку СЕБП, доцільно наголосити на тому, що саме розуміння суті поняття «компетентність» у межах доволі короткого часового проміжку зазнало суттєвих змін. Якщо в 1960–1970 рр. його пов'язували із демонстрацією

особистістю діяльності, а в 1970–1990 рр. – із володінням певними професійними навичками, то в подальшому актуальним стало «...оволодіння індивідом системи інтелектуальних, моральних та соціальних якостей, потрібних у житті» [102]. Зміна відбулася не лише стосовно загального сприйняття суті компетентності, але її складових, наочним прикладом чого є порівняння переліку таких у 2006 та 2018 рр. Найсуттєвіші зміни були спричинені ЦТ, адже у 2006 р. йшлося про «навички роботи з цифровими носіями», коли у 2018-му уже стала необхідною для кожної особи «цифрова компетентність». На нашу думку, ключовим є те, що цифрова компетентність, завдяки Рекомендаціям Парламенту та Ради Європи у 2006 р., увійшла до ключових восьми компетентностей, якими повинна оволодіти й систематично покращувати кожна особа упродовж життя. Поштовхом до такого кроку стало усвідомлення більш високої динаміки технологічного поступу порівняно із формуванням людського капіталу, коли не лише виробництво інноваційної продукції, але й її масове використання гальмувалося через відсутність необхідних знань у споживачів. Відповідно до цього в початковій версії цифрова компетентність визначалася як «...здатність упевнено, критично та творчо використовувати цифрові технології для досягнення цілей, що належать до галузі роботи, зайнятості, навчання, дозвілля, участі в житті суспільства» [196]. Вважаємо, в цьому визначенні підкреслюється не лише роль цифрової компетентності у здобутті й покращенні інших компетентностей у сучасному середовищі, насиченому цифровими технологіями, але й те, що її розвиток потребує ресурсних затрат як з боку кожної особи для покращення особистої конкурентної позиції на ринку праці, так і підприємства задля збільшення людського капіталу та досягнення стратегічних цілей завдяки його ефективному використанню. Україна не залишається осторонь цих процесів, на що вказує схвалена у 2021 р. «Концепція розвитку цифрових компетентностей до 2025 року» [63].

У межах доволі короткого часу неодноразово уточнювався зміст цифрової компетентності. У 2013 р. Європейською Комісією до застосування була

запропонована система DigComp, яка в подальшому була видозмінена у 2016-му до версії 2.0, а з 2017-ого у вигляді версії 2.1, яка і була взята в Україні за основу для наслідування. В документах Міністерства ЦТ цифрова компетентність визначена як «...інтегральна характеристика особистості, яка динамічно поєднує знання, уміння, навички та ставлення щодо використання цифрових технологій для спілкування, власного розвитку, навчання, роботи, участі суспільному житті» [106]. Сам факт постійного перегляду й поточне тлумачення вказують на високу динаміку тих процесів, що вимагають від кожної особистості систематичного адаптування, щоб залишатися в контакті із суспільством й мати змогу конкурувати на ринку праці за вищу оплату та кращі умови виконання професійних завдань.

Поточна версія DigComp 2.1. розрізняє п'ять видів цифрових компетентностей («...інформаційна грамотність та грамотність щодо роботи з даними; комунікація та взаємодія; цифровий контент; безпека; вирішення проблем») та вісім можливих рівнів їх розвитку. Така рамка також сприяє чіткості у визначенні пріоритетів стосовно розвитку СЕБП, зважаючи на доведену вище необхідність покращення компетентностей кожного співробітника служби безпеки. Вона також повинна бути використана для встановлення індивідуальних часових орієнтирів, що забезпечить поступ через стимулювання та можливість здійснення контролю за розвитком особового складу відповідних підрозділів.

Зважаючи на те, що сьогодні в безпекознавстві, зокрема в сфері забезпечення ЕБП, питанню цифрових компетентностей не приділяється належна увага, то нами зроблена спроба сформулювати методичні засади для подальшої активізації наукових розвідок у цьому напрямі. В основу таких засад покладено результати теоретичного розгляду й опитування експертів стосовно зміни складу та рівня впливу ключових загроз на ЕБП. Також взято до уваги досвід ЄС щодо розвитку цифрових компетентностей в громадян, зокрема рамку DigComp 2.1, застосування якої повинно сприяти ранжуванню із подальшим стимулюванням до покращення рівня володіння цифровими

технологіями суб'єктів безпеки, а також персоналу підприємства загалом. У графічному вигляді авторський варіант методичних засад розвитку СЕБП представлено на рис. 3.6.

Графічно нами зроблена спроба не лише представити зв'язок між усіма складовими, які створюють підґрунтя для розвитку СЕБП через формування цифрових компетентностей у суб'єктів безпеки, але ще раз підкреслити необхідність таких випереджувальних змін, які в подальшому сприятимуть ЦТ усього підприємства.

Запропоноване розуміння цифрових компетентностей суб'єктів безпеки узгоджується із тими орієнтирами, що застосовуються в ЄС та Україні, але враховують специфіку діяльності таких фахівців, тобто прив'язані до виконання безпекової діяльності. Ми не порушуємо питання професійної підготовки та підвищення кваліфікації співробітників служби безпеки, але вважаємо, що вони можуть вирішуватися на більш високому рівні за рахунок цифрових навичок.

Доцільно ще раз акцентувати увагу, що формування й розвиток цифрових компетентностей має постійний характер, тобто упродовж життя і пов'язано із узгодженнями інтересів кожної особи та підприємства. Безперечно, виконання частини завдань може здійснюватися на засадах аутсорсингу, тобто у співпраці із ІТ-компаніями, але це не зменшує потребу в постійному покращенні цифрових компетентностей внутрішніх суб'єктів безпеки.

Сам процес покращення таких компетентностей може здійснюватися: шляхом періодичного проходження спеціальних ознайомчих курсів із подальшим практичним застосуванням здобутих знань; через постійне спілкування з ІТ-фахівців для ознайомлення із новітніми тенденціями в розвитку ІКТ; в процесі обміну досвідом із зовнішніми суб'єктами безпеки.

Нами визначено три рівні, що характеризують ступінь володіння цифровими компетентностями суб'єктів безпеки.

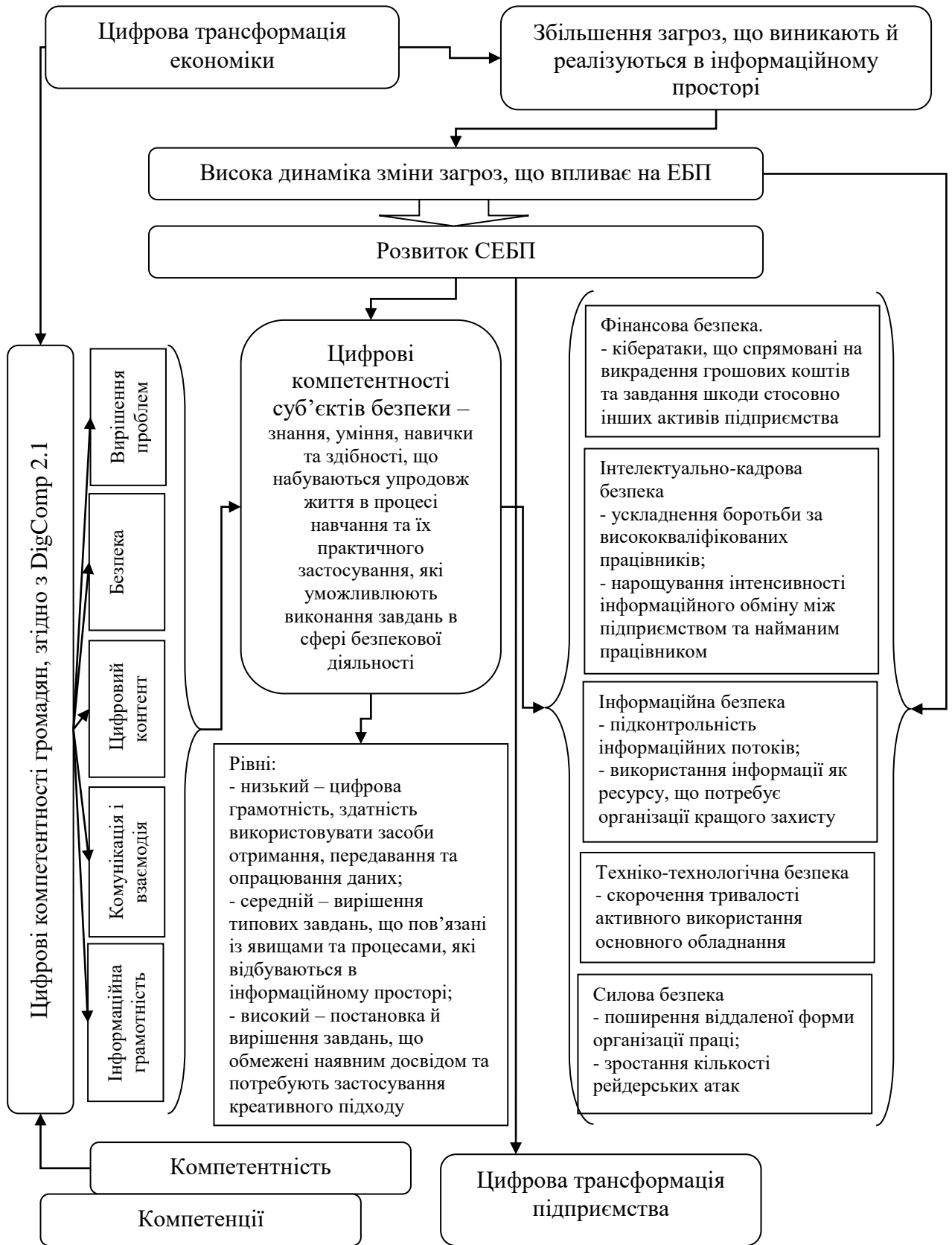


Рис. 3.6. Методичні засади розвитку СЕБП на основі формування цифрових компетентностей у суб'єктів безпеки, сформовано автором

Їх практичне застосування пов'язано із розподілом завдань у процесі виконання безпекової діяльності, а також для контролю й стимулювання самовдосконалення кожного співробітника служби безпеки.

При окресленні змісту кожного із рівнів ми не прив'язувалися до необхідності володіння певними знаннями, адже темпи технологічного поступу вимагають постійного перегляду таких критеріїв. Водночас беззаперечним є те, що стосовно дедалі більшої частини пріоритетних загроз у межах кожної функціональної складової ЕБП реалізація захисних заходів не може бути здійснена без володіння суб'єктами безпеки цифровими компетенціями.

3.3. Моделювання розвитку системи економічної безпеки підприємства

Важливість створення сприятливих та безпечних умов для ЦТП в ситуації підвищеної невизначеності розвитку й цифровізації національної економіки потребує застосування підходів щодо моделювання змін у СЕБП. Одним із кращих варіантів такого моделювання можна вважати застосування методу IDEF0, зважаючи на такі аспекти: по-перше, він був створений у 1981 р. для цілей автоматизації промислового виробництва у США, тобто безпосередньо пов'язаний із ЦТП; по-друге, його ключова перевага полягає у покращенні взаємодії в парі «аналітик-фахівець», тобто розроблені моделі є зрозумілими для широкого кола користувачів, що дозволяє чітко регламентувати кожен крок виконавця і забезпечує досягнення поставлених завдань попри високу динаміку перебігу певного процесу; по-третє, цей метод дозволяє на першому етапі побудувати контекстну діаграму, що відображає ключові моменти протікання певного процесу із подальшою глибинною деталізацією кожного з них, зважаючи на наявні умови, процес реалізації та очікувані результати, що загалом, окрім цілісності, створює деталізовану технологічну карту. Також вважаємо за доцільне підкреслити ту обставину, що IDEF0 набув застосування

й у вирішенні проблем безпекової діяльності, тобто уже існує необхідний фундамент, який створює умови для використання його у вирішенні наступних завдань. Таким фундаментом можна вважати напрацювання науковців, більшість з яких є дотичні до активної діяльності Львівської безпекової школи, зокрема В. Фостяк здійснив спробу «...моделювання процесу управління безпековою діяльністю промислових підприємств» [154], М. Копитко та Ю. Ільків проводили «...моделювання процесу формування механізму управління безпековою діяльністю інноваційно-активних підприємств» [76, с. 163], Т. Шира сконцентрував увагу на «...моделюванні забезпечення функціонування системи корпоративної безпеки підприємства» [172, с. 230], О. Силкін розробив контекстні діаграми для «...моделювання антикризового управління в процесі забезпечення фінансової безпеки підприємства» [134, с. 376], О. Поліщук досліджувала питання «моделювання забезпечення функціонування адаптивно-орієнтованої системи управління економічною безпекою промислового підприємства» [119, с. 140]. Кожен із згаданих науковців ставив перед собою конкретне завдання і вирішував його за допомогою IDEF0, але жодне з них не було пов'язано із розвитком СЕБП, що дозволяє скористатися їх досвідом для здійснення авторських розробок, які будуть слугувати складовою для подальшого теоретичного базису безпекової діяльності на рівні підприємства.

Перший етап застосування методу IDEF0 полягає у визначенні вихідних умов, які закладають необхідне підґрунтя для подальшого моделювання, адже передбачають встановлення таких важливих компонентів як «мета», «точка зору» (ініціатор та розробник), «цільова аудиторія» (виконавці), «технологія» тощо (Додаток А, рис. А.4). Попри те, що засади застосування IDEF0 є незмінними, але вирішення кожного окремого завдання на їх основі вимагає уточнення базових умов із виділенням тих аспектів, які визначають процес не лише розроблення, але й застосування моделей. Такою особливістю можна назвати визначену мету, формулювання якої відштовхується від того, що стосовно СЕБП виникають зміни під впливом різноаспектних факторів, але

досягнення поставлених завдань можливе в тому випадку, якщо відбувається підконтрольний процес трансформації, а не спонтанний.

В попередніх підрозділах нами розглядалися основні аспекти, які пов'язані із процесом розвитку СЕБП. IDEF0 уможливорює їх об'єднання та подання у вигляді ієрархічної структури функціональної моделі (рис. 3.7). В межах процесу розвитку СЕБП виділено кілька підпроцесів, що повинні протікати згідно з встановленими директивами та зберігати підконтрольність для досягнення поставлених цілей. Виділені підпроцеси відображають розуміння того, що початковий імпульс утворюють тенденції щодо ЦТЕ, зміни в діяльності підприємства та поступ в удосконаленні безпекової діяльності, зокрема за рахунок використання цифрових технологій та покращення цифрових компетентностей співробітників служби безпеки. Виявлені зміни є основою для оцінювання поточного рівня розвитку СЕБП із установленням моментів, що потребують реагування через розроблення програми розвитку та її реалізацію.

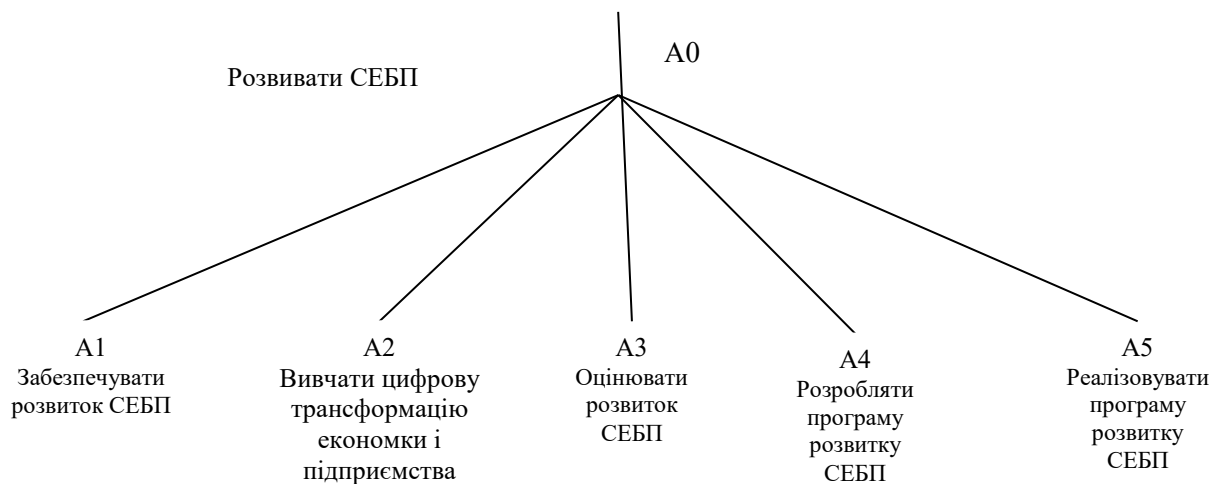


Рис. 3.7. Ієрархічна структура функціональної моделі IDEF0 розвитку СЕБП, сформовано автором

Розроблена ієрархічна структура стала основою для побудови контекстної діаграми (рис. 3.8), що за змістом відповідає системному підходу, оскільки наявні вхідні потоки у вигляді реалізації потреби в розвитку СЕБП (I1),

фінансово-матеріального забезпечення (I2), яке необхідне для реалізації програми розвитку, та інформаційного підґрунтя для здійснення змін (I3). Хід процесу визначається регламентуючими положеннями, які представлені законодавчими та внутрішніми обмеженнями, а також попередньо розробленими методичними засадами у вигляді практичних рекомендацій стосовно здійснення оцінювання та механізмів розвитку СЕБП. Для реалізації процесу розвитку необхідними є механізми, під якими в IDEF0 розуміють суб'єкти безпеки та засоби праці. Результатом виконання процесу повинна бути інформація щодо розвитку СЕБП, а також рекомендації щодо ЦТЕ загалом, що відповідає парадигмі, яка була сформована у підрозділі 1.3. Для чіткості розуміння авторського підходу кожна із складових контекстної діаграми деталізована (Додаток А, рис. А.5-А.8).

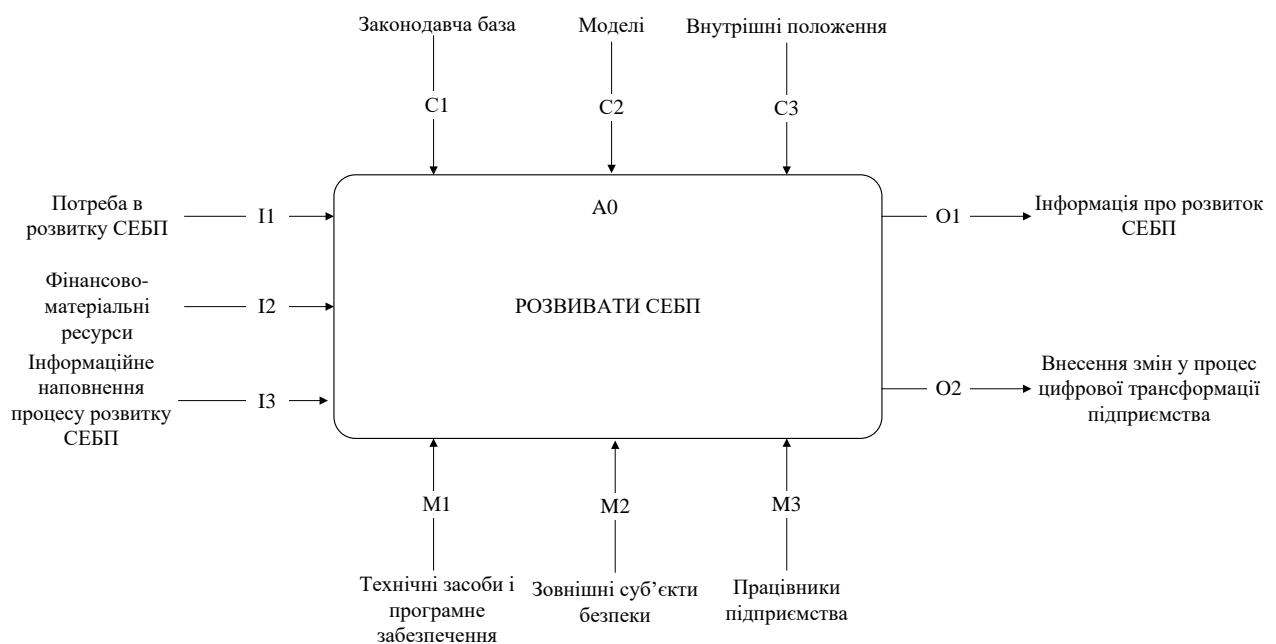


Рис. 3.8. Контекстна діаграма моделі IDEF0 розвитку СЕБП, сформовано автором

На рис. 3.9, шляхом використання програми для створення векторних діаграм, нами побудована декомпозиція першого порядку, зміст складових якої охарактеризовано нижче.

A1 – Забезпечувати розвиток СЕБП. Процес розвитку СЕБП реалізується як відповідь на ЦТЕ та наявні через це зміни у діяльності підприємства.

Пасивність суб'єктів безпеки провокує їх нездатність своєчасно реагувати на нові ризики й загрози, які виникають через більш масштабне застосування цифрових технологій й збільшення частки цифрової економіки із врахуванням національних особливостей цих трансформацій. Розвиток СЕБП повинен відповідати тенденціям змін на макро- та мікрорівні із урахуванням поступу в безпековій діяльності, зокрема в частині застосування ІКТ та зростання вимог до кваліфікаційного рівня співробітників служби безпеки. Основою розроблення програми розвитку повинна стати потреба у змінах, інформація про тенденції ЦТЕ, фактична відповідність СЕБП цим змінам та спроможність перейти на новий кращий рівень безпекової діяльності на основі оцінювання безпекового потенціалу. Результат здійснення такого процесу полягає не лише в покращенні через осучаснення СЕБП, але створення необхідних умов для успішної ЦТП загалом.

A2 – Вивчати ЦТЕ і ЦТП. ЦТ в Україні відбувається не лише з нижчими темпами у порівнянні із економічно розвинутими країнами, але орієнтована не на розвиток високотехнологічного промислового виробництва, а на більш активне впровадження цифрових технологій у сферу послуг. Попри це відстеження ЦТ не може обмежуватися національною економікою, а повинно здійснюватися через аналіз тенденцій в межах світової економіки внаслідок відкритості внутрішнього ринку. Технологічний поступ має динамічний характер і цифрові новації в інших країнах максимально швидко розпочинають застосовуватися в країнах-наслідувачах, якою сьогодні виступає й Україна. Вивчення змін на підприємстві спрямовано на виявлення тих фактів у всіх сферах діяльності, які наявні і не лише пов'язані із ЦТ, але визначають характер перебігу фінансово-господарських процесів. Результатом цього підпроцесу є інформація щодо природи змін на макро- та мікрорівні, яка є основою для розвитку СЕБП як такої, що першою повинна трансформуватися, виявити факти можливих додаткових ринкових можливостей або ризиків й загроз, які виникатимуть у тактичному й стратегічному часовому вимірах.

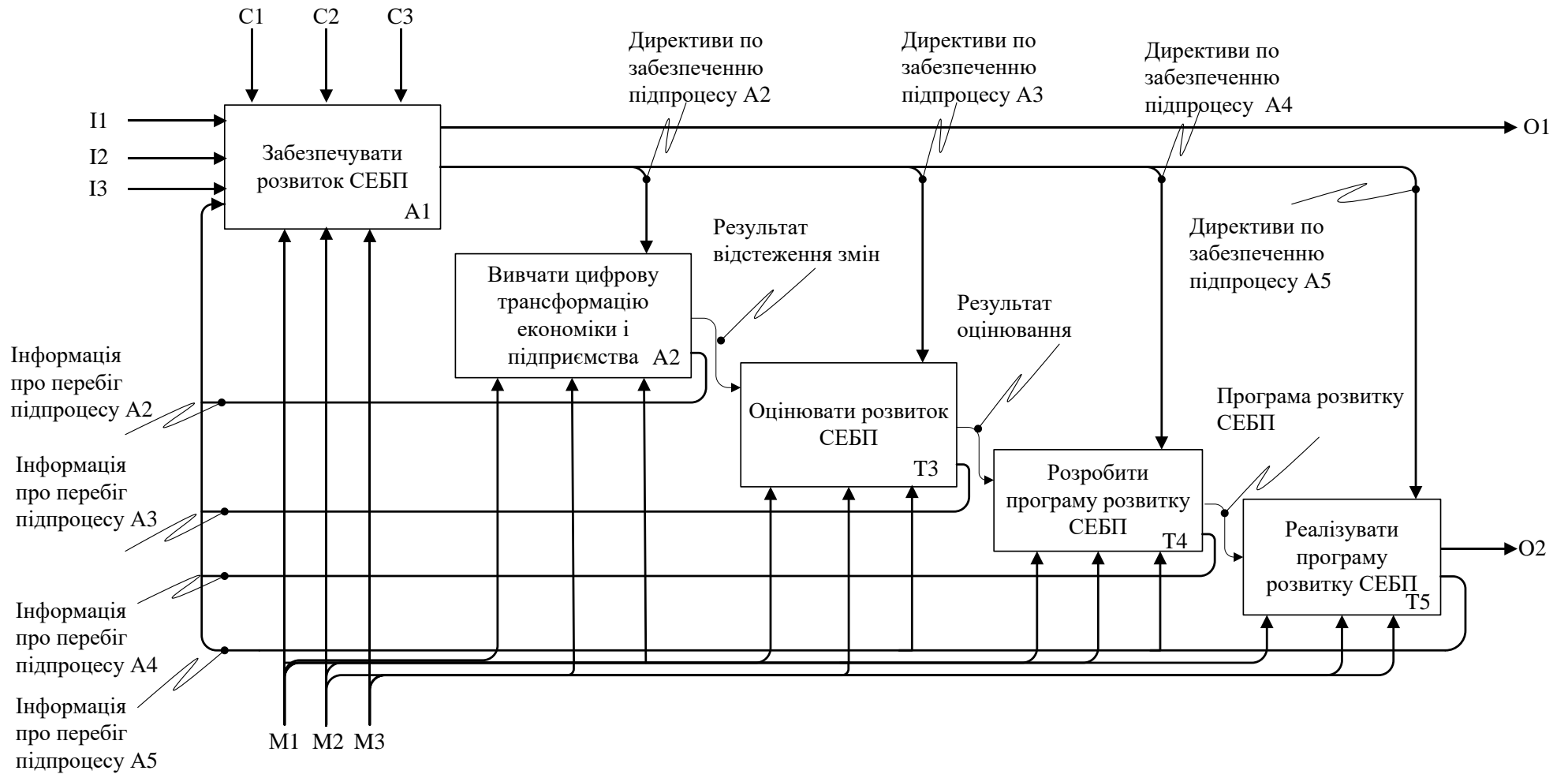


Рис. 3.9. Декомпозиція першого рівня контекстної діаграми моделі IDEF0 розвитку СЕБП, сформовано автором

A3 – Оцінювати розвиток СЕБП. У межах традиційного підходу в забезпечення ЕБП домінує позиція періодичного оцінювання СЕБП з метою констатації фактів покращення чи погіршення рівня безпеки у розрізі основних функціональних складових як інформаційного підґрунтя для прийняття управлінських рішень стосовно ліквідації виявлених загроз. Оцінювання розвитку СЕБП передбачає ретельний розгляд спроможності й результативності вирішення проблем не по факту, а в процесі безпекової діяльності задля покращення параметрів СЕБП й досягнення результатів не через ліквідацію наслідків, а за рахунок попередження та недопущення розвитку причин негативних змін та більш ефективного використання нових можливостей. Особлива увага приділяється питанню оцінювання кваліфікаційного рівня, знань, умінь, навичок та володіння цифровими компетентностями співробітників служби безпеки, їх здатності самоудосконалюватися та вивчати й застосовувати кращі практики безпекової діяльності в умовах певного підприємства. Результатом цього підпроцесу повинен бути звіт про поточний рівень СЕБП, здатність суб'єктів безпеки якісно виконувати поставлені завдання, виявлені проблемні місця та потребу внесення змін.

A4 – Розробити програму розвитку СЕБП. Інформація за підпроцесами A2 та A3 слугує необхідною основою для розроблення кількох варіантів розвитку СЕБП, враховуючи також результати оцінювання безпекового потенціалу, який фактично виступає ресурсним обмежувачем в реалізації певних планів. Кожен із альтернативних варіантів повинен формуватися, зважаючи на зміст цільового спрямування, тобто економічного, адміністративно-правового, інформаційного, техніко-технологічного й кадрового. Вибір оптимального варіанту здійснюється на основі моделювання, з огляду на зміст оптимістичного, песимістичного й реалістичного прогнозів щодо темпів ЦТЕ та характеру змін підприємства в короткостроковій й довгостроковій перспективах. Результатом цього підпроцесу є розроблена програма розвитку СЕБП, яка узгоджується із стратегією розвитку підприємства, має сформоване ресурсне забезпечення щодо реалізації та містить індикатори для відстеження її реалізації та

здійснення коригування відповідно до появи чи зміни суттєвості впливу факторів.

A5 – Реалізувати програму розвитку СЕБП. Специфіка безпекової діяльності полягає у ключовій ролі людського фактору, тому розвиток СЕБП значно охоплює питання покращення якісних характеристик суб'єктів безпеки. Оволодіння й ширше застосування цифрових технологій можливе за наявності бажання, спроможності й сприятливого клімату для покращення цифрових компетентностей, що загалом відповідає засадам інтенсивного розвитку. У випадку екстенсивного розвитку виникає необхідність додаткового набору та підготовки фахівців, які будуть виконувати вузькоспеціалізовані завдання, зокрема в сфері конкурентної розвідки та контррозвідки. Варіант зовнішнього розвитку пов'язаний із поглибленням взаємодії із зовнішніми суб'єктами безпеки як в питаннях обміну інформацією, так й передання частини завдань на аутсорсинг. Прогресивний розвиток спрямований на перехід до більш досконалої форми організації бізнесу, водночас поточні умови для українських підприємств вимагають розгляду й варіанту регресивного розвитку через суттєве скорочення економічної активності підприємницьких структур. Виконання програми пов'язано також із протидією спротиву працівників, які традиційно не мають бажання перелаштовувати сформований порядок виконання функціональних завдань. Реалізація програми повинна здійснюватися відповідно до розробленої технологічної карти із постійним відстеженням дотримання попередньо визначених рівнів індикаторів як основи для внесення коректив.

Однією із ключових особливостей методу IDEF0 є те, що кожен із підпроцесів можна в подальшому деталізувати шляхом розроблення декомпозиції другого та подальших рівнів. Нами було використано таку можливість для більш ретельного розгляду підпроцесів A2 (рис. 3.10) та A4 (рис. 3.11), результати чого будуть розглянуті нижче.



Рис. 3.10. Декомпозиція другого рівня (блок A2) контекстної діаграми моделі IDEF0 розвитку СЕБП, сформовано автором

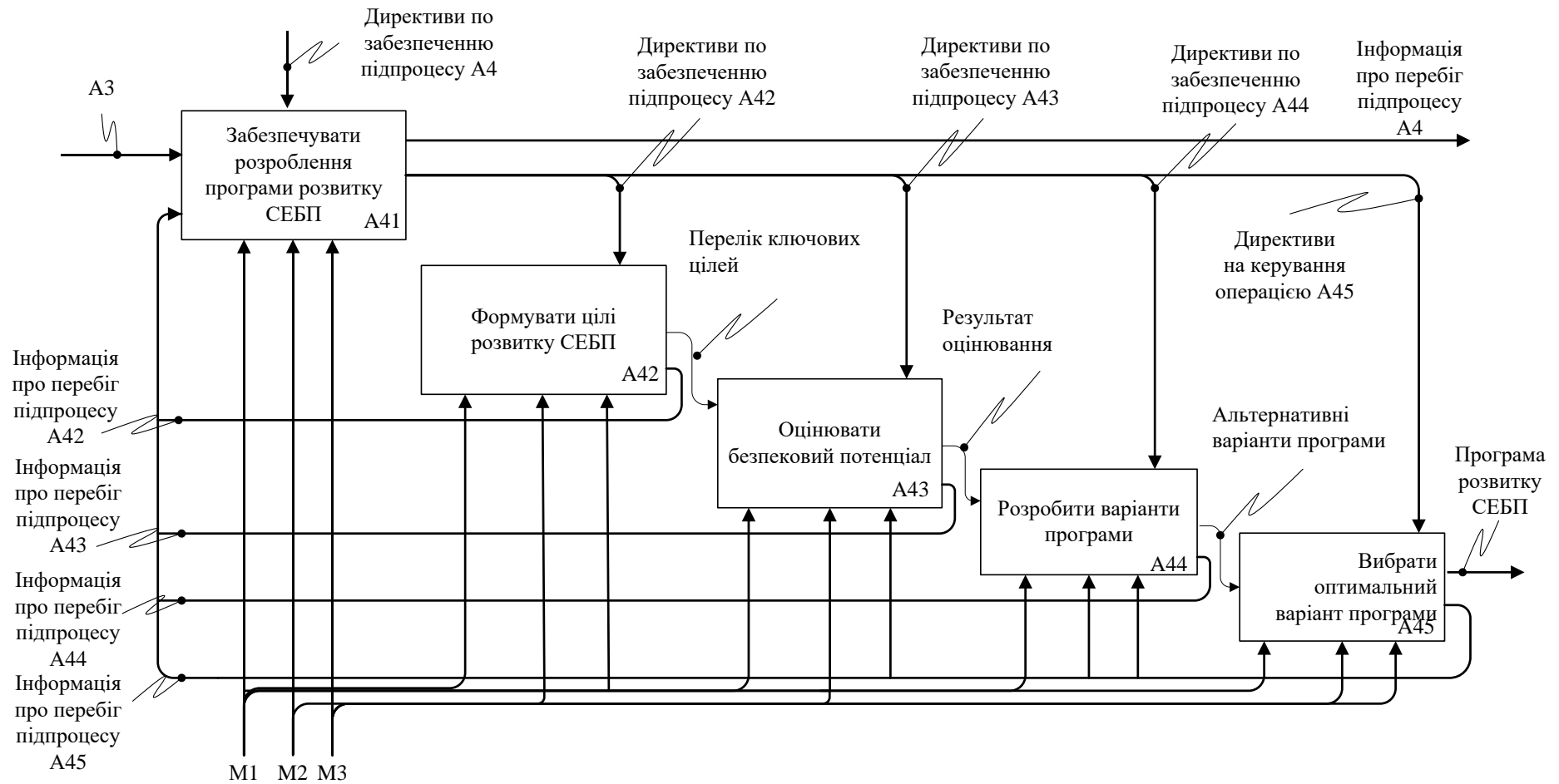


Рис. 3.11. Декомпозиція другого рівня (блок А4) контекстної діаграми моделі IDEF0 розвитку СЕБП, сформовано автором

A21 – Забезпечувати вивчення ЦТЕоміки і підприємства. Суб'єкти безпеки повинні сформувати необхідне інформаційне підґрунтя для розвитку СЕБП шляхом ретельного відстеження змін, що виникають на макро- та мікросередовищі для виявлення тих, що потребують відповідної реакції у вигляді ЦТП. Хибною є позиція, що передбачає виключно концентрацію на взаємодії із постійними постачальниками й споживачами. Попри певну стабільність, у довгостроковій перспективі можлива невідповідність ринковому середовищу через неочікуване руйнування традиційних зв'язків та нездатність конкурувати в інших умовах. Постійний моніторинг не лише сфери діяльності підприємства, а загалом ситуації в регіональному, національному й міжнародному масштабах дозволяє провадження гнучкої політики із уникненням загроз та використанням нових можливостей. Відстеження змін у діяльності підприємства, що можуть бути наслідком адаптації до динамічних умов ведення господарської діяльності, створює необхідний інформаційний базис для реагування на ці трансформації в частині їх розвитку або гальмування. Цей процес завершується звітами стосовно змін на різних рівнях з окресленням ймовірних наслідків.

A22 – Вивчати тенденції розвитку національної економіки. Українська економіка характеризується критично високим рівнем хаотичності змін із проявом у межах останнього десятиліття ознак деіндустріалізації й поглиблення сировинної орієнтації, зокрема в частині виробництва сільськогосподарської продукції та видобування корисних копалин із подальшим їх експортом у вигляді сировини, або продукції з незначною часткою доданої вартості. Політична нестабільність, демографічна криза, соціальні збурення, COVID-19 та військові дії загалом створюють несприятливе середовище для функціонування бізнесу. Збереження та створення передумов для розвитку бізнесу можливе у випадку ретельного відстеження усіх змін із відповідним своєчасним реагуванням. Результатом протікання цього підпроцесу повинні стати звіти стосовно як тих сфер національної економіки,

що стосується діяльності підприємства, так і загалом загальноекономічної ситуації.

A23 – Вивчати зміни на ринках. Існуюче технологічне відставання України від економічно розвинутих країн створює певний лаг в протіканні процесів, що повинно бути використане суб'єктами безпеки для прогнозування можливих змін, які потребують розвитку СЕБП із подальшою ЦТП загалом. Посилення глобалізаційних процесів та відкритість внутрішнього ринку також вимагає відстеження змін на світових ринках, зокрема ринку праці, виходячи із ключової ролі робочої сили як ресурсу, кількісні й якісні параметри якого через четверту ПР й орієнтацію на цифрову економіку зазнали суттєвих змін. Останнє особливо важливе з позиції погіршення демографічної ситуації та посилення трудової міграції. Цей підпроцес також пов'язаний із моніторингом технологічних змін в секторі діяльності підприємства. Результатом підпроцесу повинні стати періодичні звіти із висвітленням основних тенденцій в змінах засад здійснення господарської діяльності, які стосуються функціонування підприємства.

A24 – Досліджувати зміни в діяльності підприємства. Флуктуаційні процеси повинні бути завжди в полі зору суб'єктів безпеки для визначення моменту наближення до точки біфуркації та вибору прийняттого атрактора. Відстеження змін вимагає побудови карти внутрішнього середовища із визначенням індикаторів відстеження їх інтенсивності та встановленням критеріїв рівня реакції. Складністю відзначаються ті частини такої карти, що пов'язані із робочою силою внаслідок створення найбільшої частини внутрішніх загроз через дії чи пасивність найманих працівників. Постійний контроль із залученням працівників до безпекової діяльності завдяки формуванню в межах корпоративної культури розуміння важливості узгодженого досягнення інтересів підприємства й кожного працівника дозволяє своєчасно виявляти зміни та реалізовувати рішення щодо їх розвитку, якщо вони узгоджуються із цілями бізнесу, або гальмувати через можливі втрати.

Результатом підпроцесу повинні стати періодичні звіти щодо стану й динаміки внутрішньогосподарських процесів підприємства.

A25 – З'ясувати тенденції в безпековій діяльності. Безпекознавство, зважаючи на домінування безпекового аспекту для існування й розвитку бізнесу, активно розвивається, зокрема й шляхом впровадження інформаційних технологій та покращення цифрових компетентностей співробітників служби безпеки. Якщо раніше переконливим був факт специфіки національної економіки, що не дозволяло в певній мірі використати іноземний досвід через суттєво відмінні умови здійснення ведення бізнесу, то ЦТ змінює цю ситуацію. Вивчення кращих іноземних та українських практик протидії хакерським атакам, захисту інформаційних ресурсів, уникнення шахрайських схем, здійснення конкурентної розвідки та проведення контррозвідувальних заходів, стимулювання інтелектуально-креативної активності працівників тощо стає необхідним підґрунтям для розвитку СЕБП. Результатом цього підпроцесу повинні бути періодичні зміни про новації в безпековій діяльності з метою запозичення через реалізацію відповідної програми розвитку СЕБП.

Шляхом застосування IDEF0 нами було розроблено декомпозицію другого порядку і стосовно підпроцесу A4 (рис. 3.19).

A41 – Забезпечувати розроблення програми розвитку СЕБП. В основі цього підпроцесу покладено ключові моменти запропонованого у підрозділі 1.3 концептуального підґрунтя розвитку СЕБП. Наявність програми, де чітко встановлені цілі розвитку, що узгоджуються із тенденціями ЦТЕ й характером змін в діяльності підприємства, містяться результати оцінювання безпекового потенціалу, встановлений графік виконання основних етапів із переліком відповідних індикаторів, забезпечує необхідну цілісність та чіткість в здійсненні розвитку СЕБП. Програма розробляється співробітниками служби безпеки у взаємодії із працівниками функціональних підрозділів підприємства, які долучаються до безпекової діяльності. Результатом підпроцесу є оптимальний варіант програми розвитку СЕБП, вибраний на основі математичного моделювання та врахування думок експертів.

A42 – Формувати цілі розвитку СЕБП. Цілі визначаються на основі існуючих потреб у зміні безпекової діяльності певного підприємства, результатів оцінювання поточного рівня розвитку СЕБП та стратегії розвитку підприємства. Цілі повинні бути структуровані як економічні, адміністративно-правові, інформаційно-аналітичні, техніко-технологічні та кадрові. Стосовно досягнення кожної цілі повинні бути встановлені часові параметри, оскільки оновлення матеріально-технічної бази для більш якісного виконання поставлених завдань може бути виконано в короткий проміжок часу, але покращення цифрових компетентностей, що дозволить ефективно використовувати новіші версії програмного забезпечення для опрацювання великих обсягів інформації, пов'язано із навчанням окремих співробітників, а відтак є більш тривалим процесом. Результатом підпроцесу повинен стати перелік ключових цілей розвитку СЕБП.

A43 – Оцінювати безпековий потенціал. Спроможність досягнути поставлених цілей визначається наявним ресурсним забезпеченням (фінансове, матеріальне, інформаційне та кадрове). Важливість цього підпроцесу пов'язана із існуючою практикою здійснення забезпечення безпекової діяльності за залишковим принципом в супереч актуальній на сьогодні пріоритетності безпеки для функціонування й розвитку бізнесу. Результати оцінювання безпекового потенціалу вибудовують, разом із встановленими цілями, другу вісь координат, що визначає параметри розроблення програми розвитку СЕБП.

A44 – Розробити варіанти програми. Чисельність цілей із різними періодами досягнення, результати оцінювання поточного рівня розвитку СЕБП та безпекового потенціалу сприяють розробленню альтернативних варіантів програми. Виконання цього завдання покладається на співробітників служби безпеки, які повинні залучитися підтримкою менеджерів вищої ланки управління та проводити консультації з експертами. Кожен варіант має бути ретельно обґрунтованим та містити календарний план виконання й індикатори для контролю. Результатом підпроцесу повинні стати кілька варіантів програми розвитку СЕБП.

A45 – Вибрати оптимальний варіант програми. Процес вибору здійснюється із застосуванням таких методів як експертного аналізу та парних порівнянь за перевагою варіантів. Результат підпроцесу становить прийнята за основою та затверджена керівництвом підприємства до виконання програма розвитку СЕБП.

Застосування методу IDEF0 дозволило сформувавши цілісне уявлення стосовно процесу розвитку СЕБП, дотримуючись базових умов у вигляді тенденцій в ЦТЕ, змін в діяльності підприємства, поточного рівня розвитку й наявного безпекового потенціалу, що загалом створює необхідне підґрунтя для практичного застосування в умовах українських підприємств, результатом чого повинно стати покращення ефективності дій суб'єктів безпеки та створення безпечних умов для ЦТП загалом.

ВИСНОВОК ДО РОЗДІЛУ 3

1. Узагальнено та систематизовано зміст таких понять як «стійкість», «стабільність», «рівновага», які активно використовуються безпекознавцями, у поєднанні із «флуктуацією», «біфуркацією», «атрактором» й «гомеостазом», котрі застосовуються економістами в більшості стосовно макроекономічних процесів, що в цілому дало змогу сформувавши необхідне підґрунтя для розроблення механізму розвитку СЕБП через: ретельний розгляд взаємозв'язків між усіма поняттями; моделювання ситуації із різним ступенем зміни умов функціонування підприємства; послідовне доведення необхідності вносити зміни в діяльність суб'єктів безпеки; обґрунтування можливості реагування на тенденції в ЦТЕ виключно за рахунок попереднього формування безпечних умов подальших змін в межах підприємства.

2. Обґрунтовано, що стандартні схеми ліквідації дестабілізуючих факторів дають змогу вирішувати типові завдання, але нові, спричинені високими темпами ЦТЕ, залишаються без відповіді, тим самим негативно впливаючи на рівень ЕБП. Зважаючи на фактичну відсутність розвідок у питаннях розвитку СЕБП, було розроблено відповідний механізм управління, в межах якого

деталізовано такі його елементи як: методи та інструменти здійснення керуючого впливу; етапи реалізації (діагностика, оцінювання, планування, реалізація, контроль); цільове спрямування (інформаційне, адміністративно-правове, кадрове, економічне, техніко-технологічне). Застосування такого механізму покликано сприяти постійному осучасненні засад функціонування СЕБП у відповідності до тенденцій в ЦТЕ та створювати сприятливі умови для ЦТП.

3. Критично проаналізовано існуючі тенденції до поглиблення розвідок у безпекознавстві стосовно «цифрової безпеки» та «кібербезпеки». З'ясовано, що така активність викликана збільшенням активності підприємницьких структур у інформаційному просторі на фоні карантинних обмежень та ускладнень, спровокованих військовими діями, але результатом стає дублювання або ж заміна усталених засад безпекової діяльності без реального вирішення проблеми розвитку, зокрема СЕБП. На відміну від домінуючих сьогодні загальноприйнятних технологічних пріоритетів, доведено, що в основі розвитку СЕБП повинно лежати систематичне покращення цифрових компетентностей суб'єктами безпеки. Авторська позиція спирається на результати дослідження, проведеного експертним методом, ціллю якого було з'ясування фактичних засад здійснення безпекової діяльності широкого кола підприємств різних видів економічної діяльності, зокрема і ВПП, отримання оцінки перебігу ЦТП та тих загроз, що виникають під час цього процесу. Виявлено, що серед інших ключовою загрозою для ЕБП, що пов'язані із ЦТ, є така як «недостатній рівень цифрових компетенцій у працівників».

4. Сформовано методичні засади розвитку СЕБП, які спираються на авторське тлумачення цифрових компетентностей суб'єктів безпеки як знання, уміння, навички та здібності, що набуваються упродовж життя в процесі навчання та їх практичного застосування, які уможливають виконання завдань в сфері безпекової діяльності. Запропоновано для практичного застосування рівні таких компетентностей, що відповідає рамці DigComp 2.1 та враховує специфіку безпекової діяльності. Уточнено предметну площину

застосування цифрових компетентностей за основними функціональними складовими ЕБП та акцентовану увагу, що їх формування й розвиток повинен здійснюватися на постійній основі упродовж життя в сучасних умовах високих темпів ЦТЕ.

5. Створено основу практичної реалізації заходів стосовно розвитку СЕБП, що відбулося завдяки здійсненню моделювання, використовуючи метод IDEF0. Згідно з базовими умовами реалізації такого моделювання, було визначено основні процеси та підпроцеси, що відповідають суті раніше сформованого уявлення про теоретико-методичні аспекти розвитку СЕБП. Створені декомпозиції першого та другого порядку дають чітке уявлення стосовно послідовності виконання, відповідальних суб'єктів та необхідних умов для здійснення розвитку СЕБП. В цілому отримані результати моделювання слугують основою для практичного застосування теоретичних розробок без обмежень щодо виду економічної діяльності та масштабів діяльності підприємства з орієнтацією на своєчасне внесення змін у безпекову діяльність відповідно до тенденцій ЦТЕ та перспектив ЦТП.

Основні наукові результати опубліковані в працях: [98; 175; 180-182; 185; 192]

ВИСНОВКИ

1. Встановлено, що поточна діяльність підприємств характеризується і здійснюється під впливом різних трансформацій. З'ясовано зміст трансформації з позиції забезпечення безпеки будь-якої соціально-економічної системи, що дозволило деталізувати сутність трансформації на макрорівні через вплив промислових революцій, зокрема четвертої, за якої поширилися процеси цифрової трансформації. Обґрунтовано, що пасивність підприємства в питаннях цифрової трансформації в сучасних умовах провокує втрату конкурентних позицій із подальшим ймовірним припиненням діяльності через невідповідність темпам цифрової трансформації економіки. Систематизовано широкий перелік нових ринкових можливостей, ризиків і загроз, що спричинені цифровою трансформацією на різних рівнях управління, та є обов'язковим інформаційним підґрунтям для розвитку системи економічної безпеки підприємства.

2. Проведено комплексне дослідження з метою осучаснення трактування таких базових трактувань як «виклик», «ризик» та «загроза», що у поєднанні із характером змін у діяльності підприємства під час цифрової трансформації дало змогу переглянути парадигму розвитку підприємства із доведенням пріоритетності випереджаючого розвитку системи економічної безпеки підприємства. Сформовано концептуальне підґрунтя розвитку системи економічної безпеки підприємства, яке, спираючись на зміст зовнішніх і внутрішніх змін та можливих варіантів розвитку, визначає етапність процедури розроблення та виконання програми розвитку, яка передбачає здійснення кількісно-якісних заходів задля посилення захищеності підприємства та покращення конкурентних позицій.

3. З'ясовано, що більшість відомих сьогодні підходів до оцінювання економічної безпеки підприємства передбачають констатацію факту про певний рівень безпеки та, в окремих випадках, характеристику результативності дій суб'єктів безпеки, що загалом не визначає характер змін у безпековій

діяльності. Розроблено теоретико-методичний підхід, який передбачає встановлення рівня п'ятнадцяти якісних індикаторів, котрі визначають зміну основних параметрів системи економічної безпеки в динаміці та відносно зрушень у зовнішньому та внутрішньому середовищі, із подальшим їх об'єднанням у п'ять груп та розрахунком інтегрального показника, значення якого становить необхідну інформаційну основу для розроблення й контролю за виконанням програми розвитку.

4. Розроблено модель підсистеми інформаційного забезпечення, в межах якої визначено характер змін, які необхідно провести стосовно існуючої в умовах кожного підприємства системи інформаційного забезпечення управління, та встановлено зміст обов'язкових складових такої системи (функції, принципи, механізм роботи з інформацією, об'єкти й суб'єкти, технічні засоби, програмне забезпечення, технології, інформаційне забезпечення), що дає змогу отримувати якісні та своєчасні відомості для планування, організації, мотивації та контролю за розвитком системи економічної безпеки підприємства.

5. Сформовано механізм управління розвитком, який, разом із іншими складовими механізми забезпечення економічної безпеки підприємства, завдяки змістовому наповненню методичної основи дієвості (методи, засоби впливу, забезпечення) за основними етапами реалізації (діагностика, оцінювання, планування, реалізація, контроль) має цільове спрямування на систематичне трансформування системи економічної безпеки підприємства відповідно до тенденцій цифрової трансформації економіки та на випередження згідно із цифровою трансформацією підприємства.

6. Проведено комплексне дослідження безпекової діяльності в умовах українських підприємств, результати якого вказують на домінування серед інших загроз, що виникають під час цифрової трансформації підприємства, такої, яка пов'язана із недостатнім рівнем цифрових компетенцій у працівників. Розроблено методичні засади, які, зважаючи на характер впливу цифрової трансформації на основні функціональні складові економічної безпеки

підприємства, передбачають систематичне оцінювання та покращення цифрових компетентностей суб'єктів безпеки, що повинно забезпечити розвиток системи економічної безпеки підприємства.

7. Розроблено науково-практичний підхід, що, послуговуючись методом функціонального моделювання IDEF0, дає змогу цілісно представити етапність підготовки, розроблення й виконання програми розвитку системи економічної безпеки підприємства. Врахування кращих практик безпекової діяльності українських підприємств, збагачених досвідом дієвості під час COVID-19 та військових дій, та баченням засад цифрової трансформації, які уже реалізуються в національній економіці на основі наслідування економічно розвинутих країн, дало змогу провести моделювання, яке може бути практично застосовано в умовах будь-якого підприємства в цілях розвитку його системи економічної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Академічний тлумачний словник української мови. URL: <http://sum.in.ua/s>. (дата звернення 29.05.2022)
2. Азаренкова Г. М., Майборода А. В. Особливості формування підсистеми інформаційного забезпечення системи фінансової безпеки суб'єкта господарювання. *БізнесІнформ*. 2020. № 1. С. 210–217.
3. Апалькова В. В. Концепція розвитку цифрової економіки в Євросоюзі та перспективи України. *Вісник Дніпропетровського університету. Серія «Менеджмент інновацій»*. 2015. № 4. С. 9–18.
4. Балабанов І. Т. Ризик-менеджмент. Київ : Простір, 1996. 192 с.
5. Барановський О. І. Зміст трансформаційних процесів в економічних системах. *Вісник університету банківської справи*. 2017. № 1 (28). С. 3–14.
6. Береза З. В. Суть та складова економічної безпеки підприємства. *Наука й економіка*. 2009. № 4 (т. 2). С. 59–64.
7. Бичкова Н. В. Стійкість розвитку сучасної корпорації у контексті системно-синергетичного підходу. *Вісник Хмельницького національного університету. Економічні науки*. 2010. № 3. Т. 2. С. 90–93.
8. Бір С. Т. Мозок фірми / перекл. з англ. М. М. Лопухіна. Київ : Квітник-К, 2005. 416 с.
9. Боднар О. Цифровізація та конкурентоспроможність бізнесу – ключові драйвери розвитку української економіки. *Бізнес*. URL: <https://business.ua/litsa/item/2452-tsifrovizatsiyata-konkurentospromozhnist-biznesu-klyuchovi-drajverirozvitku-ukrajinskoji-ekonomiki> (дата звернення: 29.03.2022)
10. Бодрук О. С. Структура воєнної безпеки: національний та міжнародний аспекти: монографія. Київ: НПІМБ, 2001. 300 с.
11. Бондарь Н. Н. Сучасні тенденції розвитку підприємств. URL: <http://https://www.education.ua/blog/8047/> (дата звернення 28.08.2022)
12. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ : ТОВ «СІКГРУПУКРАЇНА», 2015. 449 с.

13. Васильців Т. Г. Узагальнення концептуальних основ економічної безпеки підприємства. *Науковий вісник НЛТУ України*. 2011. № 21.2. С. 153–158.
14. Васильців Т. Г., Баран Р. Я. Інструменти протидії системній корупції: аспекти економічної безпеки бізнесу. *Вісник Хмельницького національного університету. Серія економічна*. 2023. № 3. С. 318–322. URL: <http://journals.khnu.km.ua/vestnik/wp-content/uploads/2023/07/2023-318-49.pdf>. (дата звернення 29.11.2023)
15. Васильців Т. Г., Баран Р. Я. Напрями зниження рівня корупції як системної перешкоди забезпечення економічної безпеки суб'єктів підприємництва. *Академічні візії*. 2023. № 20. URL: <https://academy-vision.org/index.php/av/article/view/472/428>. (дата звернення 29.11.2023)
16. Васильців Т. Г., Куницька-Іляш М. В. Стан та проблематика економічної безпеки підприємств реального сектора економіки України. *Вісник Хмельницького національного університету. Серія Економічні науки*. 2022. № 3. С. 327–334. <https://doi.org/10.31891/2307-5740-2022-306-3-50> URL: <http://journals.khnu.km.ua/vestnik/wp-content/uploads/2022/07/2022-306-50.pdf>. (дата звернення 29.11.2023)
17. Васильців Т. Г., Лупак Р. Л., Куницька-Іляш М. В., Наконечна Н. В. Економічна безпека суб'єктів господарювання та держави: аспект гарантування фінансово-економічної безпеки пріоритетних галузей національної економіки України. *Наукові записки Львівського університету бізнесу та права*. 2023. № 37. С. 22–30. URL: <https://nzlubp.org.ua/index.php/journal/article/view/739/676>. (дата звернення 29.11.2023)
18. Великий економічний словник / укл. С. С. Іванов, Д. Ю. Кочетков. Київ : Видав-пол, 2005. 620 с.
19. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ : Ірпінь : ВТФ «Перун», 2009. 1736 с.
20. Веселовский В. Н. Про сутність живої матерії. Київ : Думка, 2011. 296 с.

21. Владленова І. В. Народження Четвертої хвилі: нанотехнологічне суспільство. *Практична філософія*. 2009. № 3 (33). С. 14–18.
22. Вовк О. М. Управління розвитком системи економічної безпеки підприємства: теоретичні аспекти. *Приазовський економічний вісник*. 2018. № 6(11). С. 125–129.
23. Гальчинський А. С. Глобальні трансформації: концептуальні альтернативи. Методологічні аспекти. Київ : Либідь, 2006. 312 с.
24. Гладченко Т. М. Індикатори економічної безпеки підприємницької діяльності. Донецьк : ДОНДАУ «Менеджер», 2000. № 12. С. 111–114.
25. Гобела В. В. Теоретичний аналіз екологізації як суспільно-економічного феномену. *Ефективна економіка*. 2019. № 6. URL: <http://www.economy.nauka.com.ua/?op=1&z=7114> (дата звернення 29.11.2023)
26. Гобела В. В., Дудюк В. С., Гобела В. М. Забезпечення еколого-економічної безпеки у посткризовий період. *Науковий вісник НЛТУ України*. 2021. № 5. С. 79–83.
27. Гобела В. В., Мельник С. І., Курляк М. Д. Продовольча безпека України на фоні війни: оцінка стану та прогнозування тенденцій. *Цифрова економіка та економічна безпека*. 2022. № 2. С. 92–98.
28. Гончаров С. М., Кушнір Н. Б. Глумачний словник економіста / за ред. проф. С. М. Гончарова. Київ : Центр учб. літ., 2009. 264 с.
29. Гончарук О. В., Бабенко А. А. Стан і перспективи розвитку підприємств поліграфічної промисловості в Україні та світі. *Молодий вчений*. 2018. № 1(53). С. 864–868.
30. Гудзь О. Є. Цифрова економіка: зміна цінностей та орієнтирів управління підприємствами. *Економіка. Менеджмент. Бізнес*. 2018. № 2(24). С. 4–12.
31. Гудзь О. Є., Маковій В. В. Концептуальні основи формування інформаційної політики підприємств. *Науковий вісник Ужгородського національного університету*. 2019. Вип. 23. С. 65–69.

32. Денисенко М. П., Голубєва Т. С., Колос І. В. Інформаційне забезпечення інноваційно-інвестиційної діяльності підприємства. *Вісник НУ «Львівська політехніка»*. 2009. № 647. С. 43–49.
33. Денисенко М. П., Колос І. В. Інформаційне забезпечення ефективного управління підприємством. *Економіка і держава*. 2006. № 7. С. 19–24.
34. Дерій Ж. В., Базилевич В. М. Напрями підвищення економічної безпеки підприємств АПК. Сучасні технології управління на підприємстві: колективна монографія / під заг. ред. К. Ф. Ковальчука. Донецьк : ЛАНДОН-XXI, 2013. С. 96–109.
35. Дєєва Н. Е., Делейчук В. В. Механізми залучення інвестицій емітентами в умовах розвитку цифрової економіки. Київ : Молодий вчений, 2018. 670 с.
36. Довбня С. Б., Гічова Н. Ю. Діагностика рівня економічної безпеки підприємства. *Фінанси України*. 2008. № 4. С. 88–97.
37. Донець Л. І., Ващенко Н. В. Економічна безпека підприємства : навч. посіб. Київ : ЦУЛ, 2008. 240 с.
38. Дороніна М. С. Управління економічними та соціальними процесами підприємства : монографія. Харків : ХДЕУ, 2002. 431 с.
39. Дубецька С. П. Економічна безпека підприємства України. *Недержавна система безпеки підприємництва як суб'єкт національної безпеки України* : зб. наук.-практ. конф. (Київ, 16–17 травня 2001 р.). Київ, 2003. С. 146–172.
40. Дурняк Б. В., Штангрет А. М., Мартинів В. В. Стан і тенденції розвитку підприємництва у видавничо-поліграфічній галузі. *Наукові записки*. 2008. № 2(14). С. 77–82.
41. Дяченко К. С. Методичні підходи до оцінки рівня економічної безпеки підприємств будівельної галузі. *Вісник ВНУ*. 2015. № 4(5). С. 31–36.
42. Економіка підприємства : навч. посіб. / за ред. С. Ф. Покропивного. Київ : КНЕУ, 2000. 528 с.

43. Економічна безпека підприємств, організацій та установ / Ортинський В. Л., Керницький І. С., Живко З. Б., Керницька М. І., Живко М. О. Київ : Правова єдність, 2009. 544 с.
44. Економічна енциклопедія : у 3 т. – Т. 3. (Поручництво) – Я (Японський центр продуктивності). П – Я / ред. : Б. Д. Гаврилишин, С. В. Мочерний. Київ : Акад., 2002. 952 с.
45. Єрмейчук Р. А. Обґрунтування стратегії сталого розвитку підприємства. *Економіка розвитку*. 2002. № 2 (22). С. 56–60.
46. Єрмошенко М. М. Фінансова безпека держави: національні інтереси держави, реальні загрози, стратегія забезпечення. Київ : КНТЕУ, 2001. 309 с.
47. Єрохін С. А. Структурна трансформація національної економіки (теоретико-методологічний аспект) : монографія. Київ : Світ знань, 2002. 528 с.
48. Єрохіна Є. А. Теорія економічного розвитку (системно-самоорганізаційний підхід). Черкаси : Вид-во Дім, 1999. 160 с.
49. Єфімова М. П. Інтерактивна дитяча книга в Україні: становлення та перспективи. *Українська культура: минуле, сучасне, шляхи розвитку*. 2013. №19. С. 13–16.
50. Живко З. Б. Механізм управління системою економічної безпеки підприємства. *Науковий вісник Ужгородського університету. Сер. Економіка*. 2014. Вип. 3 (44). С. 37–42.
51. Завадський Й. С., Осовська Т. В., Юшкевич О. О. Економічний словник. Київ : Кондор, 2006. 355 с.
52. Занора В. Розвиток підприємства: сутність, форми, види. *Галицький економічний вісник*. 2019. № 6(61). С. 69–78.
53. Занора В., Куценко Д., Одородько Н. Потенціал як основа розвитку підприємства: понятійно-категоріальний апарат. *Проблеми і перспективи економіки та управління*. 2019. № 2(18). С. 40–51.
54. Захаров О. І. Теоретичні основи забезпечення економічної безпеки підприємств. *Вчені записки університету «КРОК»*. 2012. № 32. С. 80–86.

55. Зурян О. В. Економічна сутність та класифікація фінансових ризиків. *Наукові праці МАУП*. 2016. Вип. 50(3). С. 141–146.
56. Зязюн І. А. Філософія поступу і прогнозу освітньої системи / Педагогічна майстерність : проблеми, пошуки, перспективи : монографія. Київ ; Глухів : РВВ ГДПУ, 2005. С. 8–10.
57. Зятковський І. Бюджетування як основа провадження контролінгу на підприємстві. *Актуальні проблеми економіки*. 2003. № 4. С. 48–51.
58. Іванова В. В. Щодо формування системи інформаційного забезпечення розвитку економіки України. *Економіст*. 2008. № 4. С. 61–63.
59. Іванов В. Л. Управління економічною стійкістю промислових підприємств на прикладі підприємств машинобудівного комплексу : монографія. Луганськ : СНУ ім. В. Даля, 2005. 268 с.
60. Іванченко Н. О., Кудрицька Ж. В., Рекачинська К. В. Бізнес-моделі в умовах цифрових трансформацій. *Вчені записки ТНУ імені В. В. Вернадського. Серія: Економіка і управління*. 2020. № 3. С. 185–190.
61. Ілляшенко О. В. Механізм системи економічної безпеки підприємства : монографія. Харків : Мачулін, 2016. 503 с.
62. Іляш О. І., Смоляр Л. Г., Дученко М. М., Джадан І. М. Стратегічні пріоритети державної політики стимулювання промислово-технологічного розвитку національної економіки України на засадах маркетингу в цілях забезпечення економічної безпеки. *Проблеми економіки*. 2022. Вип. № 1. С. 41–50.
63. Кабмін схвалив Концепцію розвитку цифрових компетентностей до 2025 року. URL: <https://thedigital.gov.ua/news/kabmin-skhvaliv-kontseptsiyu-rozvitku-tsifrovikh-kompetentnostey-do-2025-roku> (дата звернення: 15.02.2022)
64. Калетнік Г. М., Лутковська С. М. Структура фінансування та моніторингу заходів забезпечення екологічної безпеки. *Агросвіт*. 2020. № 9. С. 10–19.
65. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посіб. Київ : Атіка, 2005. 432 с.

66. Квілінський О. О. Інформаційне забезпечення управління розвитком промислового підприємства в умовах інформаційної економіки. *Економіка та управління підприємствами*. 2019. № 8. С. 73–79.
67. Кірюхін Д. І. Вступ до філософії релігії Гегеля. Філософія як спекулятивна теологія. Київ : ПАРАПАН, 2009. 204 с.
68. Ковальов Д., Сухорукова Т. Економічна безпека підприємства. *Економіка України*. 1998. № 5. С. 48–52.
69. Ковальчук А. М. Фінансово-економічна безпека підприємства в контексті адаптації до викликів цифрового середовища. *Економіка підприємства*. 2020. № 3. С. 152–159.
70. Козаченко Г. В. Естиметологічний аспект в економічній безпекології. *Проблеми економіки*. 2016. № 1. С. 167–173.
71. Козаченко Г., Пономарьов В. Економічна безпека підприємств : сутність і передумови формування. Теорія та практика управління у трансформаційний період. Донецьк : ІЕП НАН України, 2001. Т. 3. С. 3–7.
72. Козловський С. В. Управління сучасними економічними системами, їх розвитком та стійкістю : моногр. Вінниця : Меркьюрі-Поділля, 2010. 432 с.
73. Колодизев О. М., Нужний К. М. Дослідження сутності та змісту економічної стійкості підприємства. *Комунальне господарство міст*. 2007. № 78. С. 238–243.
74. Коляденко С. В. Цифрова економіка: передумови та етапи становлення в Україні та світі. *Економіка. Фінанси. Менеджмент: актуальні питання науки і практики*. 2016. № 6. С. 105–112.
75. Копитко М. І. Економічна безпека підприємств з виробництва транспортних. Львів : Ліга-Прес, 2015. 556 с.
76. Копитко М. І., Ільків Ю. І. Управління безпековою діяльністю інноваційно-активних підприємств. *Соціально-правові студії*. 2020. Випуск 3 (9). С. 162–172.
77. Корнєв Ю. Г. Інформаційне забезпечення розвитку підприємницької діяльності. *Вісник НАН України*. 2008. № 5. С. 24–31.

78. Котелевець Д. О. Тенденції розвитку цифрової економіки в Україні. *Проблеми сучасних трансформацій*. 2022. № 5. URL : <https://reicst.com.ua/pmt/article/view/2022-5-03-01> (дата звернення 04.06.2023)
79. Кривак А. П. Теоретичні принципи секторального структурування національної економіки. *Агросвіт*. 2010. № 13. С. 42–47.
80. Кристиняк М. Основні теоретичні аспекти забезпечення економічної безпеки малих підприємств в Україні. *Ефективна економіка*. 2018. № 4. URL: <http://www.economy.nauka.com.ua/?op=1&z=6260> (дата звернення 27.08.2022)
81. Кузьмін О. Є., Георгіаді Н. Г. Формування і використання інформаційної системи управління економічним розвитком підприємства : монографія. Львів : Вид-во НУ «Львівська політехніка», 2006. 368 с.
82. Кузьомко В. М. Концептуальні підходи до виокремлення функціональних складових економічної безпеки підприємства. *Формування ринкової економіки*. 2011. № 26. С. 206–216.
83. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник НАДУ при Президентові України (Серія «Державне управління»)*. 2018. Вип. 1. С. 5–10.
84. Кустовська О. В. Методологія системного підходу та наукових досліджень. Тернопіль : Екон. думка, 2005. 124 с.
85. Линьов К. О. Інформаційне забезпечення державного управління та державної служби. Київ : Київський університет імені Бориса Грінченка, 2016. 42 с.
86. Лігоненко Л. О., Селезова М. В. Інформаційне забезпечення аналізу інноваційної діяльності підприємств в Україні: стан, проблеми, шляхи їх розв'язання. *Глобальні та національні проблеми економіки*. 2017. Вип. 20. С. 415–417.
87. Ліпкан В. А. Національна безпека України. Київ : Кондор, 2006. 552 с.

88. Лучик Г. М. Сутність інформації у системі прийняття управлінських рішень. *Наукові праці Таврійського державного агротехнічного університету*. 2013. № 2(4). С. 185–195.

89. Любченко Н. Л. Сканування загроз як складова управління стабільності підприємства. *Вісник Хмельницького національного університету*. 2009. № 4. Т. 2. С. 227–231.

90. Ляшенко О. М. Категорії управління економічною безпекою підприємства. *Вчені записки Університету «КРОК»*. 2011. Вип. 27 (2). С. 17–22.

91. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства : монографія. Луганськ : Вид-во СНУ ім. В. Даля, 2011. 400 с.

92. Марина А. С., Єланська Н. О., Петренко М. А. Механізм забезпечення економічної безпеки суб'єктів господарювання. *Економіка та суспільство*. 2018. № 19. С. 495–500.

93. Марченко В. М. Методичний підхід до оцінки стійкості корпорації до зовнішніх флуктуацій. *Актуальні проблеми економіки*. 2010. № 3. С. 155–162.

94. Матвійченко О. С. Концепція індустрії 4.0: зміст, можливості та ризики. *Бізнесінформ*. 2018. № 12. С. 91–99.

95. Мельник С. І. Дослідження викликів, ризиків, загроз та небезпеки в системі забезпечення фінансової безпеки підприємства. *Проблеми системного підходу в економіці*. 2019. № 4(72). С. 172–177.

96. Мельник С. І. Основні чинники впливу на фінансову стабільність в контексті управління фінансовою безпекою підприємства. *Проблеми системного підходу в економіці*. 2019. Вип. 5/73. Ч. 2. С. 92–97.

97. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика : монографія. Львів : «Растр-7», 2020. 384 с.

98. Мельник С. І., Штангрет І. А. Методичні засади розвитку системи економічної безпеки підприємства. *Ефективна економіка*. 2024. №1. URL:

<https://www.nayka.com.ua/index.php/ee/article/view/2863/2899>

DOI:

<http://doi.org/10.32702/2307-2105.2024.1.17>

99. Мескон М., Альберт М., Хедоурі Ф. Основи менеджменту. Київ : Вид-во «Справа», 1997. 704 с.
100. Методологія операціоналізації основних понять національної безпеки: гуманітарна складова. *Політичний менеджмент*. 2006. № 3. С. 21–34.
101. Моделювання економічної безпеки: держава, регіон, підприємство: монографія / [В .М. Геєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк та ін.]; за ред. В. М. Гейця. Харків : ВД «ІНЖЕК», 2006. 240 с.
102. Наливайко О. О. Цифрова компетентність: сутність поняття та динаміка його розвитку. Компетентнісний підхід у вищій школі: теорія та практика. 2021. URL: https://www.researchgate.net/publication/354234675_CIFROVA_KOMPETENTNIST_SUTNIST_PONATTA_TA_DINAMIKA_JOGO_ROZVITKU (дата звернення 15.12.2022)
103. Нікітченко Т. О. Синергетичний підхід до управління змінами на підприємстві. *Агросвіт*. 2015. № 23. С. 58–61.
104. Новий тлумачний словник української мови : у 4-х т. Т. 4. / укл. проф. В. В. Яремко, к. філ. н. О. М. Сліпущко. Київ : Аконіт, 1998. 944 с.
105. Онищук М., Татарінова Л. Деякі тенденції книгодрукування та книгорозповсюдження у світі в умовах пандемії COVID-19. *Вісник книжкової палати*. 2021. № 9. С. 6–10.
106. Опис рамки цифрової компетентності для громадян України DigCompUA for Citizens 2.1. Міністерство цифрової трансформації. 2021. 56 с. URL: <https://cutt.ly/zn1DbLC> (дата звернення: 15.12.2022).
107. Орлик О. В. Інформаційні системи в сфері управління організацією. *Вісник соціально-економічних досліджень*. 2002. Вип. 12. С. 188–191.
108. Остапчук О. Ефективні педагогічні системи: Інноваційна стратегія проектування. *Рідна школа*. 2005. № 8. С. 16–19.

109. Палагута С. С. Особливості інформаційного забезпечення управління підприємств і організацій. *Глобальні та національні проблеми економіки*. 2017. Вип. 16. С. 418–421.

110. Пепредерій Т. С. Стратегія цифрової безпеки підприємства як драйвер цифрової трансформації економіки України. *Вісник економічної науки України*. 2019. № 2. С. 201–204.

111. Петренко С. М. Інформаційне забезпечення внутрішнього контролю господарських систем : монографія. Донецьк: Вид-во ДНТУ, 2007. 290 с.

112. Пілінський В. В. Визначення пріоритетних напрямків розвитку цифрової економіки в Україні. URL: http://nbuv.gov.ua/UJRN/Nzundiz_2016_2_9 (дата звернення: 29.03.2022)

113. Поверляк Т. І. Визначення понять «економічна стабільність» та «економічна стійкість». *Соціум. Наука. Культура* : матеріали дев'ятої Міжнародної науково-практичної інтернет-конференції (24–26 січня 2012 р. м. Київ). Київ, 2013. 156 с.

114. Подлужна Н. О. Організація управління економічною безпекою підприємства : авторефер. дис. ... канд. екон. наук : 08.06.01. НАН України ; Інститут економіки промисловості. Донецьк, 2003. 20 с.

115. Пойда-Носик Н. Визначення сутності механізму забезпечення фінансової безпеки суб'єктів підприємництва. *Вісн. Ун-ту банків. справи Нац. банку України*. 2012. № 1. С. 25–33.

116. Пойда-Носик Н. Н. Науково-методичні підходи до оцінки рівня фінансової безпеки підприємства. *Теоретичні і практичні аспекти економіки та інтелектуальної власності*. 2013. № 1. С. 288–292.

117. Політологічний енциклопедичний словник / упоряд. В. П. Горбатенко ; за ред. Ю. С. Шемшученка, В. Д. Бабкіна, В. П. Горбатенка ; 2-е вид., доп. і перероб. Київ : Генеза, 2004. 736 с.

118. Поліщук О. Б. Інформаційно-аналітичне забезпечення управління економічною безпекою підприємства. *Ефективна економіка*. 2022. № 7. URL:

<https://www.nayka.com.ua/index.php/ee/article/view/165/165> (дата звернення 13.11.2023)

119. Поліщук О. Б. Моделювання забезпечення функціонування адаптивно-орієнтованої системи управління економічною безпекою промислового підприємства. *Інфраструктура ринку*. 2022. № 67. С. 136–142.

120. Пономаренко В. С., Тридід О. М., Кизим М. О. Стратегія розвитку підприємства в умовах кризи: монографія. Харків: Вид. Дім «ІНЖЕК», 2003. 328 с.

121. Пригунов П. Я. Особливості використання сучасних концепцій управління в системі забезпечення економічної безпеки підприємств. *Європейські перспективи*. 2013. № 11. С. 103–108.

122. Присяжнюк П. В. Механізм управління: сутність, види та складові. *Ефективна економіка*. 2019. № 12. URL: <http://www.economy.nayka.com.ua/?op=1&z=7539> (дата звернення 26.08.2022)

123. Про затвердження Національної економічної стратегії на період до 2030 року : Постанова Кабінету Міністрів України № 179 від 03.03.2021 р. URL: <https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#Text> (дата звернення 04.06.2023)

124. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: <https://www.kmu.gov.ua/ua/npas/pro-shvalennya-konceptsiyirozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planuzahodiv-shodo-yiyi-realizaciyi> (дата звернення: 29.03.2022).

125. Прогноз розвитку світової економіки до 2030Е. Український інститут майбутнього. URL: <https://strategy.uifuture.org/prognoz-rozvitku-svitovoi-ekonomiki-do-2030e.html> (дата звернення 04.06.2023)

126. Проект Плану відновлення України. Матеріали робочої групи «Відновлення та розвиток економіки». URL:

<https://www.kmu.gov.ua/diyalnist/nacionalna-rada-z-vidnovlennya-ukrayini-vid-naslidkiv-vijni/robochi-grupi>. (дата звернення 04.06.2023)

127. Прохорова В. В. Економічний розвиток підприємств: теоретико-методологічний підхід : моногр. Харків : УкрДАЗТ, 2010. 523 с.

128. Раєвнева О.В. Управління розвитком підприємства: методологія, механізми, моделі: монографія. Харків: Вид-во «Вікторія», 2006. 496 с.

129. Райко Д. В. Визначення розвитку маркетингової діяльності промислового підприємства. *Маркетинг і менеджмент інновацій*. 2011. Т. 1. № 3. С. 109–117.

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

131. 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.

132. Саух І. В., Шиманська В. В., Момонт Т. В. Цифрова економіка України: сучасний стан, тенденції, проблеми розвитку. *Вісник Хмельницького національного університету*. 2019. Вип. 2. С. 228–234.

133. Серебрякова Н. А., Волкова С. А., Волкова Т. А. Формування системи забезпечення економічної безпеки підприємства. *Вісник ВДУИТ*. 2016. № 4. С. 460–465.

134. Силкін О. С. Формування класифікаційних підходів до визначення сутності фінансової безпеки підприємства в сучасних економічних умовах. *Науковий вісник Ужгородського університету. Серія «Економіка»*. 2018. Вип. 1 (51). С. 375–380.

135. Система економічної безпеки: держава, регіон, підприємство : монографія : в 3-х т. Т. 1 / О. М. Ляшенко, Ю. С. Погорелов, В. Л. Безбожний та ін.; за заг. ред. Г. В. Козаченко. Луганськ : Елтон-2, 2010. 282 с.

136. Смоляр Л. Г., Ляш О. І., Трофіменко О. О. Трансформаційні ефекти цифровізації у забезпеченні розвитку промислового виробництва в умовах Індустрії 4.0. *Підприємництво та інновації*. 2021. № 21. С. 24–30.
137. Сорочан О., Ігнатюк Д. Економічна безпека: стан і загрози в Республіці Молдова. *Zeszyty naukowe politechniki rzeszowskiej ekonomia i nauki humanistyczne*. 2002. № 3. Z. 19.
138. Сталінська О. В. Система економічної безпеки підприємства в умовах розвитку цифрової економіки. *Науковий вісник Міжнародного гуманітарного університету*. 2019. № 38. С. 80–86.
139. Статистична інформація. Державна служба статистики. URL: <https://www.ukrstat.gov.ua/> (дата звернення 03.06.2023)
140. Статистичний щорічник України 2022 / за ред. І. Є. Вернера. Київ : Державна служба статистики України, 2023. 447 с.
141. Сумін В. А. Стійкість системи управління підприємством за умов його економічної безпеки. *Дні науки : матеріали міжнародної науково-практичної конференції* (м. Донецьк, 24-25 березня 2001 р.). Донецьк : Дон. НТУ, 2001. С. 159–162.
142. Тарасов І. В. Технології індустрії 4.0. *Стратегічні рішення*. 2018. № 2. С. 62–69.
143. Ткачук Г. О. Концепція безпечності трансформаційних перетворень на підприємствах харчової промисловості. *Інформаційне суспільство: технологічний, економічний та технічний аспекти становлення : матеріали Міжн. наук. інт.-конф.* (14 листопада 2019 року, м. Київ). URL: <http://www.konferenciaonline.org.ua/arhiv-konferenciy/arhiv-konferenciy14-11-2019> (дата звернення 29.05.2022). 226 с.
144. Ткачук Т. Ю. Інформаційна безпека держави у національному законодавстві європейських країн. *Visegrad Journal on Human Rights*. 2018. № 1. С. 145–150.
145. Тур О. В. Формування поняття стратегія розвитку підприємства. *Інтелект XXI*. 2015. № 4. С. 38–45.

146. Узбек К. М. . Фрагменти побудови античної науки, філософії і культури. Донецьк : Східний видавничий дім, 2010. 234 с.
147. Українська енциклопедія: в 12-ти т. / гол. ред. М. П. Бажан; редкол. : О. К. Антонов та ін. 2-ге вид. Т. 9 : Поплужне-Салуїн. Київ : Голов. ред. УРЕ, 1983. 558 с.
148. Ус Г. О., Коваль О. О. Цифрова економіка, її розвиток та економічна характеристика. *Вісник Хмельницького національного університету*. 2021. № 6. С. 70–72.
149. Філіппова С. В., Дашковський О. С. Система формування і забезпечення економічної безпеки підприємства. *Економіка: реалії часу*. 2012. № 2 (3). С. 17–21. URL: <http://www.economics.opu.ua/n3.html>. (дата звернення 15.03.2022).
150. Філіпішин І. В. Механізм управління розвитком промислового підприємства. *Економіка промисловості*. 2011. № 4. С. 220–227.
151. Філософський енциклопедичний словник / за ред. В. І. Шинкарука. Київ : Абрис, 2002. 742 с.
152. Форд Г. Моє життя та робота. Київ : Наш формат, 2015. 344 с.
153. Фостяк В. І. Безпекова діяльність та безпековий потенціал підприємства. *Формування ринкових відносин в Україні*. 2018. № 3. С. 114–119.
154. Фостяк В. І. Формування механізму управління безпековою діяльністю промислових підприємств. *Ефективна економіка*. 2019. № 1. URL: <http://www.economy.nauka.com.ua> (дата звернення 12.12.2023)
155. Франчук В. І. Особливості організації системи економічної безпеки вітчизняних акціонерних товариств в умовах трансформаційної економіки : монографія. Львів : ЛьвДУВС, 2010. 440 с.
156. Франчук В. І. Теорія безпеки соціальних систем. Львів : ЛьвДУВС, 2016. 216 с.

157. Фролова Л. В. Механізми логістичного управління торговельним підприємством : монографія. Донецьк : ДонДУЕТ ім. М. Туган-Барановського, 2005. 322 с.
158. Хитра О. В. Синергетичний підхід до аналізу категоріального апарату зовнішньоекономічної діяльності. *Глобальні та національні проблеми економіки*. 2017. Вип. 17. С. 103–109.
159. Храмова-Баранова О. Л., Сікора Ю. А. Дизайн інтерактивних дитячих книжок та його вплив на розвиток дошкільної освіти і культури в Україні. *Гуманітарний вісник*. 2017. Вип. 11. С. 46–54.
160. Цал-Цалко Ю. С. Фінансова звітність підприємства та її аналіз. Київ : ЦУЛ, 2002. 359 с.
161. Цифрова економіка: тренди, ризики та соціальні детермінанти / кер. проекту О. Пищуліна. Київ : Центр Розумкова, 2020. 274 с.
162. Цікавська Н. Інтерпретація понять «виклик», «небезпека», «загроза» та «ризик» у теорії фінансової безпеки. *Фінансовий простір*. 2013. № 3(11). С. 110–114.
163. Чмерук Г. Г. Цифрова економіка як окремий сектор національної економіки держави. *Науковий вісник Ужгородського національного університету*. 2019. Вип. 27. С. 92–97.
164. Чужа О. Книжковий ринок Чехії в цифрах: видавництва, переклади URL: <http://litakcent.com/2016/06/23/knyzhkovyj-rynok-chehiji-v-cyfrah-vydavnyctvaperekklady/> (дата звернення 04.06.2023)
165. Шаванс Б. Еволюційний шлях від соціалізму. *Питання економіки*. 1999. № 6. С. 4–26.
166. Шаров Ю. П. Стратегічне планування в муніципальному менеджменті: концептуальні аспекти : монографія. Київ : УДАУ, 2001. 302 с.
167. Швайка Л. А. Видавничо-поліграфічна справа в Україні: стан, конкурентоспроможність, перспективи. *Поліграфія і видавнича справа*. 2011. № 2 (54). С. 15–24.

168. Шеркліф Е. Видавнича галузь України : Заключний звіт 2020 (лютий-березень 2021 року). URL: https://www.britishcouncil.org.ua/sites/default/files/333_research_uk_ua_v10.pdf (дата звернення 04.06.2021)
169. Шинкар С. М. Обліково-аналітичне забезпечення як складова управління економічної безпекою підприємства. *Глобальні та національні проблеми економіки*. 2018. № 22. С. 592–595. URL: <http://global-national.in.ua/issue-22-2018>. (дата звернення 13.11.2023)
170. Шинкаренко В. Г., Бурмака Н. М. Дослідження сутності поняття «розвиток соціально-економічної системи». *Економіка*. 2013. № 21. С. 73–86.
171. Шира Т. Б. Корпоративна безпека підприємств: теоретичні та прикладні аспекти : монографія. Львів : Укр. акад. друкарства, 2020. 364 с.
172. Шира Т. Б. Моделювання функціонування системи корпоративної безпеки підприємства. *Приазовський економічний вісник*. 2019. Вип. 6. (17). С. 228–232.
173. Шкуркіна В. М. Методологічні засади менеджменту соціокультурної діяльності. *Вісник ХДАК*. 2010. Вип. 29. С. 226–235.
174. Шликов В. Комплексне забезпечення економічної безпеки підприємства : монографія. Київ : Основа, 1999. 145 с.
175. Штангрет І. А. Безпекові аспекти управління мотивацією працівників промислових підприємств. *Соціально-економічний розвиток і безпека України: стан та перспективи* : матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Львів, 25 березня 2021 р.). Львів : Галицька видавнича спілка, 2021. С. 150–152.
176. Штангрет І. А. Безпекові аспекти цифрової трансформації промислових підприємств. *Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення* : матеріали ІХ Всеукраїнської науково-практичної конференції (м. Львів, 20–22 травня 2022 р.). Львів : УАД, 2022. С. 102–104.

177. Штангрет І. А. Інформаційне забезпечення розвитку системи економічної безпеки промислового підприємства в умовах цифрової трансформації економіки. *Східна Європа: економіка, бізнес та управління*. 2023. № 4 (41). С. 110–115. DOI: <https://doi.org/10.32782/easterneurope.41-17>. (дата звернення 29.11.2023)

178. Штангрет І. А. Концептуальне підґрунтя розвитку системи економічної безпеки підприємства. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні* : матеріали VIII Всеукраїнської науково-практичної конференції (м. Львів, 24–26 листопада 2022 р.). Львів : УАД, 2022. С. 136–138.

179. Штангрет І. А. Методичні засади забезпечення економічної безпеки підприємства. *Менеджмент і безпека: теоретичні та прикладні аспекти* : матеріали науково-практичної конференції (м. Львів, 13 травня 2022 р.). Львів: ЛьвДУВС, 2022. С. 127–129.

180. Штангрет І. А. Механізм забезпечення економічної безпеки підприємства. *Соціально-економічний розвиток і безпека України: стан та перспективи* : матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Львів, 23 березня 2023 р.). Львів : ЛьвДУВС, 2023. С. 151–153.

181. Штангрет І. А. Механізм управління розвитком системи економічної безпеки підприємства в умовах цифрової трансформації економіки. *Інфраструктура ринку*. 2023. № 71. С. 194–199. DOI: <https://doi.org/10.32782/infrastruct71-34>

182. Штангрет І. А. Механізм управління розвитком системи економічної безпеки підприємства: теоретичні засади. *Сучасні підходи до креативного управління економічними процесами* : матеріали XIV Міжнародної науково-практичної конференції (м. Київ, 13–14 квітня 2023 р.). Київ : НАУ, 2023. С. 231–233.

183. Штангрет І. А. Оцінювання розвитку системи економічної безпеки підприємства. *Інфраструктура ринку*. 2023. Вип. 74. С. 85–89. DOI: <https://doi.org/10.32782/infrastruct74-16>.

184. Штангрет І. А. Розвиток системи економічної безпеки в умовах цифрової трансформації підприємства. *Ефективна економіка*. 2022. №6. URL: <https://nauka.com.ua/index.php/ee/article/view/120>. DOI: 10.32702/2307-2105.2022.6.34 (дата звернення 29.11.2023)

185. Штангрет І. А. Розвиток системи економічної безпеки підприємства: необхідність та варіант реалізації. *Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення* : матеріали X Всеукраїнської науково-практичної конференції (м. Львів, 25–27 травня 2023 р.). Львів : УАД, 2023. С. 125–127.

186. Штангрет І. А. Система економічної безпеки підприємства: теоретичний базис формування. *Сучасні підходи до креативного управління економічними процесами* : матеріали XIII Міжнародної науково-практичної конференції (м. Київ, 14–15 квітня 2022 р.). Київ : НАУ, 2022. С. 122–124.

187. Штангрет І. А. Система інформаційного забезпечення безпекової діяльності підприємства. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні* : матеріали IX Всеукраїнської науково-практичної конференції (м. Львів, 23–26 листопада 2023 р.). Львів : УАД, 2023. С. 192–194.

188. Штангрет І. А. Теоретичні засади формування системи економічної безпеки підприємства. *Ефективна економіка*. 2022. № 4. <http://www.economy.nauka.com.ua/?op=1&z=10173> (DOI: 10.32702/2307-2105-2022.4.150) (дата звернення 29.11.2023)

189. Штангрет І. А. Трансформаційні процеси в діяльності підприємств видавничо-поліграфічної галузі. *Держава та регіони*. 2023. № 2 (128). С. 50–55. DOI: <https://doi.org/10.32782/1814-1161/2023-2-7>.

190. Штеден Ф., Кіхнер Р. Індустрія 4.0 – огляд та наслідки для політики. *Docplayer*. 2018. URL: <https://docplayer.net/121254108-Industriya-4-0-oglyadta-naslidki-dlya-politiki.html> (дата звернення 12.12.2023)
191. Яненко І. Г. Чинники і шляхи розвитку цифровізації в Україні. *Економіка України*. 2022. № 3. С. 4–22.
192. Andriyiv N., Pushak H., Petrukha N., Kokhan V., Shtangret I. Transformation of threats to demographic security and sustainable development of the region due to increased military actions. *International Journal of Sustainable Development and Planning*. 2022. Vol. 17. No. 7. P. 2221–2227. DOI: <https://doi.org/10.18280/ijspd.170722>. (дата звернення 12.12.2023)
193. Bertalanfy L. von. General system theory. Foundations, development applications. N.Y. : Braziller, 1969. 483 p.
194. Encyclopedia of Information Science and Technology, Fourth Edition (10 Volumes). IGI Global, June, 2017. 8104 p.
195. English Oxford living Dictionaries. URL: <https://en.oxforddictionaries.com/definition/challenge>. (дата звернення 30.05.2022)
196. European Union. Recommendation of the European Parliament and to the Council of 18 December 2006 on key competences for lifelong learning (2006/962/EC). *Official Journal of the European Union*. 2006. URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:394:0010:0018:EN:PDF> (дата звернення 15.02.2022)
197. Global Innovation Index 2022. WIPO. URL: <https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf> (дата звернення 04.06.2023)
198. Global Innovation Index 2023. WIPO. URL: <https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023-section1-en-gii-2023-at-a-glance-global-innovation-index-2023.pdf> (дата звернення 12.12.2023)
199. Ilyash O., Lupak R., Dzhadan I., Kolishenko R. Assessing structural components of investment and innovation provision of economic security in the basic

types of economic activity. *Journal of Economy Culture and Society*. 2021. Vol. 63. P. 17–37.

200. Ilyash O., Lupak R., Kravchenko M., Trofymenko O., Duliaba N., Dzhadan I. A forecasting model for assessing the influence of the components of technological growth on economic security. *Business: Theory and Practice*. 2022. Vol. 23(1). P. 175–186. URL: <https://journals.vilniustech.lt/index.php/BTP/article/view/15298>.

201. Industrie 4.0 in a Global Context Strategies for Cooperating with International Partners / H. Kagermann, R. Anderl, J. Gausemeier, G. Schuh, W. Wahlster (Eds.); acatech STUDY. Herbert Utz Verlag GmbH, 2016. 74 p.

202. Kenneth E.F., Watt. N.Y. Systems analysis in ecology. London: Accad. Press, 1996. 710 p.

203. Margherio, L. et al. The Emerging Digital Economy, Department of Commerce, Washington, DC. 1999. URL: http://www.esa.doc.gov/sites/default/files/emergingdig_0.pdf (дата звернення 12.12.2023).

204. Negroponte, N. Being Digital. NY : Knopf, 1995. 256 p.

205. OECD Science, Technology and Industry: Scoreboard, Edition 2005. URL: http://www.oecdilibrary.org/oecd/content/book/sti_scoreboard-2005-en (дата звернення: 01.04.2022).

206. Tapscott D. (1995). The Digital Economy: Promise and Peril in the Age of Networked Intelligence. McGrawHill, 342. (дата звернення 12.12.2023)

207. The Concept of a ‘Digital Economy’. URL: <http://odec.org.uk/the-concept-of-a-digital-economy/> (дата звернення 29.03.2022)

208. The Future of Businesses and Jobs in Asia Pacific’s Digital Economy URL: <https://www.cognizant.com/FoW/the-work-ahead-asia-pacific.pdf> (дата звернення 12.12.2023)

209. Webster’s New International Dictionary Second Edition / William Allan Neilson – Editor in Chief. – Springfield, Mass., USA: Merriam Company, 1956. 3194 p.

210. What is Digital Transformation? Theagileelephant.com. website. URL: <http://www.theagileelephant.com/what-is-digital-transformation> (the date of application: 20.03.2022)

211. WIPO (2020). World intellectual property organization. URL: <https://www.wipo.int/portal/en> (дата звернення 04.06.2023);

212. World Digital Competitiveness Ranking. World Competitiveness Center. URL: <https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/> (дата звернення 04.06.2022)

ДОДАТКИ ДОДАТОК А

Таблиця А.1

Результати оцінювання розвитку СЕБП, на прикладі ТЗОВ «Кліше», розраховано автором

№	Показники	Роки			
		2019	2020	2021	2022
1	Економічна складова (0,2)	0,54 / 0,11	0,57 / 0,11	0,61 / 0,12	0,64 / 0,13
1.1	Рівень використання безпекового потенціалу (0,3)	0,45 / 0,14	0,53 / 0,16	0,58 / 0,17	0,68 / 0,2
1.2	Результативність дій суб'єктів безпеки (0,4)	0,61 / 0,24	0,64 / 0,26	0,72 / 0,29	0,75 / 0,3
1.3	Вмотивована активність суб'єктів безпеки (0,3)	0,54 / 0,16	0,51 / 0,15	0,5 / 0,15	0,48 / 0,14
2	Адміністративно-правова складова (0,2)	0,46 / 0,09	0,46 / 0,09	0,42 / 0,08	0,4 / 0,08
2.1	Внутрішня нормативна база забезпечення ЕБП (0,4)	0,53 / 0,21	0,52 / 0,21	0,5 / 0,2	0,48 / 0,19
2.2	Рівень правового захисту персоналу, менеджменту, власників (0,2)	0,38 / 0,08	0,35 / 0,07	0,32 / 0,06	0,3 / 0,06
2.3	Взаємодія із зовнішніми суб'єктами безпеки (0,4)	0,42 / 0,17	0,45 / 0,18	0,41 / 0,16	0,38 / 0,15
3	Інформаційно-аналітична складова (0,2)	0,57 / 0,11	0,6 / 0,12	0,63 / 0,13	0,66 / 0,13
3.1	Дієвість системи отримання, перевірки й оцінювання інформації (0,3)	0,58 / 0,17	0,6 / 0,18	0,59 / 0,18	0,68 / 0,2
3.2	Спроможність виявлення й розпізнавання факторів впливу на ЕБП (0,3)	0,48 / 0,14	0,51 / 0,15	0,54 / 0,16	0,61 / 0,18
3.3	Обґрунтованість управлінських рішень (0,4)	0,64 / 0,26	0,68 / 0,27	0,72 / 0,29	0,71 / 0,28
4	Техніко-технологічна складова (0,2)	0,54 / 0,11	0,52 / 0,1	0,53 / 0,11	0,54 / 0,11
4.1	Активність застосування цифрових технологій (0,3)	0,63 / 0,19	0,65 / 0,2	0,68 / 0,2	0,68 / 0,2
4.2	Оновлення матеріально-технічної бази безпекової діяльності (0,3)	0,54 / 0,16	0,5 / 0,15	0,48 / 0,14	0,41 / 0,12
4.3	Покращення технології безпекової діяльності (0,4)	0,47 / 0,19	0,43 / 0,17	0,48 / 0,19	0,54 / 0,22
5	Кадрова складова (0,2)	0,58 / 0,12	0,62 / 0,12	0,64 / 0,13	0,67 / 0,13
5.1	Цілеспрямованість дій суб'єктів безпеки (0,4)	0,52 / 0,21	0,57 / 0,23	0,6 / 0,25	0,65 / 0,26
5.2	Покращення цифрових та професійних компетентностей (0,3)	0,68 / 0,2	0,69 / 0,21	0,68 / 0,2	0,7 / 0,21
5.3	Злагодженість дій внутрішніх суб'єктів безпеки, зокрема і у взаємодії із зовнішніми (0,3)	0,57 / 0,17	0,59 / 0,18	0,63 / 0,19	0,68 / 0,2
	Інтегральний показник розвитку СЕБП	0,54	0,54	0,57	0,58

Таблиця А.2

**Результати оцінювання розвитку СЕБП,
на прикладі ТзОВ «Ельграф», розраховано автором**

№	Показники	Роки			
		2019	2020	2021	2022
1	Економічна складова (0,2)	0,6 / 0,12	0,58 / 0,12	0,64 / 0,13	0,72 / 0,14
1.1	Рівень використання безпекового потенціалу (0,3)	0,58 / 0,17	0,63 / 0,19	0,7 / 0,21	0,78 / 0,23
1.2	Результативність дій суб'єктів безпеки (0,4)	0,67 / 0,27	0,6 / 0,24	0,65 / 0,26	0,73 / 0,29
1.3	Вмотивована активність суб'єктів безпеки (0,3)	0,52 / 0,16	0,5 / 0,15	0,58 / 0,17	0,65 / 0,2
2	Адміністративно-правова складова (0,2)	0,55 / 0,11	0,5 / 0,1	0,57 / 0,11	0,63 / 0,13
2.1	Внутрішня нормативна база забезпечення ЕБП (0,4)	0,71 / 0,28	0,63 / 0,25	0,65 / 0,26	0,71 / 0,28
2.2	Рівень правового захисту персоналу, менеджменту, власників (0,2)	0,51 / 0,1	0,42 / 0,08	0,54 / 0,11	0,59 / 0,12
2.3	Взаємодія із зовнішніми суб'єктами безпеки (0,4)	0,43 / 0,17	0,43 / 0,17	0,49 / 0,2	0,58 / 0,23
3	Інформаційно-аналітична складова (0,2)	0,68 / 0,14	0,73 / 0,15	0,76 / 0,15	0,8 / 0,16
3.1	Дієвість системи отримання, перевірки й оцінювання інформації (0,3)	0,64 / 0,19	0,72 / 0,22	0,75 / 0,23	0,78 / 0,23
3.2	Спроможність виявлення й розпізнавання факторів впливу на ЕБП (0,3)	0,68 / 0,2	0,69 / 0,21	0,74 / 0,22	0,77 / 0,23
3.3	Обґрунтованість управлінських рішень (0,4)	0,73 / 0,29	0,74 / 0,3	0,78 / 0,31	0,84 / 0,34
4	Техніко-технологічна складова (0,2)	0,44 / 0,09	0,49 / 0,1	0,59 / 0,12	0,65 / 0,13
4.1	Активність застосування цифрових технологій (0,3)	0,38 / 0,11	0,45 / 0,14	0,54 / 0,16	0,59 / 0,18
4.2	Оновлення матеріально-технічної бази безпекової діяльності (0,3)	0,43 / 0,13	0,44 / 0,13	0,52 / 0,16	0,63 / 0,19
4.3	Покращення технології безпекової діяльності (0,4)	0,51 / 0,2	0,55 / 0,22	0,68 / 0,27	0,69 / 0,28
5	Кадрова складова (0,2)	0,67 / 0,13	0,68 / 0,14	0,72 / 0,14	0,75 / 0,15
5.1	Цілеспрямованість дій суб'єктів безпеки (0,4)	0,63 / 0,25	0,65 / 0,26	0,65 / 0,26	0,7 / 0,28
5.2	Покращення цифрових та професійних компетентностей (0,3)	0,72 / 0,22	0,7 / 0,21	0,78 / 0,23	0,8 / 0,24
5.3	Злагодженість дій внутрішніх суб'єктів безпеки, зокрема і у взаємодії із зовнішніми (0,3)	0,68 / 0,2	0,69 / 0,21	0,75 / 0,23	0,78 / 0,23
	Інтегральний показник розвитку СЕБП	0,59	0,61	0,65	0,71

Таблиця А.3

**Результати оцінювання розвитку СЕБП,
на прикладі ТзОВ «ВД «Високий Замок», розраховано автором**

№	Показники	Роки			
		2019	2020	2021	2022
1	Економічна складова (0,2)	0,49 / 0,1	0,47 / 0,09	0,41 / 0,08	0,36 / 0,07
1.1	Рівень використання безпекового потенціалу (0,3)	0,48 / 0,14	0,42 / 0,13	0,3 / 0,09	0,28 / 0,08
1.2	Результативність дій суб'єктів безпеки (0,4)	0,49 / 0,2	0,5 / 0,2	0,44 / 0,18	0,4 / 0,16
1.3	Вмотивована активність суб'єктів безпеки (0,3)	0,51 / 0,15	0,48 / 0,14	0,48 / 0,14	0,41 / 0,12
2	Адміністративно-правова складова (0,2)	0,4 / 0,08	0,41 / 0,08	0,4 / 0,08	0,35 / 0,07
2.1	Внутрішня нормативна база забезпечення ЕБП (0,4)	0,38 / 0,15	0,4 / 0,16	0,42 / 0,17	0,35 / 0,14
2.2	Рівень правового захисту персоналу, менеджменту, власників (0,2)	0,4 / 0,08	0,38 / 0,08	0,35 / 0,07	0,32 / 0,06
2.3	Взаємодія із зовнішніми суб'єктами безпеки (0,4)	0,42 / 0,17	0,43 / 0,17	0,41 / 0,16	0,38 / 0,15
3	Інформаційно-аналітична складова (0,2)	0,45 / 0,09	0,45 / 0,09	0,43 / 0,09	0,41 / 0,08
3.1	Дієвість системи отримання, перевірки й оцінювання інформації (0,3)	0,54 / 0,16	0,55 / 0,17	0,5 / 0,15	0,45 / 0,14
3.2	Спроможність виявлення й розпізнавання факторів впливу на ЕБП (0,3)	0,4 / 0,12	0,4 / 0,12	0,38 / 0,11	0,35 / 0,11
3.3	Обґрунтованість управлінських рішень (0,4)	0,43 / 0,17	0,4 / 0,16	0,42 / 0,17	0,39 / 0,16
4	Техніко-технологічна складова (0,2)	0,43 / 0,09	0,43 / 0,09	0,42 / 0,08	0,38 / 0,08
4.1	Активність застосування цифрових технологій (0,3)	0,54 / 0,16	0,56 / 0,17	0,58 / 0,17	0,5 / 0,15
4.2	Оновлення матеріально-технічної бази безпекової діяльності (0,3)	0,42 / 0,13	0,43 / 0,13	0,4 / 0,12	0,38 / 0,11
4.3	Покращення технології безпекової діяльності (0,4)	0,34 / 0,14	0,32 / 0,13	0,32 / 0,13	0,31 / 0,12
5	Кадрова складова (0,2)	0,5 / 0,1	0,5 / 0,1	0,48 / 0,1	0,48 / 0,1
5.1	Цілеспрямованість дій суб'єктів безпеки (0,4)	0,42 / 0,17	0,4 / 0,16	0,38 / 0,15	0,38 / 0,15
5.2	Покращення цифрових та професійних компетентностей (0,3)	0,5 / 0,15	0,52 / 0,16	0,56 / 0,17	0,6 / 0,18
5.3	Злагодженість дій внутрішніх суб'єктів безпеки, зокрема і у взаємодії із зовнішніми (0,3)	0,6 / 0,18	0,6 / 0,18	0,54 / 0,16	0,5 / 0,15
	Інтегральний показник розвитку СЕБП	0,46	0,45	0,43	0,4

Таблиця А.4

**Результати оцінювання розвитку СЕБП, на прикладі ВПП «Місіонер»,
розраховано автором**

№	Показники	Роки			
		2019	2020	2021	2022
1	Економічна складова (0,2)	0,49 / 0,1	0,48 / 0,1	0,53 / 0,11	0,58 / 0,12
1.1	Рівень використання безпекового потенціалу (0,3)	0,42 / 0,13	0,48 / 0,14	0,54 / 0,16	0,64 / 0,19
1.2	Результативність дій суб'єктів безпеки (0,4)	0,54 / 0,22	0,56 / 0,22	0,59 / 0,24	0,63 / 0,25
1.3	Вмотивована активність суб'єктів безпеки (0,3)	0,45 / 0,14	0,41 / 0,12	0,43 / 0,13	0,45 / 0,14
2	Адміністративно-правова складова (0,2)	0,62 / 0,12	0,65 / 0,13	0,66 / 0,13	0,67 / 0,13
2.1	Внутрішня нормативна база забезпечення ЕБП (0,4)	0,61 / 0,24	0,65 / 0,26	0,68 / 0,27	0,7 / 0,28
2.2	Рівень правового захисту персоналу, менеджменту, власників (0,2)	0,5 / 0,1	0,52 / 0,1	0,58 / 0,12	0,63 / 0,13
2.3	Взаємодія із зовнішніми суб'єктами безпеки (0,4)	0,7 / 0,28	0,73 / 0,29	0,68 / 0,27	0,64 / 0,26
3	Інформаційно-аналітична складова (0,2)	0,82 / 0,16	0,82 / 0,16	0,82 / 0,16	0,82 / 0,16
3.1	Дієвість системи отримання, перевірки й оцінювання інформації (0,3)	0,75 / 0,23	0,79 / 0,24	0,8 / 0,24	0,81 / 0,24
3.2	Спроможність виявлення й розпізнавання факторів впливу на ЕБП (0,3)	0,75 / 0,23	0,8 / 0,24	0,81 / 0,24	0,8 / 0,24
3.3	Обґрунтованість управлінських рішень (0,4)	0,9 / 0,36	0,84 / 0,34	0,85 / 0,34	0,85 / 0,34
4	Техніко-технологічна складова (0,2)	0,69 / 0,14	0,73 / 0,15	0,72 / 0,14	0,68 / 0,14
4.1	Активність застосування цифрових технологій (0,3)	0,74 / 0,22	0,78 / 0,23	0,76 / 0,23	0,65 / 0,2
4.2	Оновлення матеріально-технічної бази безпекової діяльності (0,3)	0,63 / 0,19	0,65 / 0,2	0,67 / 0,2	0,68 / 0,2
4.3	Покращення технології безпекової діяльності (0,4)	0,71 / 0,28	0,74 / 0,3	0,72 / 0,29	0,7 / 0,28
5	Кадрова складова (0,2)	0,87 / 0,16	0,8 / 0,16	0,78 / 0,16	0,79 / 0,16
5.1	Цілеспрямованість дій суб'єктів безпеки (0,4)	0,75 / 0,3	0,72 / 0,29	0,76 / 0,3	0,77 / 0,31
5.2	Покращення цифрових та професійних компетентностей (0,3)	0,8 / 0,24	0,84 / 0,25	0,8 / 0,24	0,75 / 0,23
5.3	Злагодженість дій внутрішніх суб'єктів безпеки, зокрема і у взаємодії із зовнішніми (0,3)	0,85 / 0,26	0,86 / 0,26	0,8 / 0,24	0,82 / 0,25
	Інтегральний показник розвитку СЕБП	0,68	0,7	0,7	0,71

Таблиця А.5

**Результати оцінювання розвитку СЕБП,
на прикладі ТЗОВ «Кольорове небо», розраховано автором**

№	Показники	Роки			
		2019	2020	2021	2022
1	Економічна складова (0,2)	0,54 / 0,11	0,53 / 0,11	0,55 / 0,11	0,7 / 0,14
1.1	Рівень використання безпекового потенціалу (0,3)	0,48 / 0,14	0,54 / 0,16	0,62 / 0,19	0,79 / 0,24
1.2	Результативність дій суб'єктів безпеки (0,4)	0,65 / 0,26	0,58 / 0,23	0,55 / 0,22	0,75 / 0,3
1.3	Вмотивована активність суб'єктів безпеки (0,3)	0,45 / 0,14	0,48 / 0,14	0,45 / 0,14	0,53 / 0,16
2	Адміністративно-правова складова (0,2)	0,62 / 0,12	0,57 / 0,11	0,56 / 0,11	0,58 / 0,12
2.1	Внутрішня нормативна база забезпечення ЕБП (0,4)	0,72 / 0,29	0,63 / 0,25	0,64 / 0,26	0,68 / 0,12
2.2	Рівень правового захисту персоналу, менеджменту, власників (0,2)	0,7 / 0,14	0,58 / 0,12	0,59 / 0,12	0,62 / 0,12
2.3	Взаємодія із зовнішніми суб'єктами безпеки (0,4)	0,48 / 0,19	0,5 / 0,2	0,45 / 0,18	0,48 / 0,19
3	Інформаційно-аналітична складова (0,2)	0,76 / 0,15	0,72 / 0,14	0,71 / 0,14	0,67 / 0,13
3.1	Дієвість системи отримання, перевірки й оцінювання інформації (0,3)	0,69 / 0,21	0,74 / 0,22	0,75 / 0,23	0,71 / 0,21
3.2	Спроможність виявлення й розпізнавання факторів впливу на ЕБП (0,3)	0,72 / 0,22	0,7 / 0,21	0,7 / 0,21	0,68 / 0,2
3.3	Обґрунтованість управлінських рішень (0,4)	0,82 / 0,33	0,72 / 0,29	0,68 / 0,27	0,65 / 0,26
4	Техніко-технологічна складова (0,2)	0,49 / 0,1	0,53 / 0,11	0,58 / 0,12	0,57 / 0,11
4.1	Активність застосування цифрових технологій (0,3)	0,5 / 0,15	0,54 / 0,16	0,58 / 0,17	0,55 / 0,17
4.2	Оновлення матеріально-технічної бази безпекової діяльності (0,3)	0,48 / 0,14	0,45 / 0,14	0,46 / 0,14	0,45 / 0,14
4.3	Покращення технології безпекової діяльності (0,4)	0,5 / 0,2	0,58 / 0,23	0,68 / 0,27	0,65 / 0,26
5	Кадрова складова (0,2)	0,63 / 0,13	0,65 / 0,13	0,66 / 0,13	0,66 / 0,13
5.1	Цілеспрямованість дій суб'єктів безпеки (0,4)	0,52 / 0,21	0,55 / 0,22	0,58 / 0,23	0,6 / 0,24
5.2	Покращення цифрових та професійних компетентностей (0,3)	0,66 / 0,2	0,68 / 0,2	0,7 / 0,21	0,7 / 0,21
5.3	Злагодженість дій внутрішніх суб'єктів безпеки, зокрема і у взаємодії із зовнішніми (0,3)	0,72 / 0,22	0,75 / 0,23	0,73 / 0,22	0,71 / 0,21
	Інтегральний показник розвитку СЕБП	0,61	0,6	0,61	0,63

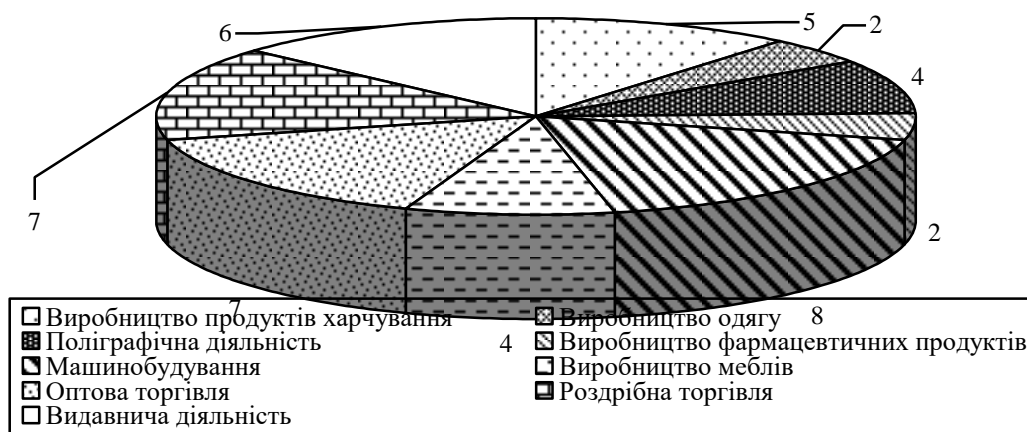


Рис. А.1. Структура групи експертів за приналежністю до діяльності підприємств певного виду економічної діяльності, *сформовано автором*

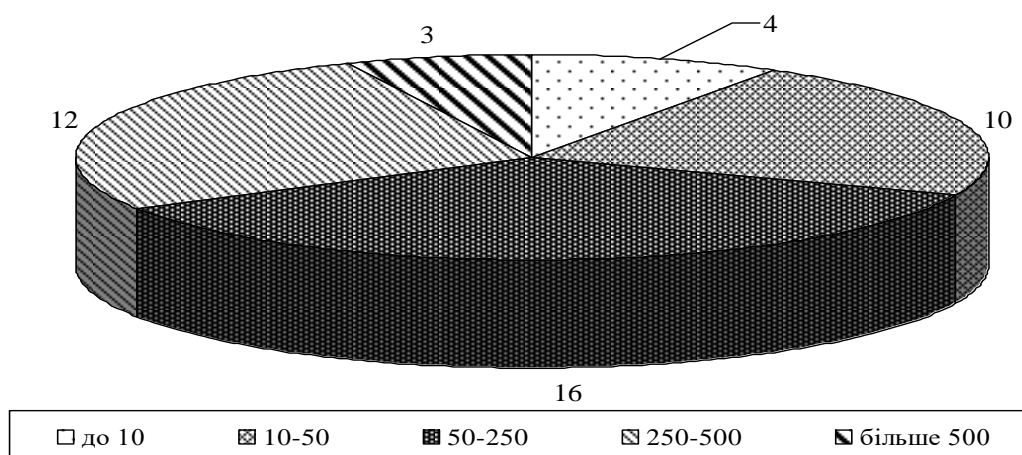


Рис. А.2. Структура групи експертів за масштабами діяльності підприємств стосовно кількості зайнятих працівників, *сформовано автором*



Рис. А.3. Варіант організації забезпечення ЕБП, які застосовуються в межах сформованої вибірки, *сформовано автором*

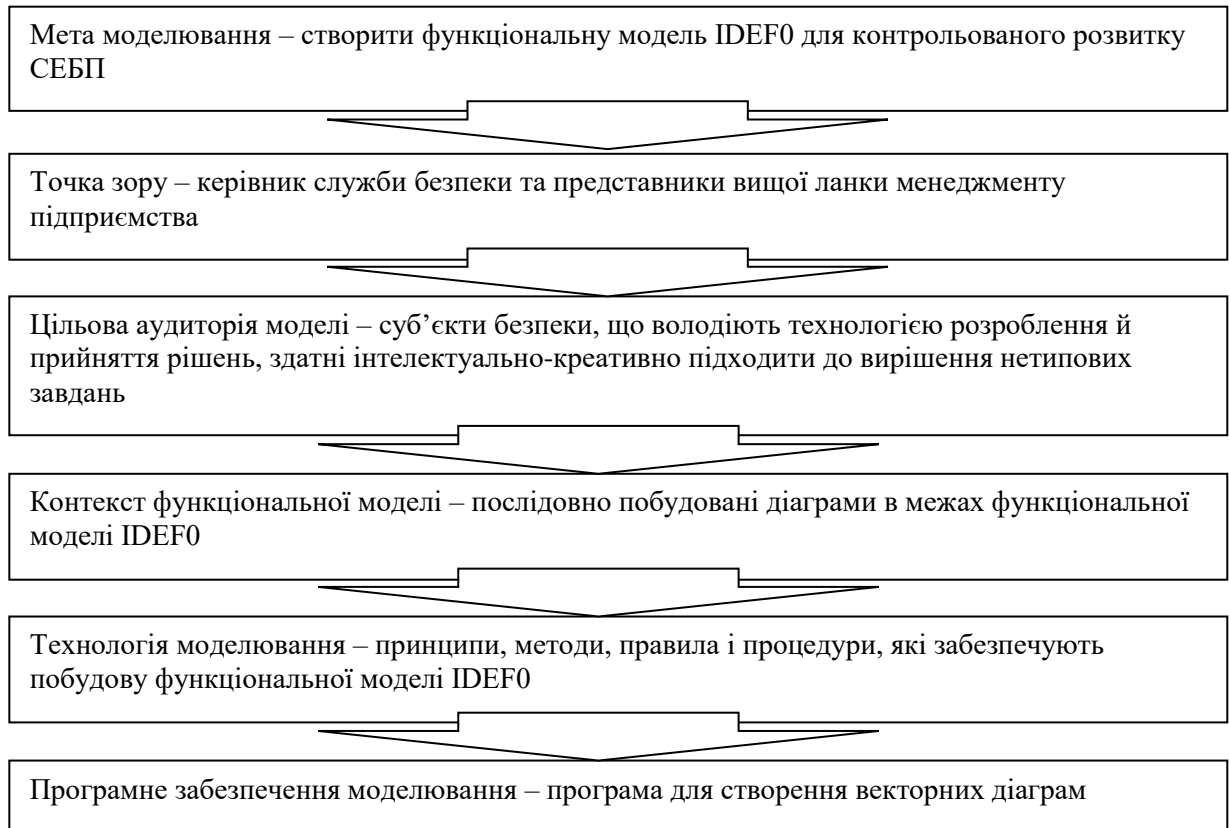


Рис. А.4. Базові умови розроблення функціональної моделі IDEF0 розвитку СЕБП, сформовано автором



Рис. А.5. Функції «Control» в діаграмі IDEF0 розвитку СЕБП



Рис. А.6. Функції «Input» у діаграмі IDEF0 розвитку СЕБП



Рис. А.7. Функції «Mechanism» у діаграмі IDEF0 розвитку СЕБП

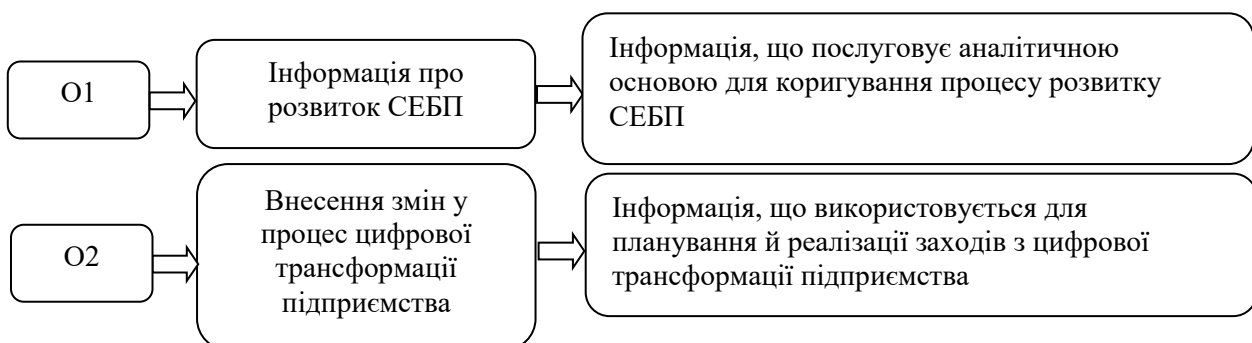


Рис. А.8. Функції «Output» у діаграмі IDEF0 розвитку СЕБП

ДОДАТОК Б


ВИСОКИЙ ЗАМОК

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ

Україна, 79018, м. Львів, вул. Героїв УПА, 65, тел. (032)237-47-02, (032)237-47-16, (032)234-90-02, e-mail: info@wz.lviv.ua

Видавничий Дім «Високий Замок»

Р/р №26001996107903 у ПАТ ПУМБ, м. Львів, ЄДРПОУ 13807781, МФО 334851.

№ 423-75-С19 квітня 2024

На № _____

ДОВІДКА**щодо використання результатів дисертаційної роботи****ШТАНГРЕТ Ірини Андріївни****«Розвиток системи економічної безпеки підприємства в умовах
цифрової трансформації економіки»**

Даним засвідчується, що результати дисертаційного дослідження Штангрет Ірини Андріївни щодо розвитку системи економічної безпеки підприємства є актуальними і такими, що були практично застосовані в діяльності структур видавничо-поліграфічної галузі. Розроблений авторкою теоретико-практичний підхід до оцінювання розвитку системи економічної безпеки підприємства дає змогу сформулювати необхідне інформаційне підґрунтя для здійснення коригуючих дій стосовно активності суб'єктів безпеки. Визначені індикатори та коригуючі коефіцієнти, після незначного уточнення у відповідності до специфіки діяльності, були застосовані для оцінювання розвитку системи економічної безпеки ТОВ «Видавничий Дім «Високий Замок».

Реалізація наукових напрацювань Штангрет Ірини Андріївни дає можливість отримати необхідний в умовах високого рівня невизначеності середовища функціонування для більшості українських підприємств соціально-економічний ефект.

Генеральний директор




Н. БАЛЮК

ДОВІДКА *N 153/42 Ву 29.06.2023*
щодо використання результатів дисертаційної роботи
Штангрет Ірини Андріївни
**«Розвиток системи економічної безпеки підприємства в умовах цифрової
трансформації економіки»**

Даним підтверджується, що складові дисертаційної роботи Штангрет Ірини Андріївни щодо розвитку системи економічної безпеки підприємства були практично застосовані в діяльності ПП «СаЮл». Здійснене авторкою моделювання розвитку системи економічної безпеки підприємства шляхом застосування методу IDEF0 дозволило сформулювати цілісне уявлення стосовно процесу безпекової діяльності в умовах ПП «СаЮл», виходячи із базових умов у вигляді тенденцій в цифровій трансформації економіки, змінах в діяльності підприємства та поточного рівня розвитку й наявного безпекового потенціалу. Отримані результати сприяли покращенню ефективності дій суб'єктів безпеки та створенню безпечних умов для цифрової трансформації підприємства загалом.

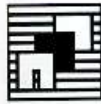
Реалізація наукових напрацювань Штангрет Ірини Андріївни дозволяє отримати необхідний, в умовах високого рівня невизначеності середовища функціонування для більшості українських підприємств, соціально-економічний ефект.

Директор ПП «СаЮл»



О. Новіцька

13798005



Науково-виробниче
товариство
з обмеженою
відповідальністю
«ППП»

ПОЛІГРАФІЧНІ ПЛІВКИ ТА ПОСЛУГИ



від 12.09.2023 № 184-3 / 123
на № від

ДОВІДКА
щодо використання
результатів дисертаційної
роботи Штангрет Ірини
Андріївни «Розвиток системи
економічної безпеки
підприємства в умовах
цифрової трансформації
економіки»

Результати дисертаційного дослідження І. А. Штангрет щодо розвитку системи економічної безпеки підприємства є актуальними і такими, що заслуговують на практичне застосування. Розроблений авторкою механізм управління розвитком системи економічної безпеки суб'єкта господарювання відзначається чітким виділенням структурних елементів, етапів реалізації та цільовим спрямуванням. Останнє сформовано виходячи із змін, які мають місце під час цифрової трансформації економіки та покликані удосконалити систему економічної безпеки підприємства задля уможливлення формування безпечних умов його розвитку.

Даним підтверджуємо, що в умовах НВТ «ППП» здійснено практичне застосування розробленого дисертанткою механізму управління розвитком системи економічної безпеки із певним коригуванням щодо специфіки господарської діяльності нашої організації. Отримані результати дозволили покращити інформаційний супровід розроблення й реалізації управлінських рішень, зокрема під час сповільнення цифрової трансформації, через посилення економічної нестабільності викликані епідемічною та військово-політичною ситуацією.

Реалізація наукових напрацювань Ірини Андріївни Штангрет дозволила отримати соціально-економічний ефект.

Генеральний директор



П. Ю. Раєвський

Научно-производственное общество
«ПОЛИГРАФИЧЕСКИЕ ПЛЕНКИ И УСЛУГИ»
НПО «ППП»

Scientific & industrial company
POLYGRAPHICAL FILMS & SERVICES
«PFS» Co. Ltd

Система управління якістю НВТ «ППП» сертифікована на відповідність вимогам **ДСТУ ISO 9001:2015**

Україна, м. Львів, вул. Зелена, 147; Україна, г. Львов, ул. Зеленая, 147; 147, Zelena Str., Lviv, Ukraine; for
для листів: 79052, м. Львів, а/с 9481 для писем: 79052, г. Львов, а/я 9481 post: p.o.b. 79052,9481, Lviv, Ukraine

тел./факс-tel./fax: (032) 270-00-49, 270-00-68, 270-90-18, E-mail: lviv@pfs.com.ua



ТзОВ "Видавництво "СВІЧАДО" вул. Лисенка, 2, а/с 808, 79008, м.Львів, Україна
 тел./факс (tel./fax) (032) 297-16-33; тел. (tel.) (032) 297-81-08; (0322) 74-23-09

"SVICHADO" Publishers Ltd. 2 Lysenko, St., P.O.BOX 808, 79008 Lviv, Ukraine
 E-mail: post@svichado.com, url: www.svichado.com

ДОВІДКА № 74/45/24 від 23.02.2024 р

щодо використання результатів дисертаційної роботи

Штангрет Ірини Андріївни

«Розвиток системи економічної безпеки підприємства в умовах цифрової
 трансформації економіки»

Даним підтверджується, що складові дисертаційного дослідження Штангрет Ірини Андріївни щодо розвитку системи економічної безпеки підприємства були практично застосовані в діяльності структур видавничо-поліграфічної галузі. Розроблені авторкою методичні засади розвитку системи економічної безпеки підприємства на основі формування цифрових компетентностей у суб'єктів безпеки сприяють досягненню оптимальності у розподілі завдань в процесі виконання безпекової діяльності, а також контролю й стимулюванню до самовдосконалення кожного співробітника служби безпеки.

Реалізація наукових напрацювань Штангрет Ірини Андріївни дозволяє отримати необхідний, в умовах високого рівня невизначеності середовища функціонування для більшості українських підприємств, соціально-економічний ефект.

Генеральний директор
 ТзОВ "Видавництво "Свічадо"


 Трояновський Богдан

ЗАТВЕРДЖУЮ

Перший проректор

Львівського державного

університету внутрішніх справ

кандидат юридичних наук, професор



Тарас СОЗАНСЬКИЙ

2024

АКТ

02.01.2024

м. Львів

№ 03

**Впровадження результатів дисертації
ШТАНГРЕТ Ірини Андріївни на тему:
«Розвиток системи економічної
безпеки підприємства в умовах
цифрової трансформації економіки»
в освітній процес ЛьвДУВС**

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

- начальника відділу забезпечення якості освіти та методичної роботи кандидата юридичних наук, доцента Руслана СТРОЦЬКОГО;
- начальника відділу організації наукової роботи кандидата юридичних наук майора поліції Людмили ПАВЛИК;
- директора Інституту управління, психології та безпеки доктора філософських наук, професора В'ячеслава БЛІХАРА;
- завідувача кафедри фінансів та обліку Інституту управління, психології та безпеки доктора економічних наук, професора Степана МЕЛЬНИКА;
- директора загальної бібліотеки Ірини КРАВЕЦЬ.

Комісія відповідно до Положення про порядок впровадження результатів наукових робіт в освітній процес, наукову, практичну, законотворчу діяльність та їх облікування у ЛьвДУВС, затвердженого наказом ЛьвДУВС від 16.08.2023 року № 270, розглянула й узагальнила основні положення і результати дисертації Ірини ШТАНГРЕТ «Розвиток системи економічної безпеки підприємства в умовах цифрової трансформації економіки», поданої на здобуття ступеня доктора філософії у галузі знань 07 «Управління та адміністрування» за спеціальністю 073 «Менеджмент», а також проаналізувала публікації, які відображають результати дослідження.

Проаналізовано основні результати дослідження ШТАНГРЕТ І. А., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Штангрет І. А. Розвиток системи економічної безпеки в умовах цифрової трансформації підприємства. *Ефективна економіка*. 2022. №6. URL: <https://nayka.com.ua/index.php/ee/article/view/120>. DOI: 10.32702/2307-2105.2022.6.34.
2. Штангрет І. А. Теоретичні засади формування системи економічної безпеки підприємства. *Ефективна економіка*. 2022. №4. URL: <http://www.economy.nayka.com.ua/?op=1&z=10173> DOI: 10.32702/2307-2105-2022.4.150.
3. Штангрет І. А. Інформаційне забезпечення розвитку системи економічної безпеки промислового підприємства в умовах цифрової трансформації економіки. *Східна Європа: економіка, бізнес та управління*. 2023. №4 (41). С. 110–115. DOI: <https://doi.org/10.32782/easterneurope.41-17>.
4. Штангрет І. А. Оцінювання розвитку системи економічної безпеки підприємства. *Інфраструктура ринку*. 2023. Вип. 74. С. 85–89. DOI: <https://doi.org/10.32782/infrastructure74-16>.
5. Штангрет І. А. Трансформаційні процеси в діяльності підприємств видавничо-поліграфічної галузі. *Держава та регіони*. 2023. №2 (128). С. 50–55. DOI: <https://doi.org/10.32782/1814-1161/2023-2-7>.
6. Штангрет І. А. Механізм управління розвитком системи економічної безпеки підприємства в умовах цифрової трансформації економіки. *Інфраструктура ринку*. 2023. № 71. С. 194–199. DOI: <https://doi.org/10.32782/infrastructure71-34>.
7. Andriyiv N., Pushak H., Petrukha N., Kokhan V., Shtangret I. Transformation of threats to demographic security and sustainable development of the region due to increased military actions. *International Journal of Sustainable Development and Planning*. 2022. Vol. 17. No. 7. P. 2221–2227. DOI: <https://doi.org/10.18280/ijstdp.170722>.
8. Штангрет І. А. Безпекові аспекти управління мотивацією працівників промислових підприємств. *Соціально-економічний розвиток і безпека України: стан та перспективи*: матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Львів, 25 березня 2021 р.). Львів: Галицька видавнича спілка, 2021. С. 148–151.
9. Штангрет І. А. Система економічної безпеки підприємства: теоретичний базис формування. *Сучасні підходи до креативного управління економічними процесами*: матеріали XIII Міжнародної науково-практичної конференції (м. Київ, 14–15 квітня 2022 р.). Київ: НАУ, 2022. С. 122–124.
10. Штангрет І. А. Методичні засади забезпечення економічної безпеки підприємства. *Менеджмент і безпека: теоретичні та прикладні аспекти*: матеріали науково-практичної конференції (м. Львів, 13 травня 2022 р.). Львів: ЛьвДУВС, 2022. С. 127–129.
11. Штангрет І. А. Безпекові аспекти цифрової трансформації промислових підприємств. *Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення*: матеріали ІХ Всеукраїнської науково-практичної конференції (м. Львів, 20–22 травня 2022 р.). Львів: УАД, 2022. С. 102–104.

12. Штангрет І. А. Концептуальне підґрунтя розвитку системи економічної безпеки підприємства. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні*: матеріали VIII Всеукраїнської науково-практичної конференції (м. Львів, 24–26 листопада 2022 р.). Львів: УАД, 2022. С. 136–138.

На основі проведеного аналізу комісія зробила висновок, що праці ШТАНГРЕТ І. А. містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Львівського державного університету внутрішніх справ, зокрема при викладанні навчальних дисциплін «Основи безпекознавства», «Фінансова безпека» та «Бюджетно-податкова безпека», під час підготовки навчально-методичних і дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії:

	Руслан СТРОЦЬКИЙ
	Людмила ПАВЛИК
	В'ячеслав БЛІХАР
	Степан МЕЛЬНИК
	Ірина КРАВЕЦЬ

ЗАТВЕРДЖУЮ

Проректор
Львівського державного
університету внутрішніх справ
доктор юридичних наук, професор



Ольга БАЛИНСЬКА

2024

АКТ

04.05. 2024

м. Львів

№ 4

**Впровадження результатів дисертації
ШТАНГРЕТ Ірини Андріївни на тему:
«Розвиток системи економічної
безпеки підприємства в умовах
цифрової трансформації економіки»
у наукову діяльність ЛьвДУВС**

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

- начальника відділу організації наукової роботи кандидата юридичних наук майора поліції Людмили ПАВЛИК;
- завідувача відділення організації освітньо-наукової підготовки (докторантура та аспірантура (ад'юнктура)) кандидата юридичних наук підполковника поліції Тетяни КОХАНЮК;
- директора Інституту управління, психології та безпеки доктора філософських наук, професора В'ячеслава БЛІХАРА;
- завідувача кафедри фінансів та обліку Інституту управління, психології та безпеки доктора економічних наук, професора Степана МЕЛЬНИКА;
- завідувача кафедри соціально-поведінкових, гуманітарних наук та економічної безпеки Інституту управління, психології та безпеки, керівника теми науково-дослідної роботи з державною реєстрацією «Економічна безпека соціально-економічних систем: проблеми теорії та практики» (номер державної реєстрації 0121U112498, 2021–2024 р.) доктора економічних наук, професора Марти КОПИТКО;
- директора загальної бібліотеки Ірини КРАВЕЦЬ.

Комісія відповідно до Положення про порядок впровадження результатів наукових робіт в освітній процес, наукову, практичну, законотворчу діяльність та їх облікування у ЛьвДУВС, затвердженого наказом ЛьвДУВС від 16.08.2023 року № 270, розглянула й узагальнила основні положення і результати дисертації Ірини

ШТАНГРЕТ «Розвиток системи економічної безпеки підприємства в умовах цифрової трансформації економіки», а також проаналізувала основні публікації, які відображають результати дослідження.

На основі проведеного аналізу комісія зробила висновок, що дисертація Ірини ШТАНГРЕТ «Розвиток системи економічної безпеки підприємства в умовах цифрової трансформації економіки» містить науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання у науковій діяльності Львівського державного університету внутрішніх справ, зокрема:

1) проведення подальших наукових досліджень з проблем: систематизації передумов розвитку системи економічної безпеки підприємства; формування концептуального підґрунтя розвитку системи економічної безпеки підприємства; обґрунтування теоретико-методичного підходу до оцінювання розвитку системи економічної безпеки підприємства; розроблення моделі підсистеми інформаційного забезпечення розвитку системи економічної безпеки підприємства; побудови механізму управління розвитком системи економічної безпеки підприємства; формування методичних засад розвитку системи економічної безпеки підприємства; розроблення науково-практичного підходу до розвитку системи економічної безпеки підприємства;

2) підготовки наукового звіту за темою науково-дослідної роботи з державною реєстрацією «Економічна безпека соціально-економічних систем: проблеми теорії та практики» (номер державної реєстрації 0121U112498, 2021–2024 р.);

3) виконання наукових робіт, цитування результатів наукової роботи, підготовки наукових доповідей та фахових статей, які презентують вже отримані результати або присвячені подальшій розробці теоретико-методичних положень та практичних рекомендацій щодо розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки.

Члени комісії:

	Людмила ПАВЛИК
	Тетяна КОХАНЮК
	В'ячеслав БЛІХАР
	Степан МЕЛЬНИК
	Марта КОПИТКО
	Ірина КРАВЕЦЬ



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УКРАЇНСЬКА АКАДЕМІЯ ДРУКАРСТВА

вул. Під Голоском, 19, м. Львів, 79020, тел. (032)242-23-40,
 Факс: (032)252-71-68, E-mail: uad@uad.lviv.ua, код ЄДРПОУ 2071004

16.11.2023 № 64-11/690

На № _____ від _____

ДОВІДКА

щодо використання результатів дисертаційної роботи

Штангрет Ірини Андріївни

**«Розвиток системи економічної безпеки підприємства в умовах цифрової
 трансформації економіки»**

Теоретичні висновки і практичні результати наукового дослідження Штангрет І. А. стосовно розроблення теоретико-методичних підходів і практичних рекомендацій щодо розвитку системи економічної безпеки підприємства в умовах цифрової трансформації економіки впроваджені кафедрою фінансово-економічної безпеки, обліку і оподаткування в навчальний процес, зокрема використані для підготовки лекційного матеріалу дисциплін «Комплексне забезпечення фінансово-економічною безпекою», «Менеджмент економічної безпеки підприємства», «Антикризове управління підприємством», «Соціально-економічна безпека» та «Наукове та методичне забезпечення діяльності фахівців з фінансово-економічної безпеки».

Проректор з науково-педагогічної роботи
 к.т.н., доцент



Я. М. Угрин

ДОДАТОК В

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Праці, в яких опубліковані основні наукові результати дисертації

1. Штангрет І. А. Розвиток системи економічної безпеки в умовах цифрової трансформації підприємства. *Ефективна економіка*. 2022. № 6. URL: <https://nauka.com.ua/index.php/ee/article/view/120>. DOI: 10.32702/2307-2105.2022.6.34.

2. Штангрет І. А. Теоретичні засади формування системи економічної безпеки підприємства. *Ефективна економіка*. 2022. № 4. URL: <http://www.economy.nauka.com.ua/?op=1&z=10173> DOI: 10.32702/2307-2105-2022.4.150.

3. Штангрет І. А. Інформаційне забезпечення розвитку системи економічної безпеки промислового підприємства в умовах цифрової трансформації економіки. *Східна Європа: економіка, бізнес та управління*. 2023. № 4 (41). С. 110–115. DOI: <https://doi.org/10.32782/easterneurope.41-17>.

4. Штангрет І. А. Оцінювання розвитку системи економічної безпеки підприємства. *Інфраструктура ринку*. 2023. Вип. 74. С. 85–89. DOI: <https://doi.org/10.32782/infrastructure74-16>.

5. Штангрет І. А. Трансформаційні процеси в діяльності підприємств видавничо-поліграфічної галузі. *Держава та регіони*. 2023. №2 (128). С. 50–55. DOI: <https://doi.org/10.32782/1814-1161/2023-2-7>.

6. Штангрет І. А. Механізм управління розвитком системи економічної безпеки підприємства в умовах цифрової трансформації економіки. *Інфраструктура ринку*. 2023. № 71. С. 194–199. DOI: <https://doi.org/10.32782/infrastructure71-34>.

7. Мельник С. І., Штангрет І. А. Методичні засади розвитку системи економічної безпеки підприємства. *Ефективна економіка*. 2024. № 1. URL: <https://www.nauka.com.ua/index.php/ee/article/view/2863/2899> DOI:

<http://doi.org/10.32702/2307-2105.2024.1.17> (особистий внесок здобувача: розроблено методичні засади розвитку системи економічної безпеки підприємства на основі формування цифрових компетентностей у суб'єктів безпеки).

8. Andriyiv N., Pushak H., Petrukha N., Kokhan V., Shtangret I. Transformation of threats to demographic security and sustainable development of the region due to increased military actions. *International Journal of Sustainable Development and Planning*. 2022. Vol. 17. No. 7. P. 2221–2227. DOI: <https://doi.org/10.18280/ijstdp.170722>. (особистий внесок здобувача: визначення впливу військових дій на демографічну безпеку України, із конкретизацією тих загроз, що пов'язані з втратою трудових ресурсів та негативно впливають на економічну безпеку підприємств. (наукове видання (журнал) індексується міжнародною наукометричною базою Scopus).

Праці, які засвідчують апробацію матеріалів дисертації

9. Штангрет І. А. Безпекові аспекти управління мотивацією працівників промислових підприємств. *Соціально-економічний розвиток і безпека України: стан та перспективи* : матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Львів, 25 березня 2021 р.). Львів : Галицька видавнича спілка, 2021. С. 150–152.

10. Штангрет І. А. Система економічної безпеки підприємства: теоретичний базис формування. *Сучасні підходи до креативного управління економічними процесами* : матеріали XIII Міжнародної науково-практичної конференції (м. Київ, 14–15 квітня 2022 р.). Київ : НАУ, 2022. С. 122–124.

11. Штангрет І. А. Методичні засади забезпечення економічної безпеки підприємства. *Менеджмент і безпека: теоретичні та прикладні аспекти* : матеріали науково-практичної конференції (м. Львів, 13 травня 2022 р.). Львів : ЛьвДУВС, 2022. С. 127–129.

12. Штангрет І. А. Безпекові аспекти цифрової трансформації промислових підприємств. *Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення* : матеріали ІХ Всеукраїнської науково-практичної конференції (м. Львів, 20–22 травня 2022 р.). Львів : УАД, 2022. С. 102–104.

13. Штангрет І. А. Концептуальне підґрунтя розвитку системи економічної безпеки підприємства. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні* : матеріали VIII Всеукраїнської науково-практичної конференції (м. Львів, 24–26 листопада 2022 р.). Львів : УАД, 2022. С. 136–138.

14. Штангрет І. А. Механізм забезпечення економічної безпеки підприємства. *Соціально-економічний розвиток і безпека України: стан та перспективи* : матеріали міжвузівської науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Львів, 23 березня 2023 р.). Львів : ЛьвДУВС, 2023. С. 151–153.

15. Штангрет І. А. Механізм управління розвитком системи економічної безпеки підприємства: теоретичні засади. *Сучасні підходи до креативного управління економічними процесами* : матеріали XIV Міжнародної науково-практичної конференції (м. Київ, 13–14 квітня 2023 р.). Київ : НАУ, 2023. С. 231–233.

16. Штангрет І. А. Розвиток системи економічної безпеки підприємства: необхідність та варіант реалізації. *Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення* : матеріали X Всеукраїнської науково-практичної конференції (м. Львів, 25–27 травня 2023 р.). Львів : УАД, 2023. С. 125–127.

17. Штангрет І. А. Система інформаційного забезпечення безпекової діяльності підприємства. *Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні* : матеріали ІХ Всеукраїнської науково-практичної конференції (м. Львів, 23–26 листопада 2023 р.). Львів : УАД, 2023. С. 192–194.

ДОДАТОК Д

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

1. Міжвузівська науково-практична конференція здобувачів вищої освіти і молодих вчених «Соціально-економічний розвиток і безпека України: стан та перспективи» (м. Львів, 25 березня 2021 р., очна форма участі).

2. XIII Міжнародна науково-практична конференція «Сучасні підходи до креативного управління економічними процесами» (м. Київ, 14–15 квітня 2022 р., заочна форма участі).

3. Науково-практична конференція «Менеджмент і безпека: теоретичні та прикладні аспекти» (м. Львів, 13 травня 2022 р., очна форма участі).

4. IX Всеукраїнська науково-практична конференція «Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення» (м. Львів, 20–22 травня 2022 р., очна форма участі).

5. VIII Всеукраїнська науково-практична конференція «Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні» (м. Львів, 24–26 листопада 2022 р., очна форма участі).

6. Міжвузівська науково-практична конференція здобувачів вищої освіти і молодих вчених «Соціально-економічний розвиток і безпека України: стан та перспективи» (м. Львів, 23 березня 2023 р., очна форма участі).

7. XIV Міжнародна науково-практична конференція «Сучасні підходи до креативного управління економічними процесами» (м. Київ, 13–14 квітня 2023 р., заочна форма участі).

8. X Всеукраїнська науково-практична конференція «Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення» (м. Львів, 25–27 травня 2023 р., очна форма участі).

9. IX Всеукраїнська науково-практична конференція «Формування стратегії соціально-економічного розвитку підприємницьких структур в Україні» (м. Львів, 23–26 листопада 2023 р., очна форма участі).