МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

Кваліфікаційна наукова
праця на правах рукопису

БІЛЬКО СТАНІСЛАВ СЕРГІЙОВИЧ

УДК 338.2:316.774:004.056+001.102

ДИСЕРТАЦІЯ

ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

051 Економіка
05 Соціальні та поведінкові науки

Подається на здобуття наукового ступеня доктора філософії

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

_____ С.С. Білько
(підпис)

Науковий керівник: Онищенко Світлана Володимирівна
доктор економічних наук, професор

Полтава 2023

АНОТАЦІЯ

Білько С.С. Формування інформаційної безпеки національної економіки. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 051 Економіка (05 Соціальні та поведінкові науки). – Національний університет «Полтавська політехніка імені Юрія Кондратюка». – Полтава, 2023.

Дисертаційна робота присвячена розробленню теоретичних положень, науково-методичних підходів та практичних рекомендацій щодо формування інформаційної безпеки національної економіки.

У дисертаційній роботі досліджено еволюцію понятійно-категорійного базису інформаційної безпеки національної економіки та сучасні підходи. Розкрито сутність інформаційної безпеки національної економіки, визначено її місце в системі національної безпеки держави. Наведено об'єктно-суб'єктну характеристику системи інформаційної безпеки національної економіки з урахуванням взаємозв'язків між елементами структури. Поглиблено концептуальні засади дослідження інформаційної безпеки з урахуванням посилення процесів цифровізації національної економіки.

Запропоновано наукову класифікацію загроз інформаційній безпеці з урахуванням цифрової трансформації національної економіки. Таксономію загроз доповнено їх розподілом за об'єктами спрямування дестабілізуючих дій: макрорівень, мезорівень, мікрорівень та нанорівень, що дозволяє підвищити інформаційну безпеку на усіх зазначених рівнях через обґрунтування важелів та інструментів побудови ефективної системи захисту інформаційних ресурсів.

Обґрунтовано науковий підхід до формування інституційного забезпечення інформаційної безпеки національної економіки в розрізі основних структурних елементів (інституційно-організаційного, інституційно-правового), що дасть змогу визначити перспективні напрями державної політики, спрямованої на реалізацію комплексу заходів з організації, взаємодії,

інформування, контролю й інших функціонально-розпорядчих дій, виконання яких забезпечить формування безпекоорієнтованого інформаційного середовища.

Запропоновано методологічні підходи до дослідження інформаційної безпеки національної економіки, визначено загальнонаукові й спеціальні методи, принципи, способи наукового пізнання. Поглиблено науково-методичні засади оцінювання інформаційної безпеки національної економіки, цільовою функцією якого є оцінювання поточного рівня, тенденцій зміни інтегрального показника інформаційної безпеки національної економіки з урахуванням домінуючих світових тенденцій розвитку цифровізації, визначення основних факторів впливу та обґрунтування стратегічних напрямів зміцнення інформаційної безпеки національної економіки.

Запропоновано методичний підхід до оцінювання рівня інформаційної безпеки, що ґрунтується на інтегральному методі, методах нормування, згладжування і експертних оцінок та передбачає використання принципово нової системи індикаторів (індикаторів цифрової, інституційної, кіберспроможності національної економіки). Узагальнено та систематизовано основні етапи проведення оцінювання рівня інформаційної безпеки. У методиці застосовується теорія нечітких множин (п’ятирівневий нечіткий класифікатор), що дозволяє визначити рівень інформаційної безпеки у відповідності до п’яти можливих. Методичний підхід передбачає також здійснення прогнозування рівня інформаційної безпеки з використанням моделі поліноміальної апроксимації, що обґрунтовується аналізом великого набору даних нестабільних величин.

Встановлено діалектику взаємодії інформаційної безпеки та національної економіки на основі виявлених кореляційних зв’язків між показниками інформаційної й економічної безпеки, а також обґрунтованого впливу рівня інформаційної безпеки на рівень розвитку національної економіки, що актуалізує необхідність усунення загроз та деструктивних факторів розвитку національної економіки на основі формування безпекоорієнтованого інформаційного середовища.

Визначено архітектоніку національної економіки в умовах цифровізації, що розкриває дуальний вплив процесів цифровізації в аспекті формування можливостей щодо створення валової доданої вартості, отримання економічними вигід суб'єктами господарювання в умовах зростання ризиків і загроз національній економіці в інформаційному середовищі.

Обґрунтовано концепти синергетичного підходу до забезпечення інформаційної безпеки національної економіки, які ґрунтуються на дослідженні інформаційної безпеки національної економіки як складної, відкритої, нерівноважної, нелінійної, з елементами самоорганізації системи. Запропоновано концептуальну модель механізму формування безпекоорієнтованого інформаційного середовища, що ґрунтується на положеннях нової парадигми використання можливостей, пов'язаних з розвитком інформаційних технологій та попередження й запобігання новим загрозам інформаційній безпеці національної економіки шляхом захисту інформації. Концептуальна модель враховує економічні інтереси суб'єктів усіх рівнів (макро-, мезо-, мікро- та нанорівня), що дозволить отримати позитивні синергетичні ефекти в напрямку зміцнення безпеки національної економіки в умовах впливу внутрішніх і зовнішніх дестабілізуючих чинників.

Доведено, що зміцнення інформаційної безпеки національної економіки ґрунтується на захищеності кожного економічного суб'єкта в інформаційному середовищі, що вимагає впровадження ефективних систем захисту інформації з метою своєчасного виявлення та оперативного реагування на реальні та потенційні загрози. На основі проведеного компаративного аналізу систем інформаційної безпеки встановлено, що модернізація структур та типологій систем захисту інформації відбувається під впливом розвитку технологій, змін у безпековому середовищі, формах, способах та технологіях застосування засобів кібервпливу.

Запропоновано нові підходи до визначення стратегічних орієнтирів державної політики, що ґрунтуються на ієрархічній структурі пріоритетних напрямів реалізації положень Стратегії інформаційної безпеки України та

Стратегії економічної безпеки України на період до 2025 року та вимагають впровадження нових, більш дієвих механізмів управління інформаційною безпекою на рівні як підприємств, так і країни в цілому, спрямованих на усунення бар'єрів, перешкод, ризиків, загроз, що змінюють середовище функціонування національної економіки в умовах цифровізації. Стратегічними орієнтирами забезпечення інформаційної безпеки національної економіки визначено: зміцнення стійкості національної економіки до кіберзагроз і реалізація національних економічних інтересів на засадах інформаційної захищеності; стимулювання розвитку галузі ІКТ з одночасним впровадженням найбільш ефективних програмно-технологічних рішень для захисту інформації та зменшення її витоків, попередження зовнішніх і внутрішніх ризиків та загроз; удосконалення нормативно-правової бази щодо реалізації державної політики інформаційної безпеки та її гармонізація зі стандартами ЄС.

Дисертація є завершеним науковим дослідженням, у якому розроблено нові теоретичні положення, науково-методичні підходи та практичні рекомендації щодо формування інформаційної безпеки національної економіки й обґрунтування стратегічних пріоритетів державної політики забезпечення безпекоорієнтованого інформаційного середовища.

Наукові положення, висновки і рекомендації, що виносяться на захист, одержані автором самостійно. Внесок автора в наукові праці, опубліковані у співавторстві, конкретизовано у списку публікацій.

Практичне значення одержаних результатів полягає у тому, що теоретичні положення, методичні підходи та висновки, викладені в дисертаційній роботі, доведені до рівня прикладних рекомендацій, які у сукупності створюють обґрунтовану основу для побудови цілісної системи формування інформаційної безпеки національної економіки. Отримані наукові результати дослідження були використані підприємствами та організаціями при розробленні положень політики формування інформаційної безпеки.

Ключові слова: інформаційна безпека, національна економіка, економічна безпека, загрози, оцінювання рівня інформаційної безпеки, політика формування інформаційної безпеки, цифровізація.

ABSTRACT

Bilko S.S. Formation of information security for the national economy. – Qualification scholary paper: a manuscript.

Thesis submitted for obtaining the Doctor of Philosophy degree in Speciality 051 Economics (05 Social and Behavioral Sciences). National University «Yuri Kondratyuk Poltava Polytechnic». – Poltava, 2023.

The dissertation is devoted to the development of theoretical provisions, scientific and methodological approaches, and practical recommendations for the formation of information security for the national economy.

The evolution of the conceptual and categorical framework of information security for the national economy and modern approaches are studied in the thesis. The essence of information security for the national economy is revealed, and its place in the state security system is determined. The object-subject characterization of the information security system for the national economy is given, taking into account the interrelationships between the elements of the structure. The conceptual foundations of information security research are deepened, taking into account the intensification of digitalization processes of the national economy.

A scientific classification of threats to information security is proposed, taking into account the digital transformation of the national economy. The taxonomy of threats is supplemented by their distribution by the objects of destabilizing actions: macro-level, meso-level, micro-level and nano-level, which allows to improve information security at all these levels by substantiating the levers and tools for building an effective system of information resources protection.

The dissertation substantiates a scientific approach to the formation of institutional support for information security of the national economy in the context of the main structural elements (institutional and organizational, institutional and legal), which will allow determining the promising directions of the State policy aimed at implementing a set of measures for organization, interaction, information, control and other functional and administrative actions, the implementation of which will ensure the formation of a security-oriented information environment.

The methodological approaches to the study of information security for the national economy are proposed, and general scientific and special methods, principles, and methods of scientific cognition are defined. The scientific and methodological bases for evaluating the information security of the national economy are deepened, the purpose of which is to assess the current level, and trends in the integral indicator of information security for the national economy, taking into account the dominant global trends in the development of digitalization, identifying the influencing main factors and substantiating the strategic directions for strengthening the information security of the national economy.

An improved approach to assessing the level of information security based on the integral method, methods of normalization, smoothing, and expert assessments, and involves the use of a fundamentally new system of indicators (indicators of digital, institutional, and cyber capabilities of the national economy). The main stages of information security assessment are generalized and systematized. The methodology applies the theory of fuzzy sets (five-level fuzzy classifier), which allows for determining the level of information security per the five possible levels. The methodological approach also provides for forecasting the level of information security using a polynomial approximation model, which is grounded in the analysis of a large data set of unstable values.

The dialectic of interaction between information security and the national economy is established based on the identified correlations between the indicators of information and economic security, as well as the reasonable influence of the information security level on the level of national economic development, which

actualizes the need to eliminate threats and destructive factors of the national economy through the formation of a security-oriented information environment.

The architectonics of the national economy in the context of digitalization is determined, which reveals the dual impact of digitalization processes in terms of creating opportunities for creating gross added value, obtaining benefits by economic entities in the conditions of growing risks and threats to the national economy in the information environment.

The concepts of a synergistic approach to ensuring information security for the national economy are grounded, based on the study of information security for the national economy as a complex, open, non-equilibrium, nonlinear, with elements of a self-organization system. A mechanism for the formation of a security-oriented information environment is developed, which is based on the provisions of a new paradigm of using the opportunities associated with the development of information technology and preventing and deterring new threats to information security for the national economy through information protection. The conceptual model takes into account the economic interests of entities at all levels (macro-, meso-, micro-, and nano-levels), which will allow for positive synergistic effects in strengthening the security of the national economy in the face of internal and external destabilizing factors.

It is proved that strengthening the information security of the national economy is based on the security of each economic entity in the information environment, which requires the introduction of effective information security systems with a view to timely detection and prompt response to real and potential threats. Based on the comparative analysis of information security systems, it is established that the modernization of structures and typologies of information security systems is influenced by the development of technologies, changes in the security environment, forms, methods and technologies of cyber influence.

New approaches to determining the strategic guidelines of the state policy based on the hierarchical structure of priority areas for implementing the provisions of the Information Security Strategy of Ukraine and the Economic Security Strategy of

Ukraine for the period up to 2025 are proposed. They require the introduction of new, more effective mechanisms for managing information security at the level of both enterprises and the country as a whole, aimed at eliminating barriers, obstacles, risks, and threats that change the environment of the national economy in the context of digitalization. The strategic guidelines for ensuring the information security of the national economy are as follows: strengthening the resilience of the national economy to cyber threats and realization of national economic interests on the basis of information security; stimulating the development of the ICT industry with the simultaneous implementation of the most effective software and technological solutions to protect information and reduce its leakage, prevent external and internal risks and threats; improving the regulatory framework for the implementation of the state policy of information security and its harmonization with the EU standards.

The dissertation is a completed scientific study that develops new theoretical provisions, scientific and methodological approaches, and practical recommendations for the formation of information security for the national economy and substantiation of strategic priorities of the state policy of ensuring a security-oriented information environment.

The scientific positions, conclusions, and recommendations submitted for defense were obtained by the author independently. The author's contribution to scientific works published in co-authorship is specified in the list of publications.

The practical value of the results obtained is that the theoretical provisions, methodological approaches, and conclusions outlined in the thesis are brought to the level of applied guidelines, which together create a reasonable basis for building an integrated system of information security for the national economy. The obtained scientific results of the study were used by enterprises and organizations in the development of information security policy provisions.

Keywords: information security, national economy, economic security, threats, assessment of the level of information security, information security policy, digitalization.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації у виданнях, що включені до міжнародних наукометричних баз

1. Bilko S., Onyshchenko S., Yanko A., Sivitska S. Business Information Security. *Lecture Notes in Civil Engineering*. 2023. Vol 299. P. 769–778. DOI: https://doi.org/10.1007/978-3-031-17385-1_65 (Scopus) (0,61 друк. арк.). *Особистий внесок здобувача: запропоновано систему забезпечення інформаційної безпеки, яка базується на чіткому алгоритмі визначених процедур, які дозволять забезпечити достовірність, конфіденційність, цілісність і доступність інформаційних ресурсів суб'єкта господарювання, а також нейтралізувати потенційні та мінімізувати реальні ризики і загрози інформаційному середовищу компанії (0,3 друк. арк.)*.

2. Bilko S., Onyshchenko S., Zhyvylo Y., Cherviak A. Determination of the peculiarities peculiarities of using information security systems in financial institutions in order to increase the financial security level. *Eastern-European Journal of Enterprise Technologies*. 2023. No. 5 (13 (125)). P. 65–76. DOI: https://doi.org/10.15587/1729-4061.2023.288175 (Scopus) (1,6 друк. арк.). *Особистий внесок здобувача: визначено топологію систем захисту інформації; запропоновано алгоритм побудови ефективних систем захисту інформації економічних суб'єктів (0,9 друк. арк.)*.

Публікації у наукових фахових виданнях України

3. Білько С. С. Інституційне забезпечення інформаційної безпеки України. *Економіка і регіон.* 2021. Вип. 3. С. 36–41. DOI: https://doi.org/10.26906/EiR.2021.3(82).2361 (0,5 друк. арк.).

4. Білько С. С. Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку. *Науковий вісник Полісся*. 2021. № 1 (24). С. 58–77. DOI: https://doi.org/10.25140/2410-9576-2022-1(24)-58-77 (1,0 друк. арк.).

5. Білько С. С., Онищенко С. В. Загрози інформаційній безпеці національної економіки. *Науковий вісник Одеського національного економічного університету.* 2022. № 11-12 (300-301). С. 50–56. DOI: https://doi.org/10.32680/2409-9260-2022-11-12-300-301-50-56 (0,66 друк. арк.). *Особистий внесок здобувача: Систематизовано та удосконалено багаторівневу класифікацію загроз інформаційній безпеці національної економіки (0,5 друк. арк.).*

6. Білько С. С., Онищенко С. В. Концепти синергетичного підходу до формування безпекоорієнтованого інформаційного середовища в Україні. *Вісник Хмельницького національного університету.* 2023. № 1 (314). С. 204–211. DOI: https://doi.org/10.31891/2307-5740-2023-314-1-31 (0,95 друк. арк.). *Особистий внесок здобувача: Розроблено авторську концептуальну модель формування безпекоорієнтованого інформаційного середовища в Україні, спрямовану на захист національних економічних інтересів та забезпечення безпеки національної економіки (0,7 друк. арк.).*

Тези доповідей на наукових конференціях

7. Білько С. С. Інституційно-правове забезпечення інформаційної безпеки України. *Розвиток фінансового ринку в Україні: загрози, проблеми та перспективи*: матеріали III Міжнародної наук.-практ. конф., м. Полтава, 27 жовт. 2021 р. Полтава, 2021. С. 37–38 (0,16 друк. арк.).

8. Білько С. С. Інформаційна безпека будівельного бізнесу в Україні. *Молодіжна наука заради миру та розвитку*: матеріали Міжнародної наук.-практ. конф., присвяченої Всесвітньому дню науки, м. Чернівці, 9–11 листоп. 2022 р. Чернівці, 2022. С. 540–543 (0,24 друк. арк.).

9. Білько С. С. Інформаційна безпека України в умовах посилення кібератак. *Сталий розвиток: виклики та загрози в умовах воєнного стану*: матеріали Міжнародної наук.-практ. Інтернет-конференції, м. Полтава, 09 черв. 2022 р. Полтава, 2022. С. 113–115 (0,15 друк. арк.).

10. Білько С. С. Забезпечення інформаційної безпеки бізнесу в умовах загроз воєнного стану. *Економічна безпека: держава, регіон, підприємство*: матеріали Міжнародної наук.-практ. Інтернет-конференції, м. Полтава, 29 верес. 2022 р. / Національний університет імені Юрія Кондратюка. Полтава, 2022. С. 52–55 (0,17 друк. арк.).

11. Білько С. С. Сутнісна характеристика загроз інформаційній безпеці України. *RECENT ADVANCES IN SCIENCE*: Proceedings of the International Conference, Boston, 15–16 February 2023. Boston, 2023. P. 30–34 (0,2 друк. арк.).

12. Bilko S. Methodical Approaches to Assessment of Information Security. *Scientific research in the modern world*: Proceedings of the 4th International scientific and practical conference, Toronto, 9–11 February 2023. Toronto, 2023. P. 505–510 (0,32 друк. арк.).

13. Білько С. С. Ризики та загрози кібербезпеці бізнесу в умовах цифровізації економіки. *Modernization of science and its influence on global processes*: collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific and Theoretical Conference, Bern, 14 April 2023. Bern, 2023. P. 14–16 (0,22 друк. арк.).

14. Білько С. С. Інформаційна безпека національної економіки в умовах зростання викликів та загроз. *Економічна безпека: держава, регіон, підприємство*: матеріали VII Міжнародної наук.-практ. Інтернет-конференції, м. Полтава, 17 трав. 2023 р. Полтава, 2023. С. 151–154 (0,17 друк. арк.).

ЗМІСТ

ВСТУП 14
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ 22
1.1. Інформаційна безпека національної економіки: зміст та місце в системі національної безпеки України 22
1.2. Ідентифікація загроз інформаційній безпеці в умовах цифровізації 39
1.3. Інституційне забезпечення інформаційної безпеки національної економіки. 54
Висновки до розділу 1 66
РОЗДІЛ 2. АНАЛІЗ ТА ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕКОНОМІКИ УКРАЇНИ 68
2.1. Аналіз цифровізації національної економіки та розвитку інформаційного середовища в Україні 68
2.2. Методичні засади оцінювання рівня інформаційної безпеки національної економіки 89
2.3. Оцінювання інформаційної безпеки економіки України 107
Висновки до розділу 2 122
РОЗДІЛ 3. НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ УКРАЇНИ 124
3.1. Концепти забезпечення інформаційної безпеки національної економіки в умовах цифровізації 124
3.2. Компаративний аналіз систем інформаційної безпеки та модернізація структур захисту інформації в Україні 139
3.3. Стратегічні орієнтири державної політики щодо забезпечення інформаційної безпеки економіки України 151
Висновки до розділу 3 165
ВИСНОВКИ 168
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 172
ДОДАТКИ 192

ВСТУП

Актуальність теми. Процеси глобалізації та цифровізації кардинально змінили імператив розвитку й економічну парадигму світу. Економічне зростання, підвищення конкурентоспроможності національних економік і якості життя населення неможливе без цифровізації господарських процесів, що безперечно позитивно впливає на розвиток соціального, економічного, технологічного, інтелектуального, інфраструктурного потенціалу. Водночас, процеси цифровізації спричинили виникнення нових ризиків і загроз функціонуванню національних економік. Інформаційні війни, інформаційний тероризм, масштабні кібератаки – ці деструктивні феномени характеризують сучасний світ та супроводжуються фінансовими втратами від інформаційних витоків. Кібератаки протягом 2020 року коштували світовій економіці понад трильйон доларів, у 2022 році – до 4,2–6 трлн дол. Прогнозується, що у 2025 році обсяг фінансових втрат від кіберзлочинності становитиме близько 10,5 трлн дол. Таким чином, забезпечити захист економічних інтересів, стійкість національної економіки та зміцнення національної безпеки загалом можливо лише за умови формування та забезпечення інформаційної безпеки національної економіки.

Проблема забезпечення захисту та безпеки національної економіки широко аналізується у працях вітчизняних науковців, зокрема, І. Бабець, З. Варналія, О. Власюка, А. Гальчинського, В. Гейця, В. Горбуліна, Я. Жаліла, З. Живко, М. Єрмошенка, Г. Козаченко, С. Пирожкова, А. Сухорукова, В. Шлемка, М. Флейчук та інших. У фундаментальних та прикладних дослідженнях розкривається генезис безпеки з позицій філософського й соціологічного сприйняття, розглядаються теоретичні засади економічної безпеки, обґрунтовується механізм її забезпечення. В умовах зростання викликів у інформаційному просторі предметом дослідження науковців виступають процеси формування інформаційної безпеки на національному рівні та в окремих економічних суб’єктах. Цій проблематиці присвячені праці зарубіжних та

вітчизняних вчених: О. Бойко, Дж. Воутерса, А. Глушко, Р. Грищука, А. Дмитренко, С. Єгоричевої, І.М. Козубцова, Г. Коца, О. Литвиненка, В. Ліпкана, С. Онищенко, Ю. Саліфу, А. Сінгха, Р. Слейтона, Н. Фісуненко, А. Хідорі, Л. Шостак, А. Янко, Г. Яровенко та інших.

Високо оцінюючи існуючий науковий доробок з проблематики дослідження, правомірно відмітити, що ряд питань щодо сутності інформаційної безпеки національної економіки, її місця в системі національної безпеки, методики оцінювання, механізму формування потребують уточнення. Відсутність системного бачення основних засад формування інформаційної безпеки національної економіки зумовили вибір теми дисертаційної роботи, обґрунтування мети та визначення завдань дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота відповідає пріоритетним напрямам наукових досліджень кафедри фінансів, банківського бізнесу та оподаткування Національного університету «Полтавська політехніка імені Юрія Кондратюка». Зокрема, в рамках виконання науково-дослідної роботи «Формування організаційно-економічних засад запобігання загрозам соціально-економічній безпеці України в умовах пандемії» (номер державної реєстрації 0122U001749, 2022–2023 рр.), автором запропоновані концептуальні положення щодо формування безпекоорієнтованого інформаційного середовища та обґрунтовано методичний підхід до оцінювання рівня інформаційної безпеки національної економіки на основі індикаторного підходу.

Мета і завдання дослідження. Метою дисертаційної роботи є вдосконалення теоретичних положень, науково-методичних підходів та надання практичних рекомендацій щодо формування інформаційної безпеки національної економіки.

Відповідно до поставленої мети в дисертації сформульовано та розв'язано наступні завдання:

– сформувати структуру та розвинути понятійно-категорійний базис інформаційної безпеки національної економіки;

– систематизувати та поглибити наукові підходи до ідентифікації ризиків та загроз інформаційній безпеці в умовах активізації процесів цифровізації;

– уточнити структуру інституційного забезпечення інформаційної безпеки національної економіки;

– здійснити моніторинг сучасних умов, тенденцій розвитку інформаційного середовища в Україні;

– надати пропозиції щодо науково-методичного підходу до оцінювання рівня інформаційної безпеки України;

– оцінити рівень інформаційної безпеки національної економіки України та з'ясувати взаємозв'язок з її економічною безпекою;

– обґрунтувати концептуальний підхід до забезпечення інформаційної безпеки національної економіки;

– розробити орієнтири державної політики щодо формування безпекоорієнтованого інформаційного середовища в Україні та забезпечення інформаційної безпеки національної економіки.

Об'єктом дослідження є процеси формування і забезпечення інформаційної безпеки національної економіки.

Предметом дослідження є науково-методичні та прикладні засади формування інформаційної безпеки національної економіки України.

Методи дослідження. Методологічною базою дослідження є фундаментальні положення економічної теорії, сучасні теорії безпекології, теорії державного регулювання економіки, наукові праці з питань управління національною економікою та забезпечення інформаційної безпеки.

Для досягнення поставленої мети та вирішення окреслених завдань у дисертаційній роботі використані загальнонаукові та спеціальні методи дослідження: діалектичний, системний та синергетичний підходи, аналіз і синтез, логічне узагальнення та групування, наукова абстракція, системний аналіз – при дослідженні теоретичних засад інформаційної безпеки національної

економіки; економіко-статистичний, графічний та ретроспективний аналіз – при визначенні тенденцій розвитку інформаційного середовища в Україні; порівняльний аналіз – при встановленні причинно-наслідкових зв'язків; нормування, згладжування, експертних оцінок та інтегрального оцінювання – при формуванні системи індикаторів та визначенні рівня інформаційної безпеки національної економіки; кореляційний і регресійний аналіз – при встановленні взаємозв'язків між інформаційною та економічною безпекою; системний підхід та структурно-логічний метод – при обґрунтуванні концептуальної моделі формування інформаційної безпеки національної економіки; метод ієрархій – при розробленні стратегічних напрямів державної політики забезпечення інформаційної безпеки національної економіки. Розрахунки здійснено з використанням програмних продуктів MiniTab, MS Excel.

Інформаційну базу дослідження сформували законодавчі та нормативно-правові акти Верховної Ради України та Кабінету Міністрів України, Укази Президента України, нормативно-правові акти профільних міністерств та відомств, аналітичні дані Європейського Союзу, Державної служби статистики України, Служби безпеки України та Департаменту кіберполіції України, Стратегія інформаційної безпеки України, Стратегія кібербезпеки України, офіційні дані досліджень міжнародних організацій, зокрема CSIS, матеріали інформаційно-аналітичних звітів міжнародних компаній (Microsoft), наукові праці вітчизняних і зарубіжних учених у сфері економічної та інформаційної безпеки, результати власних розрахунків автора.

Наукова новизна одержаних результатів. Результатом проведеного дослідження є отримання наступних наукових результатів:

удосконалено:

концептуальні засади формування інформаційної безпеки національної економіки в умовах цифровізації як системи цілей, принципів, методів, технологій цього процесу на основі синергетичного підходу, що обґрунтовується особливостями об'єкту дослідження (система інформаційної безпеки національної економіки розглядається як складна, нелійнійна, нерівноважна, з

елементами самоорганізації), які спрямовані на формування методологічного базису механізму забезпечення інформаційної безпеки національної економіки;

понятійний базис інформаційної безпеки національної економіки, що, на відміну від наявних підходів, враховує процеси цифровізації, у зв'язку з чим інформаційну безпеку національної економіки запропоновано розглядати як стан захищеності інформаційного середовища, що забезпечує реалізацію національних економічних інтересів, а також стійкість національної економіки до внутрішніх та зовнішніх, реальних і потенційних загроз, пов'язаних із активним розвитком процесів цифровізації;

науково-методичні підходи до комплексного оцінювання інформаційної безпеки національної економіки, які передбачають використання принципово нової системи індикаторів (індикаторів цифрової, інституційної, кіберспроможності національної економіки) з метою розрахунку інтегрального індексу, що дозволяє виокремити найбільш важливі проблеми з урахуванням домінуючих світових тенденцій розвитку цифровізації та обґрунтувати стратегічні напрями зміцнення інформаційної безпеки національної економіки;

набули подальшого розвитку:

наукова класифікація загроз інформаційній безпеці національної економіки, а саме, запропоновано розподіл загроз за об'єктами спрямування дестабілізуючих дій: макрорівень (держава), мезорівень (регіон, галузь), мікрорівень (підприємство), нанорівень (особа, домогосподарство), що дає можливість визначити важелі та інструменти побудови ефективної системи захисту інформаційних ресурсів і підвищення інформаційної безпеки на усіх зазначених рівнях;

науково-методичні підходи до обґрунтування ієрархії стратегічних орієнтирів забезпечення інформаційної безпеки національної економіки, які передбачають застосування методу аналізу ієрархій, що дає змогу визначити домінантність задекларованих напрямів реалізації Стратегії інформаційної безпеки та змістовно окреслити інструменти реалізації державної політики зміцнення інформаційної безпеки;

концептуальна модель механізму формування безпекоорієнтованого інформаційного середовища, яка, за відсутності подібного підходу, враховує синергетичні ефекти взаємодії суб'єктів різних його рівнів з метою захисту їх економічних інтересів на основі визначення принципів, критеріїв, методів оцінки та важелів формування, що дозволяє забезпечити розвиток національної економіки на засадах безпекоорієнтованості.

Практичне значення одержаних результатів полягає в тому, що основні наукові положення, методичні підходи й висновки доведені до рівня прикладних рекомендацій та є підґрунтям для вдосконалення системи забезпечення інформаційної безпеки національної економіки.

Науково-практичні результати дисертаційного дослідження пройшли апробацію та впроваджені у діяльність Комітету Верховної Ради України з питань гуманітарної та інформаційної політики (довідка від 27.12.2022 р. № К-04/633) при оновленні й удосконаленні законодавчої бази у сфері інформаційної політики та інформаційної безпеки, зокрема визначені стратегічні напрями державної політики в частині формування безпекоорієнтованого інформаційного середовища в Україні враховані під час опрацювання проєкту Закону України «Про внесення змін до деяких законів України щодо особливостей здійснення окремих повноважень Національною радою України з питань телебачення і радіомовлення в умовах воєнного стану»; Міжнародної торгової палати (ICC Ukraine) (довідка від 19.12.2022 р. № 282) при вдосконаленні механізмів забезпечення інформаційної безпеки як на рівні підприємств, так і національної економіки в цілому, спрямованих на попередження і запобігання ризиків та загроз ефективному функціонуванню бізнесу й національній економіці в умовах цифровізації; Спілки підприємців малих, середніх і приватизованих підприємств України (довідка від 07.03.2023 р. № 2) при розробці Програми дій Ради та виконавчої дирекції Спілки підприємців малих, середніх і приватизованих підприємств України по реалізації Основних напрямів розвитку Спілки, а також регіональних програм розвитку підприємництва щодо посилення достовірності, конфіденційності, цілісності інформації, яка циркулює на об'єктах економічної

інфраструктури в умовах зростання глобальних викликів; Департаменту економічного розвитку, торгівлі та залучення інвестицій Полтавської обласної військової адміністрації (довідка від 10.05.2023 р. № 15) при розробленні підходів до забезпечення інформаційної безпеки економіки на регіональному рівні, що ґрунтуються на виборі найбільш ефективних програмно-технологічних рішень для захисту інформації та попередження реалізації загроз, передбачає впровадження нових, більш дієвих механізмів управління економікою, спрямованих на посилення захищеності економічного та інформаційного середовища; Головного управління Державної казначейської служби України у Полтавській області (довідка від 23.05.2023 р. № 201801-14/3035-2023) при обґрунтуванні напрямів забезпечення захисту інформаційних ресурсів, безпечного функціонування інформаційно-обчислювальної та внутрішньої платіжної систем установи, нейтралізації потенційних та мінімізації реальних ризиків і загроз в інформаційному середовищі.

Результати дисертаційного дослідження впроваджено в освітній процес Національного університету «Полтавська політехніка імені Юрія Кондратюка» при викладанні таких навчальних дисциплін, як «Соціально-економічний розвиток територій та територіальних громад», «Моделювання економічних ризиків», «Методологія наукових досліджень у сфері безпекознавства», «Організація та управління системою фінансово-економічної безпеки підприємств», «Організація та управління інформаційно-аналітичним забезпеченням фінансово-економічної безпеки суб'єктів господарювання», «Управління захистом комерційної таємниці в банківських і фінансових установах», «Інформаційна безпека та захист інформації» (довідка від 07.09.2023 р. № 10-9/2005/1).

Особистий внесок здобувача. Дисертаційна робота є завершеним та самостійно виконаним науковим дослідженням, в якому удосконалено теоретичні підходи та надані практичні рекомендації щодо формування інформаційної безпеки національної економіки. Одержані автором наукові результати знайшли відображення в опублікованих працях. Особистий внесок

автора у результати досліджень, опублікованих у співавторстві, конкретизовано у наведеному списку публікацій.

Апробація результатів дисертації. Основні положення і результати дисертаційного дослідження пройшли апробацію й отримали схвальну оцінку на міжнародних наукових та науково-практичних конференціях, у тому числі: III Міжнародній науково-практичній конференції «Розвиток фінансового ринку в Україні: загрози, проблеми та перспективи» (м. Полтава, 2021 р.), Міжнародній науково-практичній конференції «Молодіжна наука заради миру та розвитку» (м. Чернівці, 2022 р.), Міжнародній науково-практичній Інтернет-конференції «Сталий розвиток: виклики та загрози в умовах воєнного стану» (м. Полтава, 2022 р.), Міжнародній науково-практичній Інтернет-конференції «Економічна безпека: держава, регіон, підприємство» (м. Полтава, 2022 р.), International conference «Recent advances in science» (Boston, USA, 2023), 4th International scientific and practical conference «Scientific research in the modern world» (Toronto, Canada, 2023), III International Scientific and Theoretical Conference «Modernization of science and its influence on global processes» (Bern, Swiss Confederation, 2023).

Публікації. Основні результати дослідження за темою дисертації опубліковано у 14 наукових працях, з яких 2 статті у закордонних виданнях, проіндексованих у базі даних Scopus, 4 статті у наукових фахових виданнях, 8 тез доповідей у матеріалах міжнародних наукових та науково-практичних конференціях. Загальний обсяг публікацій – 6,95 д.а., з яких особисто автору належить 5,53 д.а.

Структура й обсяг дисертації. Дисертаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел й додатків. Загальний обсяг роботи складає 211 сторінок, що містить 41 рисунків, 19 таблиць та 9 додатків. Список використаних джерел містить 192 найменувань.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ

1.1. Інформаційна безпека національної економіки: зміст та місце в системі національної безпеки України

Процес цифровізації охопив усі галузі економічної діяльності в Україні та світі. Економічний вплив інформаційно-комунікаційних технологій на галузі економіки чи сфери життя (на макрорівні), конкретні продукти чи послуги (на мікрорівні) визначається доданою вартістю. Цифрові інструменти та технології дають змогу підвищити рівень виробництва інноваційної продукції, скоротити період від розроблення ідеї до реалізації готової продукції, забезпечити відповідний рівень рентабельності від упровадження передових технологій і створити конкурентні переваги для держави.

Водночас цифровізація є не тільки інструментом реалізації національних економічних інтересів, здатним створити нові можливості для зміцнення економічної безпеки держави, але й джерелом нових ризиків та загроз безпеці національної економіки за всіма її складовими (макроекономічна, соціальна, виробнича, фінансова, енергетична, зовнішньоекономічна, інвестиційно-інноваційна, продовольча, демографічна безпека). Мова йде, у першу чергу, про кібератаки та кіберзлочини, динаміка яких характеризується геометричною прогресією та спричиняє величезні втрати світової економіки.

В умовах поглиблення процесів цифровізації відбулася принципова зміна структури економіки та продуктивних сил. Інформація завжди була одним з універсальних та важливих видів ресурсів. Втім сьогодні інформація виступає безпосередньою продуктивною силою, найважливішим фактором виробництва поряд з традиційними – землею, працею, капіталом.

Розглядаючи інформацію з точки зору економічної теорії, як домінуючий виробничий фактор, її правомірно визначити як сукупність відомостей, даних, що відображають відносини й процеси, пов'язані з виробництвом, розподілом, обміном та споживанням матеріальних і нематеріальних благ, і є корисними для економічних суб'єктів. Універсальний характер інформації в умовах цифровізації полягає в тому, що вона виступає одночасно і предметом, і засобом праці, пронизує усі фактори, залучені у процес виробництва [1]. Ефективне функціонування економічної системи ґрунтується на використанні інформаційно-технологічних досягнень у виробництві в поєднанні з комплексними інтегрованими рішеннями інформаційної підтримки.

Унікальність інформації як виробничого фактору обумовлена поєднанням рідкості й поширеності, скінченності та невичерпності [2, 3]. Жоден інший фактор виробництва не характеризується такими категорійно протилежними властивостями. Рідкість інформації полягає у її корисності та економічній ефективності для окремих категорій споживачів, водночас існує можливість її широкого розповсюдження. Інформація як ресурс характеризується невичерпністю в процесі споживання (використання), для неї не властивий фізичний знос. Втім інформація може втратити економічну цінність через зменшення актуальності або неможливості її застосування.

Посилення ролі інформації в економіці підтверджується формуванням нової течії економічної теорії, яка досліджує проблематику інформаційної нерівності («асиметричної інформації») та її вплив на розвиток економічних систем.

На противагу традиційній неокласичній теорії, положення якої ґрунтувалися на здатності прийняття економічними суб'єктами оптимальних (раціональних) рішень, що здатні забезпечити максимальну ефективність функціонування економіки країни [4], проведені представниками теорії «асиметричної інформації» дослідження показали, що в сучасних умовах суб'єкти економічних відносин володіють різним обсягом інформації про стан

ринків, відповідно, не завжди діють ефективно і можуть стримувати економічний розвиток держави.

Ці дослідження були проведені науковцями Джорджом Акерлофом, Майклом Спенсом та Джозефом Стігліцом [5–8], які сформували теорію інформації в економіці, в рамках якої запропонували моделі ринкової рівноваги з асиметричною інформацією, що пояснюють роль та значущість інформації в різних економічних процесах – від сільськогосподарських до фінансових ринків. Вчені доводять, що врахування інформаційної асиметрії дозволяє зрозуміти реальні економічні процеси, а усунення асиметрії є ключовим напрямом державної політики щодо підтримки ефективності ринкового саморегулювання.

В цьому аспекті необхідним виступає забезпечення оптимальності інформаційних потоків, тобто руху (передачі та обміну) інформації між економічними суб'єктами з урахуванням взаємозв'язків між ними. Циркуляція інформаційних потоків в економічній системі являє собою інформаційний обмін та безпосередньо впливає на рівень інформаційної асиметрії, що актуалізує питання забезпечення достовірності, доступності, цілісності інформаційних ресурсів та захищеності інформаційного середовища загалом від можливих ризиків і загроз.

У наукових джерелах поняття «інформаційне середовище» використовується для опису сукупності інформації, інформаційних потоків, інформаційної інфраструктури, суб'єктів інформаційних відносин та взаємозв'язків між ними. Інтегрування новітніх інформаційних технологій і цифрових інновацій в усі галузі економіки та їх вплив на економічні процеси концептуально означає становлення інформаційного середовища як невід'ємної складової економічної системи, формування принципово нової структури національної економіки, де інформація виступає головним ресурсом.

У сучасних дослідженнях переважна більшість науковців підходять до розгляду національної економіки як системи. Гринів Л. С, Кічурчак М. В. [9, с. 16] вважають національну економіку організаційно-економічною системою взаємопов'язаних сфер господарської діяльності, яка характеризується

технологічною та територіально-галузевою пропорційністю, обмежена державними кордонами. Круш П. В. трактує національну економіку, як «економіку певної країни, що має ознаки економічної системи (загальне) та власні особливості і принципи розвитку (особливе), що проявляються в таких формах: економічний потенціал, структура господарського комплексу та галузей господарства, внутрішні чинники соціально-економічного розвитку, господарський механізм регулювання та координації та ін.» [10, с. 8].

Мочерний С. В., Устенко О. А., Ларіна Я. С., Юрій С. І. розглядають національну економіку як систему економічних відносин між людьми в процесі взаємодії з розвитком продуктивних сил у всіх сферах суспільного виробництва, цілісність якої, у рамках єдиної централізованої держави, гарантується відповідним економічним механізмом [11, с. 576]. Ряд науковців [12, с. 10] вважають національну економіку структурно і організаційно єдиною системою взаємозв'язаних галузей і сфер діяльності, якій властива пропорційність, взаємозумовленість розміщення на території, обмеженій державними кордонами. Згідно з підходом авторів [13], національна економіка є економічною системою, в якій завдяки стабільним, динамічним, повторюваним і стійким зв'язкам поєднані умови й фактори виробництва, результати діяльності, сукупність економічних агентів та економічних відносин, інститути, традиції, принципи й механізми господарювання, що у своїй взаємодії утворюють єдиний господарський комплекс.

Національну економіку зарубіжні вчені трактують як економіку нації в цілому, яка є економічною одиницею і зазвичай вважається унікальною, що перевищує суму окремих одиниць усередині неї [14].

Аналізуючи наведені визначення, правомірно виділити характерні риси національної економіки:

– національна економіка є системою, якій притаманні складність, стійкість та структурна зв'язність;

– ефективність функціонування національної економіки залежатиме від раціональної пропорційності між її підсистемами;

– національна економіка схильна до змін і, при відповідних інституційних умовах, здатна стабільно розвиватися;

– головними ознаками національної економіки є національний суверенітет, територіальна визначеність, ресурсно-виробничий потенціал, господарсько-організаційна структура, товарообмінні ознаки;

– статичні, динамічні та синтетичні властивості національної економіки проявляються під впливом часу.

В основу концептуального розуміння національної економічної системи правомірно покладено технолого-сингулярний вектор її розвитку, який характеризується зростанням ролі інформації як головного виробничого ресурсу, частки сектору інформаційно-комунікаційних технологій у ВВП, формуванням глобального інформаційного простору, де відбувається ефективна інформаційна взаємодія економічних суб'єктів.

Інформація є основою для формулювання стратегічних, тактичних та оперативних задач економічного розвитку на макро-, мезо-, мікро- та нанорівнях [15]. Водночас в умовах цифровізації та поширення таких феноменів як інформаційні й гібридні війни інформація стала чинником, здатним дезорганізувати державне управління, фінансову систему, призвести до технологічних аварій, воєнних конфліктів [16]. Так, військове вторгнення російської федерації на територію суверенної незалежної України супроводжується розгорнутою агресором війною на інформаційному полі, яка завдає не менше шкоди, ніж прямі воєнні дії. Потреба підтримки національної економіки під час зовнішньої агресії передбачає необхідність забезпечення її функціонування на засадах інформаційної захищеності.

Ретроспективний аналіз теоретичних напрацювань засвідчив, що безпека національної економіки розглядається через призму досягнення стійкості, незалежності, ефективності у протистоянні зовнішнім і внутрішнім дестабілізуючим чинникам. Водночас, актуалізація інформаційної безпеки як основи функціонування національної економіки на засадах захищеності потребує переосмислення категорійного базису, уточнення змістового

наповнення окремих категорій, впровадження нових понять і встановлення структурно-логічних зв'язків між ними.

Термін «національна безпека» з'явився на початку XX ст. 26-й президент США Т. Рузвельт цю категорію визначив як сукупність умов, що надійно забезпечують національний суверенітет, захист стратегічних інтересів і повноцінний розвиток суспільства, життя і здоров'я всіх його громадян.

На сучасному етапі розвитку людства, незважаючи на, здавалося б, зрозумілу змістовну наповненість поняття безпеки, у зарубіжній і вітчизняній літературі використовують кілька десятків трактувань, що свідчить про неоднозначність його змісту, а також про відсутність єдиного наукового підходу до визначення цієї категорії. Семантичний аналіз визначення поняття безпеки засвідчує відсутність принципових суперечностей з цього питання між різними науками, які займаються вивченням проблеми. Наявність розбіжностей у наукових поглядах вказує на різні підходи до цієї проблеми, які пояснюються не методологічними особливостями, притаманними тій чи іншій науці, а суб'єктивним чинником, тобто позицією конкретного автора.

Останнім часом в Україні сутність категорії «безпека» набула нового системного і глибокого сенсу захисту життєво важливих інтересів від ризиків, загроз і небезпек. У відповідності до статті 3 Конституції України декларується, що «людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю» [17].

Варто погодитися з Л. М. Шипіловою, котра відмічає, що дефініції головним чином визначаються природою об'єкта дослідження і залежать лише від суб'єктивних уявлень. З погляду вичерпності визначення поняття «безпека» є імперативним, тож логічним є академічний підхід, який визначає поняття безпеки в тісному зв'язку з поняттям «система», а своєю чергою поняття «система забезпечення національної безпеки» включає державні та недержавні органи, які в межах своєї компетенції гарантують безпеку особи, суспільства і держави на різних рівнях [18].

О. І. Барановський, на основі онтологічного підходу до категорії «безпека», доводить внутрішню суперечливу єдність із дефініцією «небезпека». Безпека становить єдність наявності та відсутності небезпеки. Неузгодженість єдності небезпеки і безпеки виражається і в тому, що небезпечне для одного водночас є безпечним для іншого. Небезпека і безпека – це «два боки однієї медалі», єдність протилежностей, що забезпечує розвиток системи та її гармонію. Провідну роль у цій гармонії відіграє безпека, яка виступає гарантією збереження системи. Науковець розкриває генезис безпеки з філософської, соціологічної та релігійної точки зору [19].

Таким чином, безпека є найважливішою історичною й економічною категорією, що забезпечує дієздатність та життєдіяльність національної економіки і економічних суб'єктів усіх рівнів, їх захищеність від внутрішніх і зовнішніх загроз.

Актуальність проблематики безпеки стала основою для формування нової галузі знань – безпекології, необхідність виокремлення якого обґрунтував В. А. Ліпкан [20], та окреслив ключові завдання наукових досліджень – визначення категорійного базису, загальних і специфічних закономірності функціонування безпекових систем та структурування національної безпеки, яка є складним, полісистемним явищем.

Національна безпека у різних країнах трактується по-різному. У Законі України «Про національну безпеку України» національна безпека тлумачиться як «захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз» [21]. З позиції застосування у дослідженні системного підходу правомірно відмітити, що національна безпека містить складові (структуру), які, своєю чергою, теж мають свої складові, і вони теж тощо. Саме це підкреслює полісистемний характер національної безпеки, коли існують системи вищих і нижчих рівнів (рангів). Водночас підсистема національної безпеки є «надсистемою» для складових безпеки наступного рівня,

а підсистеми третього рівня виступають «надсистемою» для складових четвертого рівня тощо.

Невід'ємним елементом системи національної безпеки та фундаментальною категорією безпекології є економічна безпека різних рівнів та суб'єктів.

Еволюція теоретичних концепцій економічної безпеки на макрорівні (безпеки національної економіки), фундаментальною основою яких визначено захист національних економічних інтересів від реальних та потенційних загроз, бере початок з моменту утворення соціальних організацій і формування державності. Тому окремими питаннями безпеки національної економіки, зокрема, уявленням про економічні інтереси як категорію економічної теорії та їхній захист від різного роду ризиків і загроз, займалися ще античні мислителі Арістотель, Епікур, Демокріт і Платон. Подальші дослідження категорії «економічна безпека» по відношенню до національної економіки (макрорівень) проводилися в рамках формування наступних теорій економічної безпеки держави: камералістської – теорія забезпечення зовнішньоекономічної безпеки через впровадження ввізних мит (40-і рр. XIX ст.); кейнсіанської – концепція забезпечення захищеності від внутрішніх макроекономічних загроз (депресії й безробіття) шляхом використання державних субсидій, замовлень, контролю (30-ті рр. XX ст.); інституціональної – теорія захисту від адміністративних бар'єрів, що обмежують розвиток конкуренції та спричиняють появу тіньової економіки (80-ті рр. XX ст.).

Фактори розвитку економіки на засадах безпечного функціонування стали об'єктами наукових досліджень у теорії економічного розвитку (Й. Шумпетер, Р. Солоу); кейнсіанській та неокейнсіанській моделі економічного зростання (Є. Домар, Дж. Роінсон, А. Гаррод); економічній теорії добробуту (Дж. Бентам, А. Пігу, В. Парето); теорії ризиків (Дж. Кларк, Ф. Найт); теорії катастроф (Е. Ласло, Т. Оліва); теорії самоорганізації та системного упорядкування (І. Блауберг, Р. Барталанфі, Г. Хакен); моделі рівноважного зростання та

оптимального розміру бюджету й державних видатків (Р. Барро) [22–25; 26, с. 143–147; 27] та ін.

У сучасних умовах проблеми забезпечення стійкості національної економіки від негативного впливу широкого спектра загроз у контексті забезпечення економічної безпеки держави широко аналізуються у працях вітчизняних учених.

Зокрема, В. М. Геєць трактує дефініцію «економічна безпека держави» як можливість економіки забезпечувати незалежний і вільний розвиток та стабільність країни, достатній оборонний потенціал для забезпечення здатності реагування в будь-яких несприятливих умовах [28, с. 5]. З. С. Варналієм економічна безпека розглядається як комплекс заходів по забезпеченню стійкого розвитку й удосконаленню структури економіки, що передбачає формування механізму протидії зовнішнім і внутрішнім загрозам [29, с. 396]. На думку О. С. Власюка, економічна безпека є багатовекторною категорією, що визначає мету, стратегічні пріоритети й критерії оцінки стану забезпечення сталого економічного розвитку країни, тобто є своєрідним каркасом національної безпеки, який забезпечує економічну і загальну стабільність держави. Це поняття також включає в себе сукупність умов, що дають змогу країні ефективно захищати власні економічні інтереси, задовольняти потреби держави і суспільства, забезпечувати сталий економічний розвиток, протистояти зовнішнім економічним загрозам і використовувати власні конкурентні переваги [30, с. 8]. Економічна безпека, згідно з підходом А. О. Єпіфанова, являє собою якісний стан економічної системи, який характеризує здатність забезпечити нормальні умови функціонування системи та її розвитку в межах визначених завдань і в разі формування різних внутрішніх і зовнішніх загроз – система, здатна протистояти і забезпечувати свою працездатність [31, с. 18]. У свою чергу, Я. А. Жаліло трактує економічну безпеку держави як багатофакторну категорію, що визначає здатність економіки до розширеного відтворення з метою задоволення потреб населення та протидії негативному впливу чинників, що загрожують її стабільному та збалансованому розвитку [32, с. 141–143].

Теоретичне узагальнення наукових досліджень дозволило систематизувати підходи до визначення поняття «економічна безпека» (рис. 1.1).

Рис. 1.1. Систематизація основних концептуальних наукових підходів до визначення категорії «економічна безпека держави»

Джерело: складено автором

Враховуючи, що інформація є стратегічним національним ресурсом, а від рівня її захищеності залежить захист економічних інтересів громадян, бізнесу та держави, значення інформаційної складової для забезпечення як економічної, так і національної безпеки загалом зростає.

Необхідність забезпечення інформаційної безпеки задекларована на найвищому рівні. Статтею 17 Конституції України визначено, що поряд із захистом суверенітету і державної цілісності України, «забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [17].

Концептуальні положення інформаційної безпеки закріплені у Стратегії інформаційної безпеки, згідно з якою інформаційна безпека України – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі, скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [33].

Досліджуючи категоріальну визначеність інформаційної безпеки у нормативно-правових актах, наукових працях правомірно відмітити два аспекти її трактування. З одного боку, інформаційна безпека є самостійним елементом національної безпеки країни, а з іншого – інтегрованою складовою будь-якої іншої безпеки, зокрема, економічної.

В економічних дослідженнях поняття «інформаційна безпека» розглядається з позиції захисту національних економічних інтересів та національної економіки. Важливість та необхідність забезпечення інформаційної безпеки обґрунтовується співвідношенням витрат на впровадження й експлуатацію систем інформаційної безпеки і фінансових втрат у випадку реалізації загроз [34]. Роль інформаційної безпеки визначається здатністю заходів і методів інформаційної безпеки, як важливого елемента економічної безпеки на всіх рівнях, протидіяти загрозам економічній цілісності держави. Аналіз напрацювань фахівців у безпековій сфері дозволяє систематизувати концептуальні наукові підходи щодо тлумачення категорії «інформаційна безпека» (рис. 1.2).

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Закон України «Про Концепцію Національної програми інформатизації» [35]	Закон України «Про національну безпеку України» [21]	Стратегія інформаційної безпеки [33]	Харченко Л. С., Ліпкан Н. А., Логінов О. В. [36]
Інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки	Поняття «інформаційна безпека» не розкривається, увага фокусується на напрямах державної політики щодо забезпечення інформаційної безпеки, кібербезпеки	Інформаційна безпека України – складова частина національної безпеки України…	Інформаційна безпека –це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СТАН ЗАХИЩЕНОСТІ

Стратегія інформаційної безпеки [33]	Гасеський В. К., Авраменко В. А. [37]	Баранов О. П. [38]	Петрик В. М. [39]
Інформаційна безпека України – стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом	Інформаційна безпека – це стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації	Інформаційна безпека – це стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій	Інформаційна безпека –це стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток, технічний, інтелектуальний, соціально-політичний, морально-етичний, за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СТАН СИСТЕМИ ТА ПРОЦЕС ЗАХИСТУ

Ліпкан В. А. [40]	Нижник Н. Р., Ситник Г. Л., Білоус В. Т. [41]	Данільян О. Г., Дзьобань О. П., Панов М. І. [42]	Литвиненко О. В. [43]
Інформаційна безпека – це стан, який характеризується відсутністю небезпеки, тобто чинників і умов, які загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища	Інформаційна безпека – стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни	Інформаційна безпека – це безпека об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошення даних про той чи інший об'єкт, що є державною таємницею	Інформаційна безпека як єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності

Рис. 1.2. Підходи до трактування поняття «інформаційна безпека»
Джерело: узагальнено автором за вказаними даними

У науковій літературі на сьогодні сформувалося три основні концептуальні підходи до дефініції сутності інформаційної безпеки:

1) як складової національної безпеки;

2) як стану захищеності інформаційного середовища й національних інтересів від можливих загроз;

3) як стану системи, що здатний забезпечити цільові параметри безпеки.

Перший підхід ґрунтується на нормативно-правовому аспекті і визначає інформаційну безпеку як пріоритетну функцію державної політики. Втім, у положеннях законодавчих актів, де інформаційна безпека розкривається як складова національної безпеки (Закон України «Про Концепцію Національної програми інформатизації», Закон України «Про національну безпеку України»), відсутня норма, що містить дефініцію поняття «інформаційна безпека».

Другий підхід пов'язує інформаційну безпеку зі станом захищеності інтересів на різних рівнях (держави, суспільства, особи). Тобто акцент зроблено на меті формування й забезпечення інформаційної безпеки з урахуванням деструктивних наслідків реалізації можливих загроз. Втім, цей підхід не враховує категорійну різницю між дефініціями «інформаційна безпека» та «безпека інформації», пов'язуючи загрози інтересам суб'єктів виключно з неповнотою, невчасністю й недостовірністю інформації, та залишаючи поза увагою вплив інформаційних потоків, інформаційних технологій, інформаційної інфраструктури, суб'єктів інформаційних відносин і взаємозв'язків між ними на економічні процеси.

Згідно з третім підходом інформаційна безпека розглядається як стан системи, за якого вона здатна протистояти ризикам і загрозам, та не ініціювати їх виникнення. Водночас інформаційна безпека трактується як процес, тобто певний порядок дій щодо захисту інформації, інформаційних ресурсів, який передбачає застосування ряду правових, організаційних, технічних, правових інструментів для упередження реалізації загроз. Враховуючи комплексність підходу, доцільно відмітити, що не розкривається економічний аспект інформаційної безпеки. Перетворення інформації в стратегічний ресурс розвитку економіки, поширення процесів цифровізації, зростання частки сектору інформаційно-комунікаційних

технологій, актуалізує сприйняття інформаційної безпеки як базису безпечного функціонування та розвитку національної економіки.

На основі екстраполяції наукових підходів до визначення економічної безпеки в інформаційну площину, враховуючи дефініції поняття «інформаційна безпека» правомірно виокремити сутнісні характеристики феномену «інформаційна безпека національної економіки», а саме: стан захищеності інформаційного середовища як невід'ємної складової економічної системи; захист інформації як стратегічного національним ресурсу і основи економічних інтересів громадян, бізнесу, держави від реальних та потенційних загроз; ключовий фактор забезпечення розвитку національної економіки на безпекових засадах в умовах цифровізації.

Багатоаспектність категорії зумовлює необхідність доповнення існуючих підходів. На основі узагальнення концептуальних положень, інформаційну безпеку національної економіки доцільно розглядати як стан захищеності інформаційного середовища, що забезпечує захист і реалізацію національних економічних інтересів, стійкість суб'єктів на макро-, мезо-, мікро- та нанорівнях до внутрішніх та зовнішніх, реальних та потенційних загроз, у тому числі, пов'язаних із активним розвитком ІТ-технологій.

Спираючись на конфліктний та захисний підходи до розуміння ключової категорії науки про інформаційну безпеку національної економіки в умовах цифровізації, дотримуємося позиції, що найважливішими елементами інформаційної безпеки національної економіки є забезпечення стабільності, стійкості, економічної незалежності й здатності до саморозвитку та прогресу національної економіки.

Системний підхід дослідження полягає в наступному:

– у логічно обґрунтованій послідовності комплексного вивчення об'єкта, виявленні та залученні резервів підвищення ефективності його функціонування;

– у дослідженні кожного об'єкта як складового елементу економічної системи вищого порядку, а результатів його діяльності – як наслідків взаємодії внутрішніх та зовнішніх чинників;

– у сприйнятті об’єкта як системи чи впорядкованої сукупності взаємопов’язаних елементів, які організовано взаємодіють в напрямі досягнення спільної мети.

Розглядаючи інформаційну безпеку національної економіки з позицій системного підходу [44], як інтегровану складову будь-якої іншої безпеки, доцільно представити її структуру, тобто спосіб закономірного зв’язку компонентів системи.

Система інформаційної безпеки національної економіки як сукупність взаємопов’язаних елементів, що взаємодіють із середовищем як єдине ціле й відокремлені від нього, має ряд властивостей [34, 45, 46]:

– взаємозалежність, взаємозв’язок і взаємодія системи із зовнішнім середовищем;

– адаптивність – прагнення системи досягти стану стійкої рівноваги, що передбачає адаптацію її параметрів до умов зовнішнього середовища (проте «нестійкість» не в усіх випадках є дисфункціональна для системи, вона може бути умовою динамічного розвитку);

– комунікативність – наявність складної ієрархічної сукупності істотних зв’язків між системою і середовищем;

– емерджентність – цілі та функції компонентів системи не завжди відповідають цілям і функціям системи в цілому;

– мультиплікативність – як позитивні, так і негативні ефекти функціонування компонентів системи мають властивість множення, а не додавання;

– синергізм – односпрямованість (або цілеспрямованість) дій компонентів посилює ефективність функціонування системи.

Базисом інформаційної безпеки національної економіки є захист національних економічних інтересів. Потрібно враховувати той факт, що загрози безпеці національної економіки впливають на інтереси всіх суб’єктів економічних відносин.

У вітчизняних наукових джерелах виділяють три типи інтересів:

– інтереси домогосподарств;

– інтереси суб’єктів господарювання;

– національні економічні інтереси.

Системність у дослідженні передбачає врахування усіх типів інтересів. В протилежному випадку неможливо зробити висновок про те, чи є заходи, що проваджуються в напряму забезпечення інформаційної безпеки, найбільш оптимальними.

Об’єктами інформаційної безпеки національної економіки є держава, суспільство, окремі громадяни, домогосподарства, підприємства, організації, установи, окремі території та основні елементи системи економічної безпеки. Одночасно держава є не лише об’єктом, а й основним суб’єктом інформаційної безпеки національної економіки та реалізує свої функції в цій сфері через органи законодавчої, виконавчої й судової гілок влади. Це не виключає участі громадян та їхніх об’єднань у забезпеченні економічної безпеки. Крім того, подібні заходи повинні всіляко заохочуватися державою. Втім участь громадян в забезпеченні безпеки національної економіки неможлива без усвідомлення ними важливості цього державного питання і виявлення активної громадянської позиції.

Необхідно детально зупинитися на формуванні вихідних умов системи інформаційної безпеки національної економіки:

1) економічна незалежність, тобто можливість здійснювати державний контроль над національними ресурсами, використовувати національні конкурентні переваги для забезпечення рівноправної участі держави в міжнародній торгівлі;

2) стійкість і стабільність, що передбачає забезпечення міцності і надійності усіх елементів економічної системи, захисту усіх форм власності, створення гарантій ефективної підприємницької діяльності та стримування дестабілізуючих чинників;

3) здатність до саморозвитку і прогресу, тобто можливість самостійно реалізовувати та захищати національні економічні інтереси, систематично здійснювати модернізацію виробництва, розвивати інтелектуальний і трудовий потенціал країни, проваджувати ефективну інвестиційну й інноваційну політику;

4) еквіфінальність (від лат. aequi – рівний, співрозмірний), тобто здатність досягнути стану захищеності національної економіки, через використання різних методів, що відрізняються траєкторією впливу.

Вищезазначені наукові підходи візуалізовані на рисунку 1.3 у вигляді концептуальної моделі системи інформаційної безпеки національної економіки.

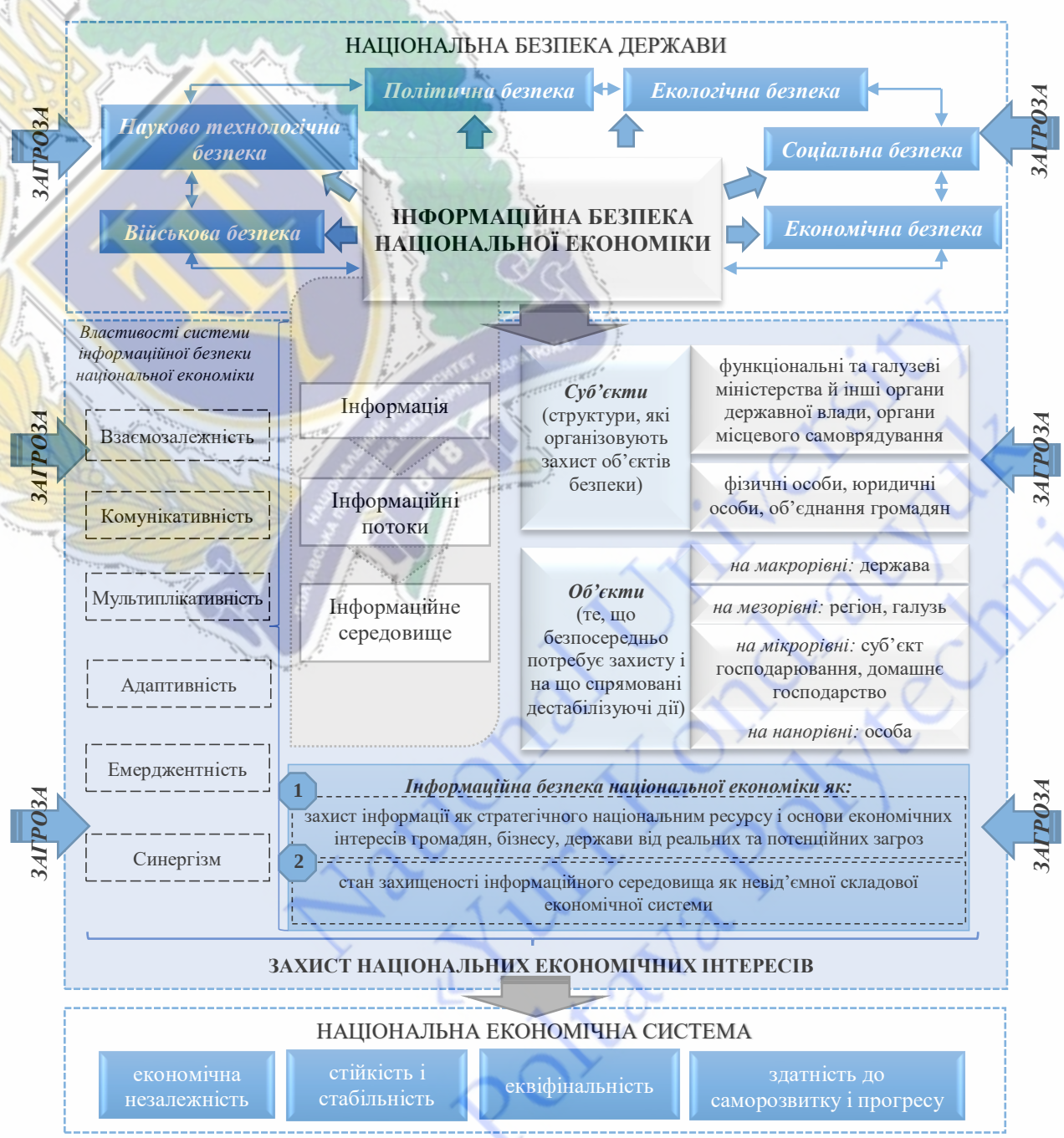

Рис. 1.3. Концептуальна модель системи інформаційної безпеки національної економіки

Джерело: розроблено автором

Таким чином, обґрунтовані на основі системного підходу концептуальні основи інформаційної безпеки національної економіки правомірно визначити базисом для окреслення пріоритетних напрямів її забезпечення. Водночас необхідним постає систематизація теоретичних уявлень щодо ідентифікації загроз інформаційній безпеці національної економіки в контексті цифрової трансформації, що є умовою їх своєчасного виявлення та ефективної протидії.

1.2. Ідентифікація загроз інформаційній безпеці в умовах цифровізації

З позиції захисного підходу у процесі дослідження сутнісного змісту інформаційної безпеки національної економіки категорійним базисом правомірно визначити такі поняття як «виклик», «ризик», «загроза» та «небезпека». Ці категорії мають деструктивний та протилежний до стану безпеки характер і потребують проведення етимологічного аналізу.

Найменш розкритим в економічній літературі є поняття «виклик». Вітчизняними вченими цей термін досить часто використовується як відповідник до англійського слова «challenge», що трактується в Оксфордському словнику як нове або складне завдання, яке перевіряє чиїсь здібності [47]. У відповідності до Великого тлумачного словника сучасної української мови слово «виклик» тлумачиться як «вимога, спонукання до будь-яких дій, відносин; заклик до змагання, до участі в чому-небудь; категорична, різка пропозиція вступити в боротьбу, поєдинок» [48, с. 136]. Науковці у галузі безпекології дотримуються думки, що виклик є сукупністю обставин, необов’язково деструктивного впливу, проте які вимагають своєчасного реагування.

Результати аналізу трактування поняття «ризик» в економічній літературі свідчать про відсутність єдиного підходу, що пояснюється, в тому числі, різносторонністю проявів цього феномена. Систематизація та узагальнення наукових підходів (Додаток А) дозволили окреслити найпоширеніші дефініції категорії «ризик»:

– усвідомлена небезпека виникнення небажаної події в будь-якій системі, наслідки якої визначені в часі та просторі;

– невизначеність, пов’язана з імовірністю виникнення несприятливих ситуацій і наслідків під час реалізації проекту;

– імовірність несприятливих наслідків;

– об’єктивно-суб’єктна категорія, пов’язана з подоланням невизначеності та конфліктності в ситуації неминучого вибору, що відображає ступінь досягнення очікуваного результату, невдачі та відхилення від цілей, з урахуванням впливу контрольованих і неконтрольованих факторів за наявності прямих та зворотних зв’язків.

З моменту становлення безпекології як науки одним із головних об’єктів вивчення визначено категорію «загроза». Тому спектр наукових підходів до трактування цього поняття досить широкий. Більшість вітчизняних науковців розуміють загрозу як безпосередню небезпеку нанесення чи заподіяння шкоди інтересам об’єкту безпеки, створення перепон у їх реалізації, досягненні цілей та констатований негативний вплив на стійкість і стабільність діяльності. Узагальнюючи досліджені наукові підходи (Додаток Б), загрози безпеці правомірно визначити як конкретні внутрішні або зовнішні умови й фактори, які здійснюють негативний вплив на процеси функціонування і розвитку та для їх відновлення потребують зниження кількісних чи зміни (пом’якшення) якісних характеристик.

Етимологічний зміст категорії «небезпека» засвідчує його походження від слова «безпека» й означає «відсутність безпеки». Тому поняття «безпека» і «небезпека» правомірно окреслювати як категорійно протилежні за значенням: стан захищеності інтересів та, відповідно, стан незахищеності. Науковцями дефініція «небезпека» розглядається як можливість виникнення обставин, за яких поєднання різних чинників можуть деструктивно впливати на складну систему, що спричинить погіршення чи неможливість її функціонування і розвитку [64]. Таким чином, під «небезпекою» доцільно розуміти об’єктивно

існуючу реальність, що здатна порушити стан рівноваги суб'єктів та спричинити негативні наслідки.

Узагальнюючи дефініції зазначених категорій, необхідним є встановлення концептуальних підходів щодо визначення взаємозв'язків між ними (рис. 1.4).

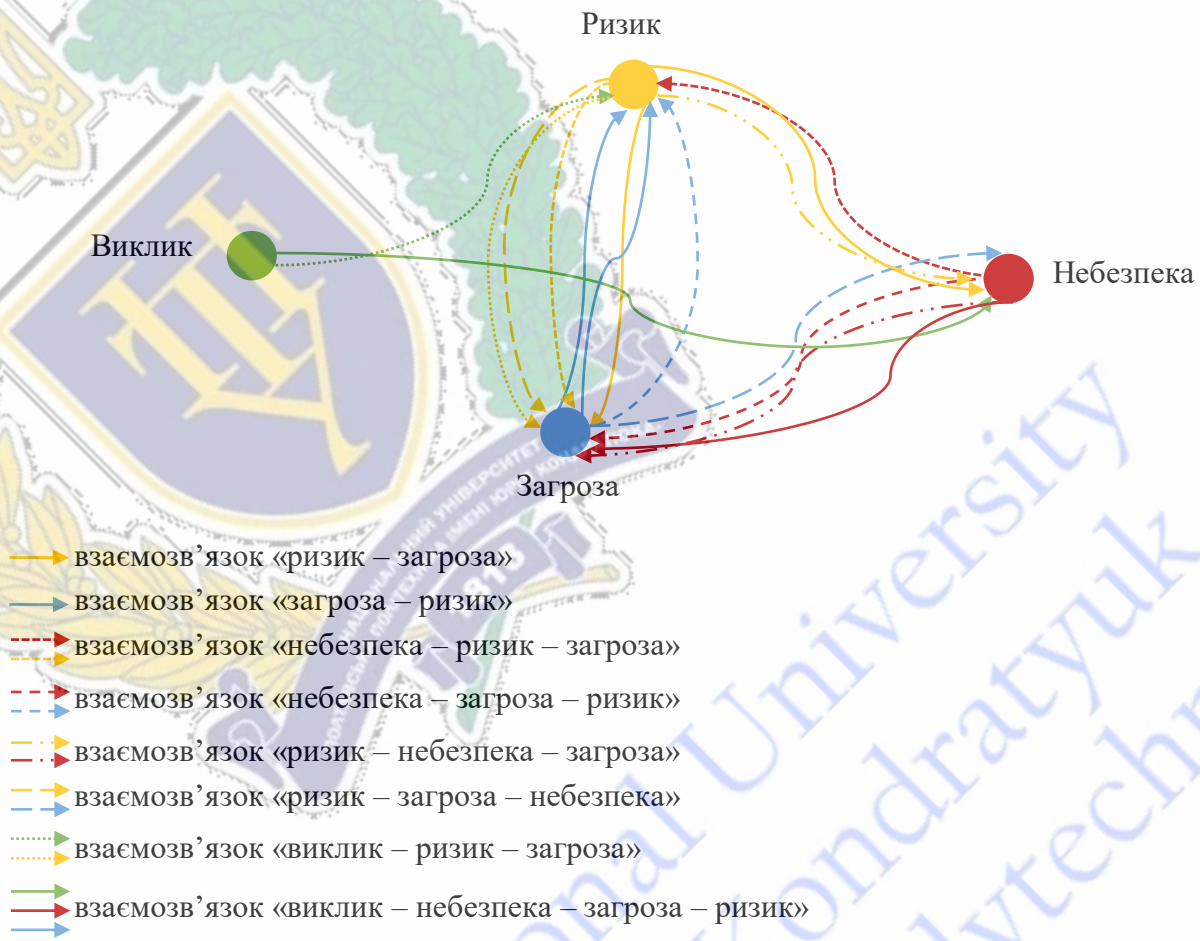

Рис. 1.4. Взаємозв'язок понять «виклик», «ризик», «загроза» та «небезпека»

Джерело: узагальнено автором за даними [47–63]

Згідно з підходом Т. Васильців [56], О. Барановського [65] ризики генерують потенційну можливість завдання шкоди і виступають джерелами загроз. Розглядають ризик як результат впливу загроз на об'єкт безпеки І. Мігус, С. Лаптєв [49]. Ряд авторів вихідною точкою формування ризиків та загроз визначають небезпеку [50, 66].

Науковий підхід, що відстоює взаємозв'язок «ризик – небезпека – загроза», визначає загрозу частиною ризику й конкретною формою небезпеки, що виникає в результаті негативного наслідку прийнятого рішення або невиправданого ризику [51, 59, 67]. Колектив авторів у складі Н. Нижник, Г. Ситник, В. Білоус, розглядають ризик як первинну категорією, а небезпека випливає із загрози і є конкретним її проявом [68]. У дослідженнях І. Бойко обґрунтовується взаємозв'язок «виклик – ризик – загроза» [55], а Л. Калашнікової – логічний ряд «виклик – небезпека – загроза – ризик» [69].

Таким чином, проведений етимологічний аналіз понять «виклик», «ризик», «загроза» та «небезпека», аналіз наукових підходів до визначення взаємозв'язків між цими категоріями дає можливість зробити певні узагальнення. Виклик являє собою об'єктивний стан напруженості, що потребує реагування. На відміну від ризиків та загроз, він сам по собі не є деструктивним фактором. Наявність виклику не впливає на стан безпеки. Але за відсутності належного реагування може стати підґрунтям виникнення ризиків. Вважаючи, що безпека – це відносний стан, за якого всі системи об'єкта безпеки функціонують з максимальною ефективністю, то ризик можна асоціювати з моментом появи можливої небезпеки. Його можна охарактеризувати як явище, яке містить у собі негативні фактори, здатні деструктивно вплинути на об'єкт безпеки. Ризик правомірно визначити умовою появи небезпеки. Тобто після його появи об'єкт потрапляє у стан небезпеки, проте небезпека в цей момент є гіпотетичною. Небезпека стає реальною, коли з'являється загроза як реальна подія. Загроза є активним деструктивним фактором та емпіричним проявом небезпеки. Відповідно небезпеку правомірно розглядати як імовірність заподіяння шкоди об'єкту безпеки, яка знаходиться в динамічному стані і зазнає змін під впливом конкретних ризиків та загроз в наявних обставинах.

Логіку окреслених міркувань можна обґрунтувати наступним чином. Процеси цифровізації стали викликом для інформаційної безпеки на усіх рівнях. За умови ігнорування цього виклику виникає ризик, пов'язаний із можливою втратою даних, порушенням цілісності та конфіденційності інформації тощо.

З’являється небезпека для інформаційного середовища. Водночас такі поняття як кібератаки являються загрозами інформаційній безпеці, оскільки безпосередньо здатні завдати шкоди об’єкту, на який спрямована їх дія.

Враховуючи семантичну схожість дефініцій «ризик», «загроза», «небезпека» та відмінність характеристик можливості прояву деструктивних факторів візуалізація взаємозв’язку понять «виклик», «ризик», «загроза» та «небезпека» представлена наступною схемою (рис. 1.5). На рисунку візуалізовано залежність діями суб’єкта щодо протидії небезпеці та ступенем її розвитку. Високий ступінь стійкості до потенційно небезпечних чинників нейтралізує їх, створюючи умови захищеності та потенційної безпеки. Зі збільшенням імовірності виникнення шкідливих подій та їхніх наслідків, коли дії з їхньої нейтралізації неможливі або недостатні, формується стан небезпеки. У разі порушення балансу між ступенем імовірності негативних чинників і реалізацією засобів захисту від них формується стан підвищеної ймовірності негативного впливу від настання тих чи інших подій, який можна кваліфікувати як загрозу.

Інформаційна безпека в умовах воєнного стану безумовно являється основною детермінантою забезпечення стабільного функціонування національної економіки України. Необхідність формування інформаційної безпеки зумовлюється наявністю загроз та їх деструктивними наслідками [70]. Основою своєчасного виявлення, унеможливлення реалізації та мінімізації негативного впливу загроз інформаційній безпеці є їх оперативна ідентифікація.

Процес формування інформаційної безпеки національної економіки має ґрунтуватися саме на ідентифікації загроз її стабільному функціонуванню. Згідно з Великим тлумачним словником сучасної української мови [48] ідентифікувати означає ототожнювати, тобто встановлювати подібність певного об’єкту відомому на підставі збігу ознак. Основними завданнями ідентифікації загроз інформаційній безпеці національної економіки є їх своєчасне виявлення, встановлення характеру, напряму впливу. Забезпечення ідентифікації загроз ґрунтується на їх систематизації. Систематизацію загроз інформаційній безпеці національної економіки доцільно здійснювати з урахуванням чинного законодавства.

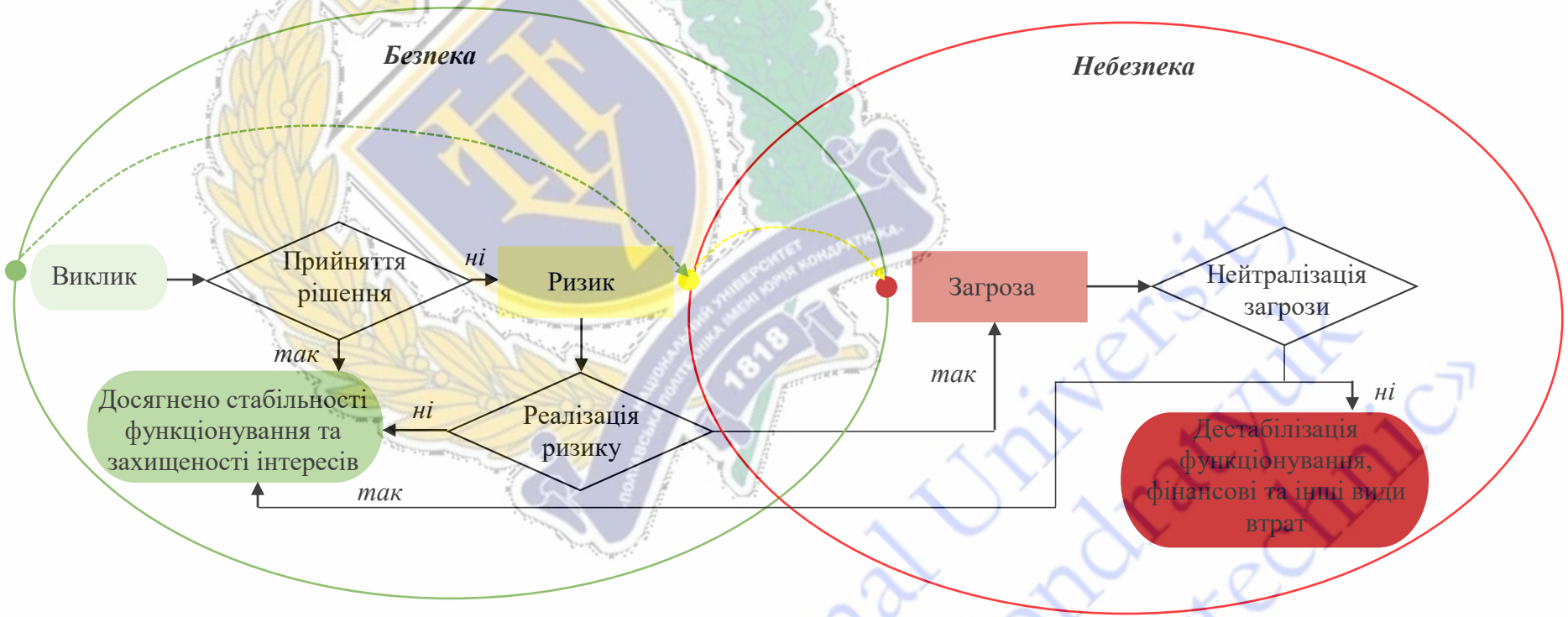

Рис. 1.5. Візуалізація проявів деструктивних факторів та їх впливу на інформаційну безпеку національної економіки

Джерело: складено автором

Стратегією національної безпеки України (введена в дію Указом Президента України від 14 вересня 2020 року № 392/2020) у переліку поточних та прогнозованих загроз національній безпеці і національним економічним інтересам визначено стрімкий розвиток інформаційних технологій, що сприяє поширенню таких явищ як злочинність у кіберпросторі, деструктивна пропаганда в інформаційному середовищі; слабкість системи стратегічних комунікацій; відсутність цілісної інформаційної політики держави; несанкціоновані втручання кіберхарактеру в функціонування об'єктів критичної інфраструктури [71]. Стратегією інформаційної безпеки (введена в дію Указом Президента України від 28 грудня 2021 року № 685/2021) визначається поняття «інформаційна загроза» як «потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні» [33]. Цим законодавчим актом загрози інформаційній безпеці розмежовуються за рівнем реалізації на глобальні та національні. У Стратегії кібербезпеки України (введена в дію Указом Президента України від 26 серпня 2021 року № 447/2021) виокремлено такі види загроз як гібридна агресія (кібервійна), кібертероризм, кіберзлочинність, кібершпигунство [72].

Систематизація загроз інформаційній безпеці згідно нормативних документів України подано на рисунку 1.6.

Аналізуючи Стратегію національної безпеки України, правомірно зазначити, що описані загрози можна розділити на дві групи: зовнішні та внутрішні. Втім варто зауважити, що зазначений перелік загроз не може вважатися вичерпними та константними. В умовах посилення процесів глобалізації та цифровізації, загострення військових конфліктів в Україні і світі загрози трансформуються та модифікуються [73].

Рис. 1.6. Загрози інформаційній безпеці України відповідно до нормативних документів

Джерело: систематизовано автором на основі [33, 71, 72]

У зв’язку з динамічними умовами функціонування національної економіки та світової економічної системи загалом величина впливу внутрішніх і зовнішніх загроз інформаційній безпеці постійно змінюється. Оскільки можливості мінімізації внутрішніх загроз набагато вищі, і їх створюють виключно органи влади та суспільство, пріоритетним завданням є побудова стійкої національної інформаційної інфраструктури.

У відповідності до положень Стратегії інформаційної безпеки виокремлено глобальні і національні загрози інформаційній безпеці України, які впливають на інтереси особи, суспільства та держави. Водночас Стратегією не враховано інтереси економічних суб’єктів (фізичних осіб – підприємців, домогосподарств, підприємств). Хоча саме ця категорія зазнає найбільших фінансових втрат у разі реалізації загроз інформаційній безпеці, що безпосередньо впливає на економіку України.

У Стратегії кібербезпеки хоча й наводиться найбільш короткий перелік загроз, втім враховується їх деструктивний вплив на національну економіку України та світову економіку загалом. Виокремлені кібервійна, кібертероризм, кібершпигунство, кіберзлочинність також потребують деталізації. Так, у рамках кіберзлочинності можна виділяти реалізацію таких загроз як фішинг, інсайдерські атаки, цільові кібератаки й DDoS-атаки.

Аналіз доктринальних, довідкових та наукових джерел дозволив розширити класифікацію загроз інформаційній безпеці національної економіки. Зокрема, за джерелами походження доцільно виділити комунікативні загрози і технологічні загрози. До першої групи відносяться деструктивний інформаційний вплив на громадян через соціальні мережі, дезінформаційні компанії, обмеження свободи слова тощо. Друга група загроз інформаційній безпеці передбачає завдання шкоди національній економіці та національній безпеці України через несанкціоноване втручання в діяльність інформаційних систем [74, с. 189–199; 75].

За спрямуванням науковці виокремлюють наступні загрози інформаційній безпеці: загрози порушення конфіденційності («витік» інформації з обмеженим

доступом, неправомірне використання якої спричинить значні втрати власника, в тому числі фінансові; неправомірний доступ до інформації); загрози порушення цілісності (модифікація інформації, що зберігається в інформаційній системі, неправомірна зміна даних), загрози порушення доступності (їх реалізація унеможливлює або ускладнює доступ до інформаційних ресурсів) [76, с. 120–129; 77, с. 167–169].

В аспекті формування та забезпечення інформаційної безпеки національної економіки найбільшої вагомості набуває класифікація загроз на реальні та потенційні. У випадку реальної загрози дестабілізація об'єкту впливу є неминучою та не обмежена часом і простором. Реалізація потенційних загроз можлива за певних умов інформаційного середовища, наявності вразливості інформаційної системи, низького чи недостатнього рівня захищеності інформаційних ресурсів та ін.

З урахуванням філософської концепції загальної об'єктивної зумовленості явищ і процесів, за ступенем детермінізму можна виділити: випадкові загрози, які можуть бути реалізовані чи не відбутися (наприклад, загроза DDoS-атаки на суб'єкт господарювання); закономірні загрози, які характеризуються стійким, повторюваним характером та зумовлені об'єктивними умовами розвитку цифровізації й посилення напруги на світовій арені (кібератаки хакерських угруповань на офіційні сайти державних органів влади) [78, 79].

Класифікацію загроз інформаційній безпеці національної економіки доцільно також доповнити розподілом за об'єктами, тобто на що безпосередньо спрямовані дестабілізуючі дії: макрорівень (держава), мезорівень (регіон, галузь), мікрорівень (суб'єкт господарювання), нанорівень (домогосподарство, особа) [73]. Такий розподіл дасть можливість визначити важелі й інструменти побудови ефективної системи захисту інформаційних ресурсів та підвищення інформаційної безпеки на усіх зазначених рівнях.

Систематизована та удосконалена багаторівнева класифікація загроз інформаційній безпеці національної економіки (рис. 1.7) дозволяє ідентифіковувати загрози та вживати превентивних заходів.

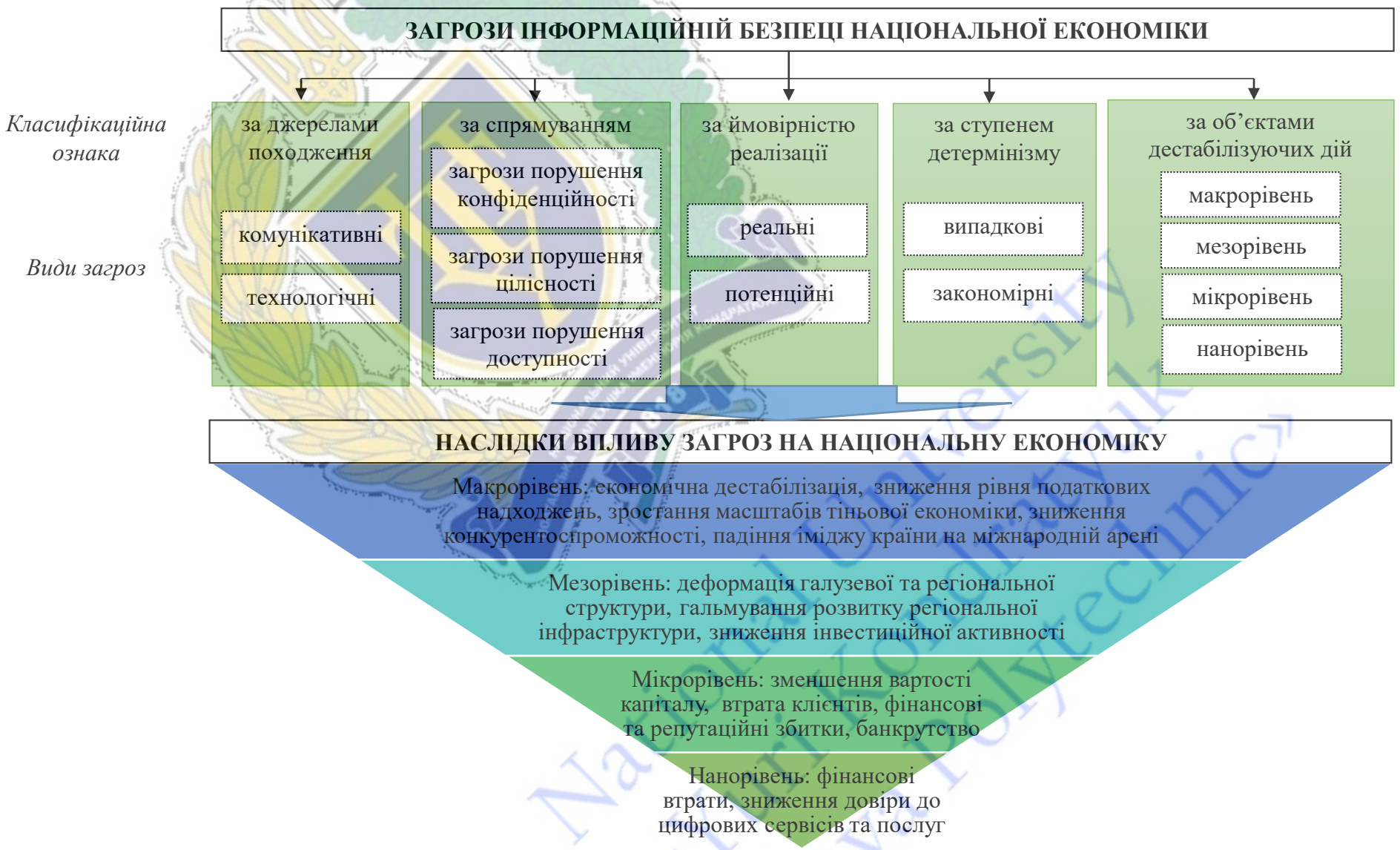

Рис. 1.7. Класифікація загроз інформаційній безпеці національної економіки та наслідки їх впливу

Джерело: розроблено автором

Водночас вона є умовною, оскільки в умовах стрімкого цифрового розвитку загрози швидко модифікуються та трансформуються.

Доцільність використання удосконаленої класифікації при дослідженні загроз інформаційній безпеці підтверджується тим, що виокремлення реальних та потенційних загроз, авторський розподіл загроз за об'єктами є базисом для формування напрямів запобігання, протидії, мінімізації негативного впливу від їх реалізації. Крім того, систематизація загроз за наведеними ознаками у нормативно-правових актах дозволить підвищити їх регуляторний вплив та сформувати безпекоорієнтоване інформаційне середовище в Україні.

Водночас, високий рівень розвитку кіберпростору та організації кіберзагроз підтверджує необхідність зміни парадигми стратегії кібербезпеки: вона має ґрунтуватися не на апостеріорній реакції, а на засадах прогнозування та планування захисту від майбутніх дій кіберзлочинців. З цією метою необхідно постійно аналізувати сучасні тренди кіберзагроз.

Найнебезпечнішим трендом на макрорівні є використання кіберзброї в конфліктах між країнами, що набуває нових форм. У цьому деструктивному діалозі кібератівність відіграє провідну роль. Атаки на критичну інфраструктуру, цілеспрямована дестабілізація функціонування мережі Інтернет в окремих країнах відкривають нову епоху проведення кібератак.

Основними кіберзагрозами бізнесу, тобто мікрорівня, правомірно виділити наступні [80–82].

1. Фішинг – один із найбільш поширених видів кіберзлочинів, який призводить до значних фінансових втрат щорічно. Мета полягає у викраденні конфіденційних та облікових даних, таких як логін для входу або дані кредитної картки, а потім обманом змусити людей встановити зловмисне програмне забезпечення.

2. Зловмисне програмне забезпечення – хакери розробляють шкідливе програмне забезпечення, з метою отримання постійного бекдор-доступу до пристроїв компанії, який складно виявити. У цьому разі вони зможуть віддалено керувати пристроєм і використовувати його для викрадення даних, дослідження

локальної мережі або надсилання спаму із зараженого пристрою. 91% кібератак починаються з фішингового електронного листа. Фішинг і шкідливе програмне забезпечення тісно взаємопов'язані.

3. Програми-вимагачі – це форма шкідливого програмного забезпечення, яка може завдати катастрофічних збитків бізнесу. Програми-вимагачі блокують інформаційну систему фірми та позбавляють доступу до критично важливих даних, доки не буде заплачений викуп за поверення конфіденційної інформації та відновлення контролю над системами. Програми-вимагачі ставлять бізнес перед важким вибором: заплатити зловмисникам або втратити дані та доступ до них. Більшість компаній вирішують платити хакерам. Втім, навіть за умови сплати викупу, власники бізнесу не завжди отримують доступ до своїх даних.

4. Компрометація корпоративної електронної пошти (BEC – Business Email Compromise) – один із найдорожчих кіберзлочинів. Процес починається з того, що злочинці зламують корпоративні системи, щоб отримати доступ до інформації про їхні платіжні системи. Потім вони обманюють співробітників і спонукають їх здійснювати платежі на фальшиві банківські рахунки замість реальних. Підроблені запити на оплату буває складно ідентифікувати, оскільки вони практично ідентичні реальним запитам. BEC може призвести до величезних фінансових втрат для бізнесу, а відстеження і повернення платежів, якщо взагалі відбудеться, може зайняти місяці.

5. Внутрішні загрози – частина співробітників компанії мають доступ до конфіденційної інформації. Незалежно від того, чи вони є нинішніми чи колишніми співробітниками, партнерами чи підрядниками, 25% витоків даних відбуваються через внутрішні загрози. Недобросовісні працівники можуть діяти через жадібність, незадоволені співробітники – через злобу. У будь-якому разі, поширення ними важливої інформації здатне завдати значних фінансових збитків.

6. Ненавмисне розголошення – співробітники можуть випадково розголосити конфіденційну інформацію і завдати фінансової шкоди компанії.

Помилка може полягати у випадковому надсиланні електронного листа всім співробітникам компанії. Великі підприємства піддаються особливому ризику, за умови, що співробітники мають доступ до основних баз даних.

7. Розвідка сховища – компанії зберігають величезні обсяги даних у хмарі та вважають їх автоматично захищеними. Втімце не завжди так. Кіберзлочинці шукають незахищене хмарне сховище з метою отримання доступу до даних. Хмарні інтерфейси не завжди підтримуються безпечними системами, що робить їх легкою мішенню для кіберзлочинців. Ймовірно, найвідомішим прикладом став злам незахищеного хмарного бакету S3, що містив величезну кількість секретних даних Агентства національної безпеки. Дані було зламано 2017 року, що мало серйозні наслідки. Компанії повинні усвідомлювати, що зберігання конфіденційної інформації є ризиковим, якщо не вживати відповідних заходів.

8. Соціальна інженерія – передбачає створення кіберзлочинцями фіктивних осіб та профілів в соціальних мережах, щоб завоювати довіру своїх жертв та отримати інформацію, необхідну для завершення операції. Ці відносини використовуються для досягнення кінцевих цілей – фішингу та встановлення шкідливого програмного забезпечення, щоб заблокувати роботу бізнесу, отримати доступ до даних компанії та отримати фінансову вигоду. Будь-яку форму соціальної взаємодії, кінцевою метою якої є обман бізнесу, можна класифікувати як соціальну інженерію.

На рисунку 1.8 схематично представлено загрози кібербезпеці суб’єктів господарювання відповідно до звіту за 2022 рік про глобальні ризики у сфері IT від Cisco Talos. Основні причини найдорожчих витоків даних пов’язані з зазначеними кібератаками.

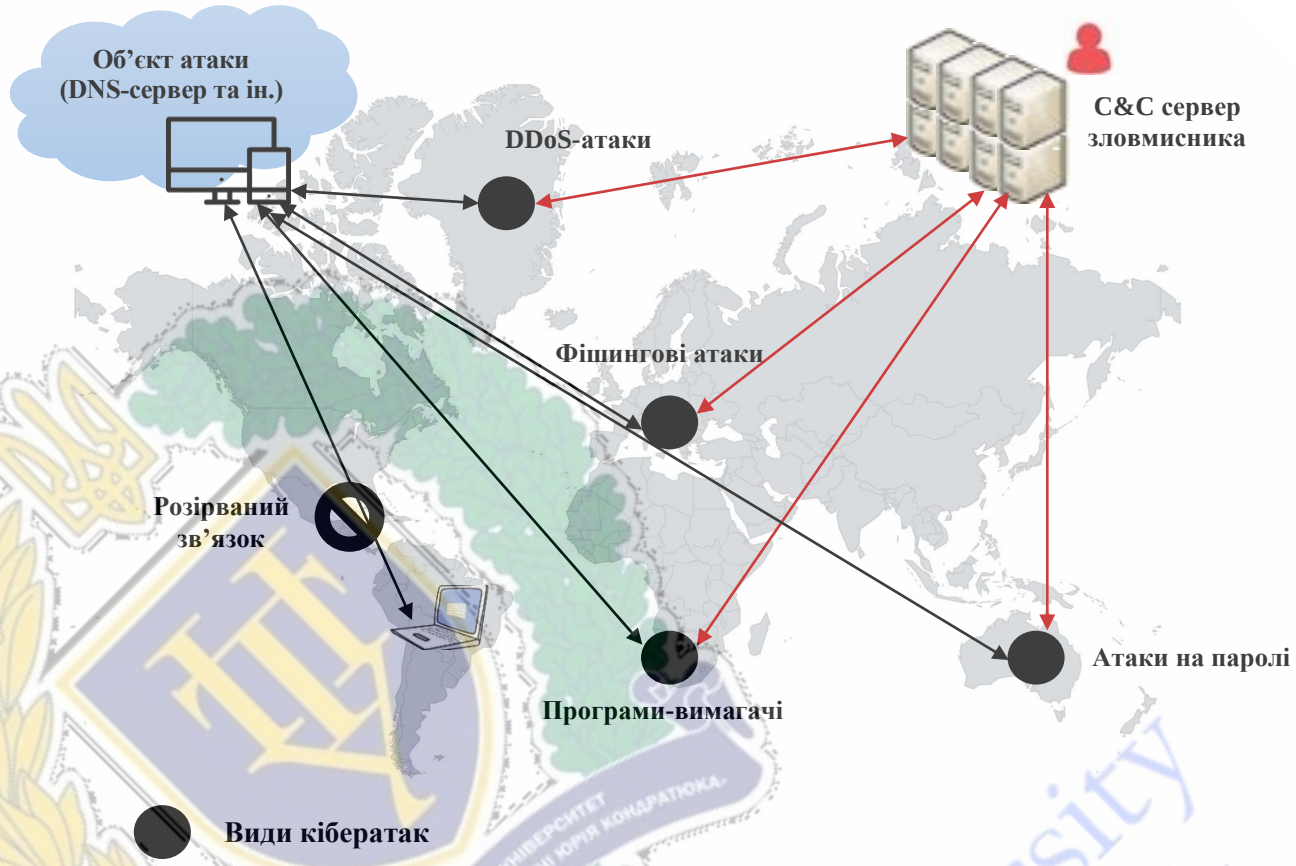

Рис. 1.8. Найпоширеніші види кібератак

Джерело: побудовано автором за [83]

Фінансові збитки від кібератак складно оцінити. Проте, за орієнтовними підрахунками експертів, світова економіка зазнає втрат, що вимірюються трильйонами доларів США. Проте найбільша небезпека – не в сумі грошей, а в загрозі бізнесу. Так, кожна п'ята компанія, що піддалася кібератаці, була змушена закрити свій бізнес. У 48% компаній сталася втрата даних або обладнання, а з 42%, які заплатили викуп, чверть – не отримали обіцяні дані [84].

Окреслені загрози інформаційній безпеці вимагають провадження дієвих механізмів їх попередження та нейтралізації як на рівні держави, так і на рівні суб'єктів господарювання.

Отже, поглиблення цифрових трансформацій національної економіки внаслідок інформаційно-технологічного розвитку спричиняє вільне й неконтрольоване переміщення інформаційних потоків в глобальному інформаційному просторі та призводить до виникнення потенційних і реальних загроз інформаційній безпеці України. Протистояти ризикам та загрозам в

інформаційній сфері у сучасних умовах здатна ефективно організована система забезпечення інформаційної безпеки, що має ґрунтуватися на взаємодії державних органів, недержавних структур і громадян. В цьому аспекті питання формування сприятливого регуляторного середовища як основи розроблення ефективних форм реалізації державної політики забезпечення інформаційної безпеки національної економіки набуває особливої актуальності.

1.3. Інституційне забезпечення інформаційної безпеки національної економіки

Теоретико-методологічним підґрунтям дослідження інституційного забезпечення інформаційної безпеки правомірно вважати фундаментальні положення інституціоналізму та неоінституціоналізму [85]. Доцільність використання інституціонального підходу аргументується ефективністю його інструментарію у процесах формування інституційної архітектоніки й механізму забезпечення інформаційної безпеки.

Дослідження інституційного забезпечення інформаційної безпеки доцільно розпочати з деталізації та систематизації категоріального апарату, зокрема понять «інститут», «інституції», «інституційне забезпечення».

Аналіз наукових підходів до визначення категорій «інститут» та «інституція» дає змогу дійти висновку про однорідність їхнього економічного змісту та відмінності у ступені системності. Інституцію правомірно вважати системою, при цьому інститут є фундаментальним і неподільним елементом інституції [86].

Один із основоположників інституціоналізму, Дж. Коммонс, характеризує інституції у вузькому значенні, як «систему законів чи природних прав, в межах яких індивіди діють як в'язні» та у широкому – як «колективну дію по контролю, лібералізації та розширенню індивідуальної діяльності» [87]. Згідно з підходом представника неоінституціоналізму Д. Норта поняття «інституції» охоплює

будь-які види обмежень, створені для спрямування людської взаємодії в певному напрямі. Призначення інституцій у суспільстві полягає в тому, щоб зменшити невизначеність через встановлення постійної структури людської взаємодії [88]. Зазначений підхід підтримав Е. Остром, який визначає інституції як сукупність правил прийняття рішень у певних сферах діяльності [89].

Формування категоріальної системи інституціоналізму продовжує досліджуватися та удосконалюватися вітчизняними вченими. Зокрема, Т. Гайдай розглядає поняття інституції за функціональним призначенням – як систему норм і правил, які упорядковують, структурують соціально-економічну взаємодію економічних суб'єктів і соціальних груп [90].

Узагальнюючи підходи представників «нового» інституціоналізму, доцільно визначити інститути як систему норм і правил, що містить у собі формальні та неформальні правила, які регулюють відносини між економічними суб'єктами й передбачають наявність організаційних структур для досягнення певних цілей.

Формою прояву інституцій є інститути. Сутнісними характеристиками цієї категорії можуть бути як правові норми, так і порядок встановлення зв'язків між ними, «що дає змогу упорядкувати (регламентувати) взаємовідносини між суб'єктами права з метою надання їм стійкого характеру, для чого створюються відповідні організаційні структури й органи контролю» [91]. Поняття «інститут» є базовим у теорії інституціоналізму і позначає певний звичай, порядок, прийнятий у суспільстві, а також їхнє закріплення у вигляді закону або організації.

Т. Веблен, як основоположник інституціоналізму, визначає інститути як закріплення звичаїв і порядків у вигляді закону [92]. Згідно з підходом Дж. Коммонса провідними інститутами в державі є профспілки, політичні партії, корпорації, а фундаментальними інституційними дефініціями – «ринкова сила», «ринкові угоди», «діючий колективний інститут». Ці категорії визначають економічну поведінку в суспільстві [87].

Д. Норт визначає інститути суб'єктом інституційного механізму. Як зазначає Д. Норт «…не існує інших рішень, крім використання інституційних механізмів, щоб установити правила гри, і використання організації – щоб забезпечити дотримання цих правил» [88]. Дж. Ходжсон трактує поняття «інститут» як систему соціальних правил, а саме: «довготривала система укладених і вкорінених правил, що структурує соціальні взаємодії» [93].

Справедливо зазначає Д. Буркальцева, що аналіз інститутів повинен здійснюватися залежно від мікро- або макрорівнів дослідження. На мікрорівні виробники, підприємці та фінансові посередники організовують діяльність фірм, виконують функції з формування й обслуговування ринкової інфраструктури. На макрорівні роль основних суб'єктів, які виконують функції координації системи відіграють держава, домогосподарства, а також міжнародні інституційні організації [94].

У контексті проведеного дослідження інституційне забезпечення правомірно визначити як процес формування інституцій (формальні та неформальні норми, які впливають на поведінку суб'єктів) та інститутів (юридичні норми), які консолідовано у формі організацій (підприємства, інфраструктура, державні органи), законів (нормативно-правові акти) та правил у процесі еволюції суспільства [88].

Інституційне забезпечення інформаційної безпеки – це сукупність державних і недержавних інституцій, які забезпечують створення нормативно-правових, організаційних та економічних умов, необхідних для формування та реалізації ефективної державної політики у сфері інформаційної безпеки.

У складі інституційного забезпечення інформаційної безпеки правомірно виділити дві складові:

– інституційно-правове забезпечення;

– інституційно-організаційне забезпечення.

Вищим рівень інституційно-правового забезпечення інформаційної безпеки є міжнародні акти, зокрема документи Міжнародної організації зі стандартизації (International Organization for Standardization, ISO), Міжнародної

електротехнічної комісії (International Electrotechnical Commission, IEC), Організації Об'єднаних Націй (ООН) та її спеціалізованих установ – Міжнародного союзу електрозв'язку (International Telecommunication Union, ITU), Організації Об'єднаних Націй з питань освіти, науки і культури (United Nations Educational, Scientific and Cultural Organization, UNESCO) та ін.

Міжнародною організацією зі стандартизації спільно з Міжнародною електротехнічною комісією розроблено ряд міжнародних стандартів у сфері інформаційної безпеки, серед яких ISO/IEC 27000 – серія міжнародних стандартів, яка включає кращі практики і рекомендації в галузі інформаційної безпеки; CoBiT (Control Objectives for Information and Related Technology) – відкритий IT-стандарт, який містить положення щодо забезпечення IT-безпеки. Щодо Міжнародних стандартів серії ISO/IEC 27000, то вони включають близько 60-ти документів, які містять вимоги до системи інформаційної безпеки: від стандарту ISO/IEC 27001 до стандарту ISO/IEC 27799, зокрема ISO 27001 – система управління інформаційною безпекою, ISO 27005 включає рекомендації управління ризиками інформаційної безпеки, ISO 27017 містить рекомендації щодо заходів інформаційної безпеки для хмарних обчислень, ISO 27701 – система управління захистом даних.

Аналізуючи нормативний доробок ООН та її спеціалізованих установ, доцільно відмітити значний вклад UNESCO у нормативно-правове підґрунтя розвитку інформаційного суспільства та забезпечення інформаційної безпеки. Зокрема, організацією розроблено програми «Інформаційне суспільство для всіх» (1996 р.) та «Інформація для всіх» (2001 р.), концепти яких направлені на зменшення інформаційної асиметрії. Вагомий вклад у міжнародну нормотворчу діяльність зроблено Міжнародним союзом електрозв'язку, що приймає участь у розробці міжнародних стандартів у сфері інформаційної безпеки, в тому числі кібербезпеки, формує стратегічні документи з цих питань. Так, у 2007 році представлено Глобальну програму кібербезпеки (ITU-GCA), положеннями якої визначено цілі, принципи та стратегії розроблення законодавства у сфері боротьби з кіберзлочинністю. Також прийнято ряд резолюцій, спрямованих на

підвищення рівня захищеності при використанні інформаційно-комунікаційних технологій та зміцнення інформаційної безпеки.

Необхідно відмітити діяльність Європейського Союзу у напрямку створення інституційно-правового забезпечення інформаційної безпеки. Доктрина Європейського інформаційного суспільства була проголошена у 1994 році у доповіді М. Багнемана «Європа і глобальне інформаційне суспільство: рекомендації для Європейської ради ЄС» (Recommendations to the European Council «Europe and the global information society»). Ця доповідь вважається фундаментальною науково-аналітичною працею з проблематики впливу сучасних інформаційних технологій на економічний розвиток та суспільні трансформації. Подальші нормативно-проєктні напрацювання включають програми соціально-економічного розвитку, директиви інформаційної та кібербезпеки, які оновлюються та актуалізуються з урахуванням поширення процесів цифровізації.

Система нормативно-правових актів, що регулюють питання інформаційної безпеки в Україні включає: Конституцію України, Закон України «Про національну безпеку України», Закон України «Про інформацію», Закон України «Про Концепцію Національної програми інформатизації», Стратегію інформаційної безпеки, Стратегію кібербезпеки України, Концепцію розвитку цифрових компетентностей, Міжнародні стандарти серії ISO/IEC 27000, нормативні документи у сфері технічного захисту інформації та державні стандарти України стосовно створення і функціонування комп'ютерних систем захисту інформації, а також інші нормативно-правові акти, що регулюють відносини у сфері інформаційної безпеки.

До 2021 року інституційно-правове забезпечення інформаційної безпеки зводилося до опосередкованого розгляду окремих її аспектів або стосувалося системи технічного захисту інформації.

Так, статтею 17 Конституцією України, поряд із захистом суверенітету і державної цілісності України, передбачено що «забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього

українського народу» [17]. В Законі України «Про національну безпеку України» визначені напрями державної політики щодо забезпечення інформаційної безпеки, кібербезпеки [21]. Водночас, як доповнення, у Законі України «Про Концепцію Національної програми інформатизації» інформаційна безпека визнається як невід'ємна частина політичної, оборонної, економічної й інших складових національної безпеки [35]. Положеннями Закону України «Про інформацію» регулюються відносини у сфері захисту інформації, а одним із основних напрямів державної інформаційної політики визначається забезпечення інформаційної безпеки України [96].

Ухвалену Урядом у вересні 2021 року Стратегію інформаційної безпеки правомірно вважати концептуальною основою забезпечення інформаційної безпеки в Україні. Стратегією визначені методологічні аспекти забезпечення інформаційної безпеки України, упередження появи та мінімізації загроз національній безпеці в інформаційній сфері, захисту прав громадян на інформацію та захист персональних даних.

Таким чином, прийняття Стратегії інформаційної безпеки є свідченням усвідомлення необхідності забезпечення інформаційної безпеки України як основи захисту національних інтересів в умовах цифровізації. Цей документ окреслив вектори державної політики у зазначеній сфері та стане базисом для формування ґрунтовного інституційно-правового забезпечення інформаційної безпеки.

В цілому, інституційно-правове забезпечення інформаційної безпеки має бути спрямоване на регулювання взаємовідносин між суб'єктами інформаційної безпеки, регламентувати їх права, обов'язки та відповідальність; нормативне забезпечення дій суб'єктів інформаційної безпеки на різних рівнях – особи, суспільства, держави; встановлення порядку застосування важелів та інструментів забезпечення інформаційної безпеки

Таким чином, поняття «інституційно-правове забезпечення інформаційної безпеки» правомірно трактувати як нормативну форму реалізації функцій державних і недержавних інституцій у сфері забезпечення інформаційної

безпеки національної економіки та протидії ризикам і загрозам, спричинених поширенням негативних інформаційних впливів.

Інституційно-організаційне забезпечення пропонується розглядати як систему організацій (органів влади), які забезпечують формування та реалізацію державної політики у сфері інформаційної безпеки .

Органами державної влади, на які покладено функції формування та реалізації державної політики щодо інформаційної безпеки правомірно визначити: Президента України, Верховну Раду України, Кабінет Міністрів України, Міністерство оборони України, Міністерство цифрової трансформації, Міністерство культури та інформаційної політики України, Державну службу спеціального зв'язку та захисту інформації, Державний комітет телебачення і радіомовлення України, Раду національної безпеки і оборони України, Департамент кіберполіції Національної поліції України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України, а також місцеві органи виконавчої влади й органи місцевого самоврядування.

У структурі Верховної Ради України питання інформаційної безпеки належать до компетенції трьох профільних комітетів: Комітету з питань гуманітарної та інформаційної політики, Комітету з питань свободи слова та Комітету з питань цифрової трансформації. Формування державної політики у сфері інформації й інформаційної безпеки (окрім питань, які належать до сфери національної безпеки й оборони) знаходиться у предметі відання Комітету з питань гуманітарної та інформаційної політики. Діяльність Комітету з питань свободи слова спрямована на забезпечення свободи слова; захисту прав і свобод, гарантій безпечної діяльності працівників засобів масової інформації; прав громадян на інформацію. Основними завданнями Комітету з питань цифрової трансформації є здійснення законопроектної та контрольної діяльності у напрямку розвитку цифрового суспільства та цифрової індустрії в Україні; підтримки інновацій у сфері цифрового підприємництва та розвитку екосистеми стартапів; забезпечення кіберзахисту та кібербезпеки державних інформаційних ресурсів тощо [97].

Доцільно також відмітити наявність спеціальної посадової особи у структурі Верховної Ради України, яка виконує обов'язки щодо захисту персональних даних – Уповноваженого Верховної Ради України з прав людини [98]. З метою забезпечення здійснення контролю за виконанням законодавства в сфері захисту персональних даних у Секретаріаті Уповноваженого Верховної Ради України з прав людини функціонує Департамент з питань захисту персональних даних.

Президент України як Глава держави і Верховний Головнокомандувач Збройних Сил України, визначає державну інформаційну політику, політику у сфері захисту інформації, інформаційної безпеки та законодавчі основи її реалізації.

Рада національної безпеки і оборони України як координаційний орган при Президентові України уповноважена приймати рішення щодо визначення концептуальних підходів та напрямів забезпечення національної безпеки в цілому та, в тому числі, в інформаційній сфері з урахуванням масштабу потенційних і реальних загроз національним інтересам.

Як вищий орган у системі органів виконавчої влади Кабінет Міністрів України у відповідності до статті 116 Конституції України забезпечує інформаційний суверенітет України, реалізацію внутрішньої і зовнішньої інформаційної політики та державної політики інформаційної безпеки [17].

У Положенні «Про Міністерство культури та інформаційної політики» визначено, що Міністерство забезпечує формування і реалізацію державної політики у сферах культури, державної мовної політики, державного іномовлення, популяризації України у світі, а також інформаційного суверенітету України й інформаційної безпеки.

Міністерство цифрової трансформації є невід'ємним елементом інституційно-організаційного забезпечення інформаційної безпеки та забезпечує формування та реалізацію державної політики у сфері цифровізації, цифрових інновацій, цифрової економіки, електронного врядування й електронної демократії, розвитку інформаційного суспільства.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації як центрального органу виконавчої влади зі спеціальним статусом, згідно з чинним законодавством, є реалізація державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування Державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації.

Реалізацію державної політики в сфері протидії кіберзлочинності як невід'ємної складової державної політики у сфері інформаційної безпеки здійснює Департамент кіберполіції Національної поліції України.

Доцільно відмітити наявність у складі Центрального управління Служби безпеки України підрозділів, які виконують повноваження у сфері забезпечення інформаційної безпеки держави та реалізовують превентивні заходи щодо протидії кібератакам на комунікаційні системи державних органів та об'єкти критичної інфраструктури – Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки та Ситуаційного центру забезпечення кібербезпеки.

У чинному законодавстві не визначений спеціально уповноважений центральний орган виконавчої влади у сфері інформаційної безпеки України. Центральним органом виконавчої влади зі спеціальним статусом у сфері захисту інформації визначено Державну службу спеціального зв'язку та захисту інформації. Водночас особливий статус має Рада національної безпеки і оборони України, оскільки є єдиним органом, який має повноваження координувати та контролювати діяльність органів виконавчої влади з реалізації політики інформаційної безпеки України та вносити Президенту України пропозиції щодо її уточнення та ресурсного забезпечення [99]. Відсутність чіткої координації, розподілу функціональних обов'язків серед перелічених органів державної влади знижує рівень ефективності державної політики у сфері інформаційної безпеки. Враховуючи вищезазначене правомірно представити архітектоніку інституційного забезпечення інформаційної безпеки національної економіки (рис. 1.9).

Рис. 1.9. Інституційне забезпечення інформаційної безпеки національної економіки

Джерело: побудовано автором

Інституційний забезпечення інформаційної безпеки національної економіки є важливою структурною складовою державного механізму, що забезпечує формування норм і правил, які регламентують взаємодію економічних суб'єктів щодо запобігання загрозам інформаційній безпеці національної економіки. Система інституційного забезпечення інформаційної безпеки національної економіки має бути спрямована на превентивне виявлення, моніторинг і прогнозування загроз національним економічним інтересам; координацію повноважень органів державної влади щодо забезпечення інформаційної безпеки національної економіки; розроблення і реалізацію відповідних законодавчих та нормативно-правових актів щодо підтримки розвитку процесів цифровізації національної економіки на засадах інформаційної захищеності.

Зростання загроз інформаційній безпеці національної економіки є цілком об'єктивним процесом, зумовленим динамічними змінами економічної системи на основі розвитку інформаційних технологій, та актуалізує значення держави в реалізації ефективної політики забезпечення інформаційної безпеки національної економіки. Загрози інформаційній безпеці національної економіки здебільшого спрямовані на систему державної статистики; кредитно-фінансову систему; автоматизовані інформаційно-облікові системи органів державної влади, що забезпечують діяльність суспільства і держави в економічній сфері; системи бухгалтерського обліку підприємств, установ і організацій незалежно від форм власності; системи збирання, опрацювання, зберігання і передачу податкової, фінансової, біржової, митної інформації й інформації про зовнішньоекономічну діяльність держави, а також підприємств, організацій та установ незалежно від форм власності.

Інституційно-правове та інституційно-організаційне забезпечення інформаційної безпеки, враховуючи взаємозв'язки між суб'єктами (система державних і недержавних інституцій, а також громадян України), формують інституційне середовище інформаційної безпеки, ефективність функціонування якого визначатиме рівень захисту економічних інтересів громадян, суб'єктів

підприємництва та держави загалом як соціальних об’єктів інформаційної безпеки.

Підвищення ефективності інституційного забезпечення інформаційної безпеки національної економіки має передбачати реалізацію комплексу заходів, зокрема:

– докорінна реструктуризація системи державної статистичної звітності для забезпечення достовірності, повноти та безпеки інформації, шляхом запровадження юридичної відповідальності посадових осіб за підготовку первинної інформації, організації контролю за діяльністю служб з обробки та аналізу статистичної інформації;

– організація і здійснення державного контролю за створенням, розвитком і захистом систем і засобів збирання, оброблення, зберігання та передавання статистичної, фінансової, біржової, податкової та митної інформації;

– удосконалення національних сертифікованих засобів та методів захисту інформації, що циркулює в економічній системі;

– удосконалення нормативної правової бази, що регулює інформаційні відносини у сфері економіки.

Підсумовуючи вищезазначене, правомірно відмітити доцільність застосування інституціонального підходу. Адже це дало можливість вивчити концептуальні засади інформаційної безпеки та окреслити інституційну архітектоніку її забезпечення. Встановлено, що інституційне забезпечення інформаційної безпеки являє собою складну багатокомпонентну систему, яка включає інституційно-правове та інституційно-організаційне забезпечення.

На сьогоднішній день проблема інституційно-організаційного забезпечення інформаційної безпеки в Україні полягає у відсутності спеціально уповноваженого органу, що суперечить сучасним тенденціям організації регуляторних процесів. Адже відсутність чіткої координації та розподілу функціональних обов’язків серед органів державної влади знижує рівень ефективності державної політики у сфері інформаційної безпеки.

Відмічаючи важливість та значення ухваленої Стратегії інформаційної безпеки, проблема недостатньої розробленості нормативно-правової бази у сфері інформаційної безпеки залишається актуальною та потребує розв'язання. Таким чином, удосконалення інституційного забезпечення інформаційної безпеки вимагає комплексного підходу і передбачає впровадження якісних змін в інституційно-організаційному та інституційно-правовому забезпеченні.

Висновки до розділу 1

1. Обґрунтовано змістовне наповнення категорійного базису інформаційної безпеки національної економіки в умовах цифровізації, що встановлює логічні зв'язки між базовими поняттями управління розвитком національної економіки, забезпеченням інформаційної безпеки та розвитку процесів цифровізації. На основі систематизації наукових концепцій трактування поняття «інформаційна безпека національної економіки» виділено три основні наукові підходи, а саме, визначення інформаційної безпеки як складової національної безпеки; як стану захищеності інформаційного середовища та національних інтересів від можливих загроз; як стану системи, який здатний забезпечити цільові параметри безпеки. Поглиблено змістовне наповнення категорії «інформаційна безпека національної економіки».

2. Дослідження інформаційної безпеки як невід'ємного елементу національної економіки дало підстави для визначення дуального взаємозв'язку між процесами цифровізації та елементами системи інформаційної безпеки національної економіки, зокрема розгляд цифровізації господарської системи як інструменту реалізації національних інтересів, що створює нові можливості для зміцнення безпеки національної економіки (підвищення конкурентоспроможності національної економіки, стимулювання інновацій, модернізація та розвиток інфраструктури й пріоритетних галузей економіки), а також як джерела виникнення нових внутрішніх і зовнішніх дестабілізуючих чинників

функціонуванню національної економіки, що пов'язано з ризиками й загрозами в інформаційному просторі та, в тому числі, у кіберпросторі.

3. Обґрунтовано, що головним фактором розвитку національної економіки у сучасних умовах виступають процеси цифровізації. Становлення Індустрії 4.0 та впровадження принципів Індустрії 5.0 докорінно змінили структуру національної економіки, що підтверджується результатами проведеного аналізу формування валової доданої вартості за видами економічної діяльності за 2010 – 2022 роки. Встановлено зростання частки галузей, що становлять основу постіндустріальної економіки та є базисом розвитку цифрової економіки, зокрема галузі інформації та телекомунікації.

4. Систематизовано та удосконалено багаторівневу класифікацію загроз інформаційній безпеці національної економіки, що дозволяє ідентифіковувати загрози та вживати превентивних заходів. Розподіл загроз за об'єктами є базисом для формування напрямів запобігання, протидії, мінімізації негативного впливу від реалізації. Основними загрозами інформаційній безпеці національної економіки на сучаному етапі є: поширення злочинності у кіберпросторі, слабкість систем превентивного реагування на кіберінциденти; відсутність цілісного інституційного забезпечення державної політики інформаційної безпеки; недостатній рівень інформаційної стійкості економічних субєктів до деструктивних інформаційних впливів.

5. Здійснено обґрунтування інституційного забезпечення інформаційної безпеки національної економіки в розрізі основних структурних елементів (інституційно-правового та інституційно-організаційного), що може стати підґрунтям для визначення перспективних напрямів реалізації державної політики щодо організаційної, інформаційної, контрольної та іншої функціональної діяльності органів державної влади, завдяки провадженню якої національна економіка перебуває в безпеці.

Основні результати дослідження відображені у наукових працях автора [70, 73, 81, 82, 85, 95].

РОЗДІЛ 2
АНАЛІЗ ТА ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕКОНОМІКИ УКРАЇНИ

2.1. Аналіз цифровізації національної економіки та розвитку інформаційного середовища в Україні

Сучасні тенденції функціонування інформаційного середовища тісно пов'язані з поступовим формуванням цифрової економіки. Розвиток цифрової економіки в останні десятиліття є стратегічним напрямом провідних країн світу. У зв'язку з цим сучасний етап розвитку суспільства характеризується інтеграцією безпекових аспектів інформаційних та економічних процесів, що вимагає переходу системи управління як на макро-, так і мезо- та мікрорівні на якісно новий рівень.

Цифрова економіка є типом економіки, за якого додатковими факторами виробництва виступають цифрові дані. Їх використання як ресурсу може значно підвищити ефективність, продуктивність, цінність послуг і товарів та побудувати цифрове суспільство. Цифрова трансформація економіки означає інтеграцію цифрових технологій у всі сфери економічної діяльності. Інформаційно-комунікаційні технології та штучний інтелект стали рушіями соціально-економічного зростання і формування нової якості життя.

Інформаційне цифрове середовище забезпечує конкурентні переваги для інноваційного розвитку економічних систем. На сьогоднішній день розмір цифрової економіки, за різними оцінками, становить від 15,5 % до 17,5 % світового ВВП. Близько 40% доданої вартості, що створюється світовим сектором інформаційно-комунікаційних технологій, припадає на США і Китай. Прогнозується, що до 2030 року частка цифрової економіки у ВВП найбільших країн світу досягне 50–60% [100, 101]. Так, у 2018 році розмір світового ВВП, що припадав на цифровізовані підприємства, склав 13,5 трлн дол. За підсумками

2023 року прогнозується зростання показника майже в чотири рази (близько 53,3 трлн дол.), що перевищить половину номінального світового ВВП (рис. 2.1).

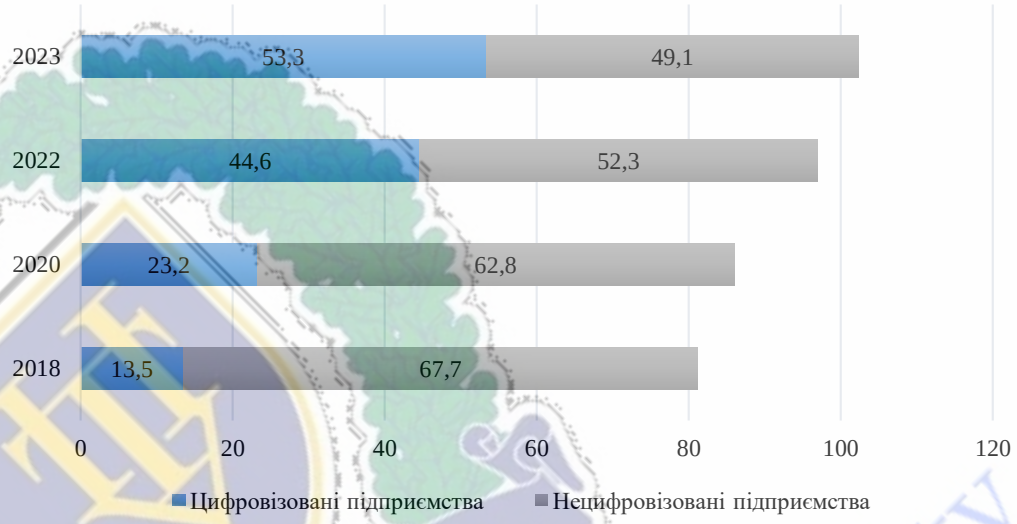

Рис. 2.1. Обсяг продукції цифровізованих та нецифровізованих підприємств у світовому ВВП, трлн дол.

Джерело: побудовано автором на основі даних [102]

Одним із показників, який характеризує розвиток цифрової економіки є Міжнародний індекс цифрової економіки та суспільства (I-DESI), що ґрунтується на порівняльному аналізі показники цифрової ефективності країн-членів ЄС та 19 інших країн світу (Австралія, Албанія, Боснія і Герцеговина, Бразилія, Канада, Чилі, Ісландія, Ізраїль, Японія, Мексика, Чорногорія, Північна Македонія, Норвегія, Сербія, Південна Корея, Швейцарія, Туреччина, Велика Британія, США) [103]. За підсумками 2022 року держави-члени ЄС розташувалися на перших п’яти позиціях з десяти найкращих у індексі I-DESI (рис. 2.2). Загальні бали індексу залишаються вищими для країн, що не входять до ЄС, ніж для держави-членів ЄС за кожен рік. Найвищий показник I-DESI мала Данія. Вона також була провідною країною в ЄС згідно з показниками індексу DESI за 2021 рік. Провідною країною поза ЄС стала Ісландія.

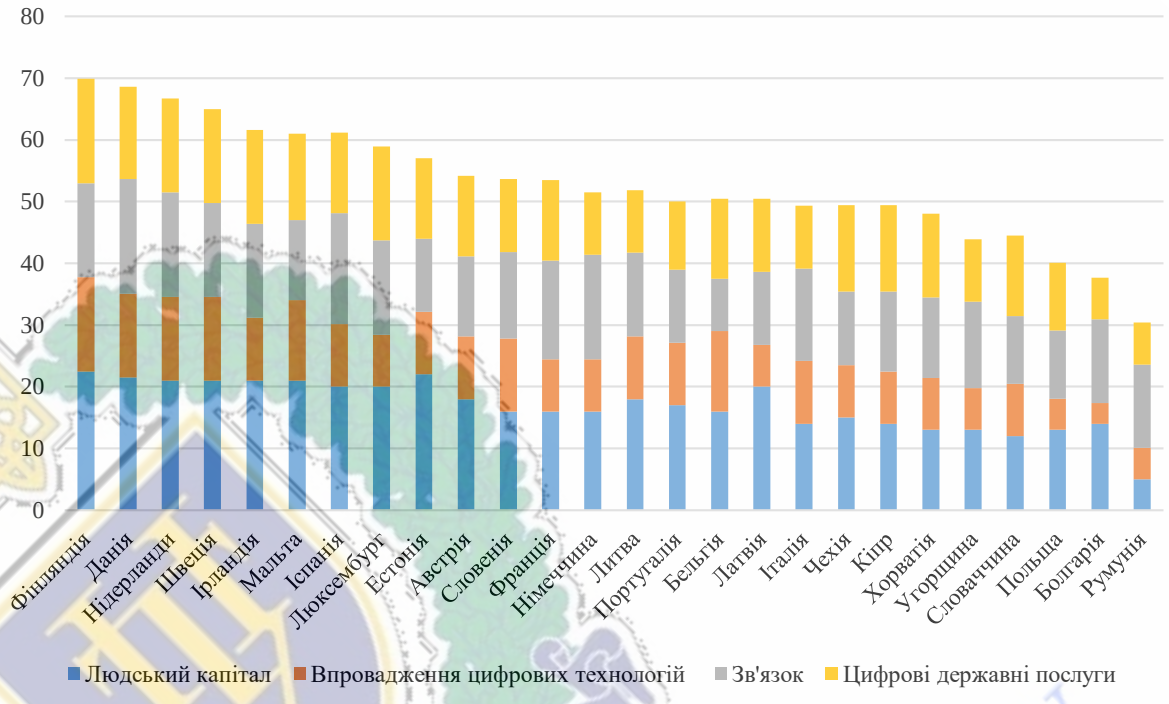

Рис. 2.2. Інфографіка Міжнародного індексу цифрової економіки та суспільства за 2022 рік

Джерело: побудовано автором на основі даних [104]

В цілому, у розвинених країнах рівень кібербезпеки і показники розвитку цифрової економіки вищі, ніж в країнах, які розвиваються. Кореляції в даних доводять, що безпека цифрових систем і прозорість цифрових суб'єктів, особливо з точки зору використання даних, є важливими, якщо технологія має бути поширена серед суспільства; ключовим прикладом є електронне урядування. Вирішення питань кібербезпеки сприятиме використанню ресурсів електронної участі.

В Україні відсутня модель розрахунку економічного впливу інформаційно-комунікаційних технологій на галузі національної економіки. Проте сукупний обсяг ІКТ-обладнання та послуг, спожитих в Україні в 2018 році, склав орієнтовно 1,5 млрд дол. Тоді як, наприклад, економіка Польщі спожила ІКТ-продукції на 6,5 млрд дол. Це означає, що темпи цифровізації галузей національної економіки є нижчими у порівнянні з країнами Європейського Союзу. Водночас, рівень споживання інформаційно-комунікаційної продукції та

послуг є одним із головних показників рівня модернізації країни, її інноваційності та конкурентоздатності.

З метою досягнення у 2030 р. ВВП на рівні 1 трлн дол. необхідно збільшити споживання ІКТ-продукції, в першу чергу за рахунок реалізації масштабних національних проєктів цифрових трансформацій (табл. 2.1).

Таблиця 2.1

Показники цифровізації економіки в Україні

Роки / Показники	2023	2024	2025	2026	2027	2028	2029	2030
Внутрішній ринок (споживання ІКТ), млрд дол	3,0	4,5	6,0	8,0	10,0	12,0	14,0	16,0
Темп зростання споживання ІКТ, %	-	150,0	133,3	133,3	125,0	120,0	116,7	114,3
Темп зростання ВВП за рахунок цифровізації економіки, %	2,0	3,5	4,5	6,0	7,5	9,0	11,0	14,0
Частка цифрової економіки у загальному ВВП, %	5,0	8,0	11,0	15,0	20,0	28,0	40,0	52,0

Джерело: узагальнено автором за даними [105]

Національна економіка набула інформаційного характеру: конкурентоспроможність і продуктивність суб'єктів господарювання залежать від можливості генерувати, обробляти й ефективно використовувати інформацію, що ґрунтується на знаннях. Тобто в сучасних умовах інформація одночасно є продуктом та ключовим економічним ресурсом у інформаційній економіці з погляду доданої вартості. Отже, вплив цифровізації на макрорівні визначається створеною доданою вартістю у галузях економіки, а на мікрорівні – для кожного конкретного продукту чи послуги. Виходячи з вищезазначеного, проведемо аналіз формування доданої вартості в розрізі галузевої структури національної економіки України (рис. 2.3 – рис. 2.6), використовуючи офіційні дані Державної служби статистики України (Додаток В). Саме галузева структура відіграє провідну роль у національній економіці, оскільки у галузевому розрізі здійснюється виробництво та відбувається облік статистичних даних.

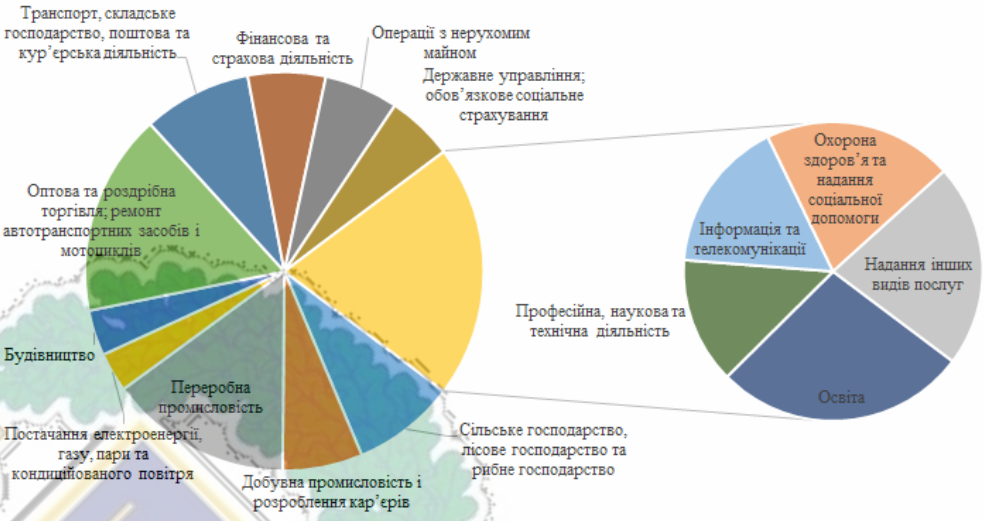

Рис. 2.3. Структура валової доданої вартості за видами економічної діяльності (2010 р., у фактичних цінах)

Джерело: побудовано автором на основі даних [106]

Згідно з представленими результатами у 2010 році найбільший вклад у формування валової доданої вартості національної економіки мали такі види економічної діяльності як оптова та роздрібна торгівля (16,4%), переробна промисловість (14,8%), транспорт, складське господарство, поштова та кур'єрська доставка (8,8%). Вклад галузі інформації та комунікації становив 3,4%.

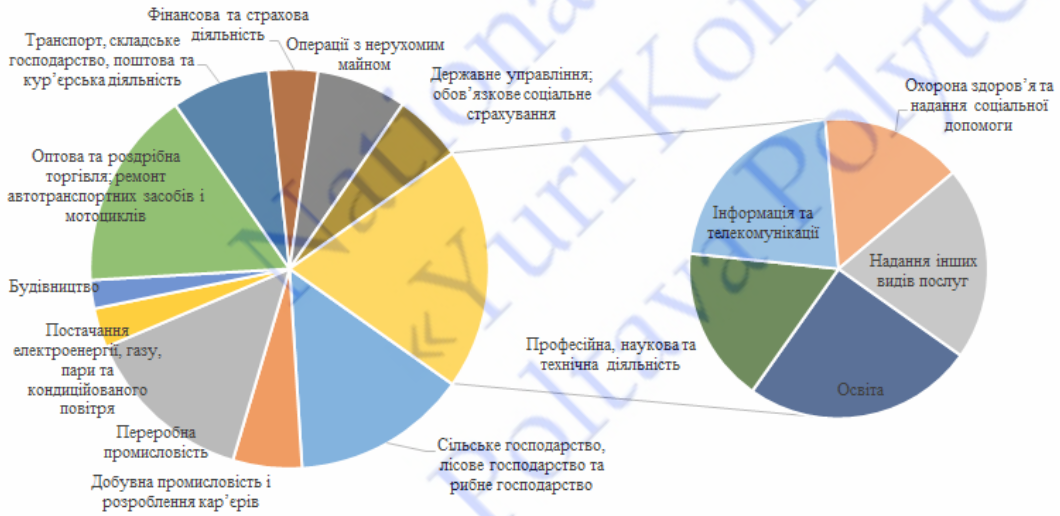

Рис. 2.4. Структура валової доданої вартості за видами економічної діяльності (2015 р., у фактичних цінах)

Джерело: побудовано автором на основі даних [106]

За п’ять років відбулася зміна частки галузей національної економіки у структурі валової доданої вартості: оптова та роздрібна торгівля (16,2%) і переробна промисловість (14,0%) зазнали незначного зменшення, у той час як внесок сільського, лісового, рибного господарство зріс з 8,4% до 14,2%. Позитивна динаміка спостерігається і в галузі інформації та комунікації становив (4,3%).

У 2020 році внесок нематеріального капіталу в формування доданої вартості перевищив внесок матеріального капіталу. Так, вклад галузі оптова та роздрібна торгівлі займає незмінно лідируючі позиції (16,2%). Водночас відмічається зростання частки інформації та комунікації становив (4,3%) та державного управління (8,5% у порівнянні з 5,6% у 2015 році) (рис. 2.5).

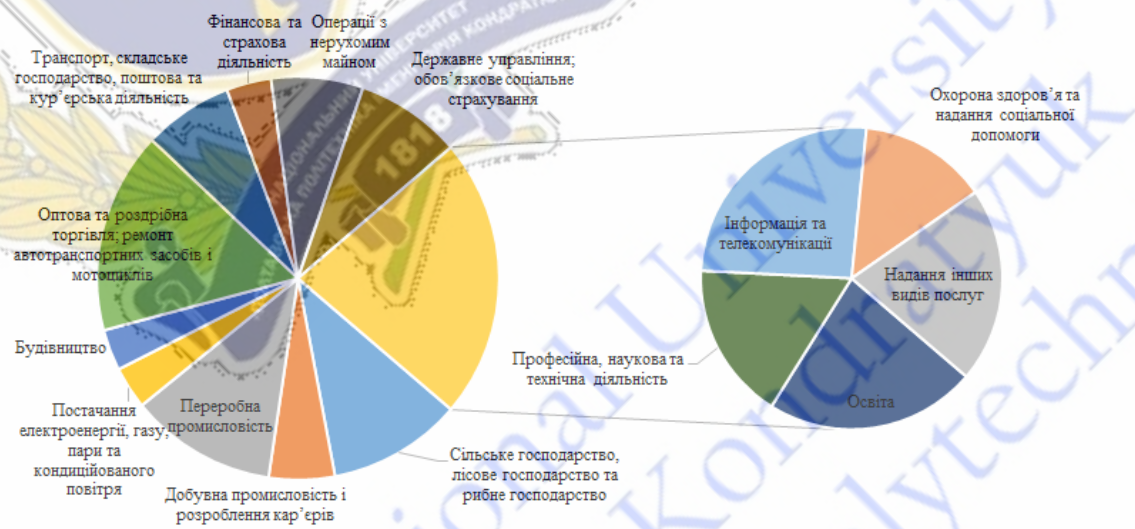

Рис. 2.5. Структура валової доданої вартості за видами економічної діяльності (2020 р., у фактичних цінах)

Джерело: побудовано автором на основі даних [106]

Це пов’язано із новими державними ініціативами сприяння цифровізації економіки, які беруть свій початок з 2019 року, з моменту запуску нової програми ЄС «EU4Digital: підтримка цифрової економіки та суспільства у Східному партнерстві», спрямовану на поширення переваг Єдиного цифрового ринку Європейського Союзу на Україну та інші держави Східного партнерства

задля стимулювання економічного зростання, створення робочих місць, покращення якості життя суспільства і підтримки бізнесу. Держава стала ключовим споживачем і користувачем інновацій: цифрову трансформацію визначено як пріоритетну політику, сформувано моду на цифрову культуру, популяризовано освіту в секторі hi-tech, реалізовано інфраструктурні проекти (підключення до мобільного покриття 4G 90% населення України, запуск електронних послуг у державному та приватному секторах), ініційовано та реалізовано численні проєкти цифрової трансформації (з 2020 року повноцінно впровадженно системи «ProZorro» та «e-Health», офіційно запущено портал державних послуг «Дія»).

Структура валової доданої вартості за видами економічної діяльності у 2022 році представлена на рисунку 2.6.

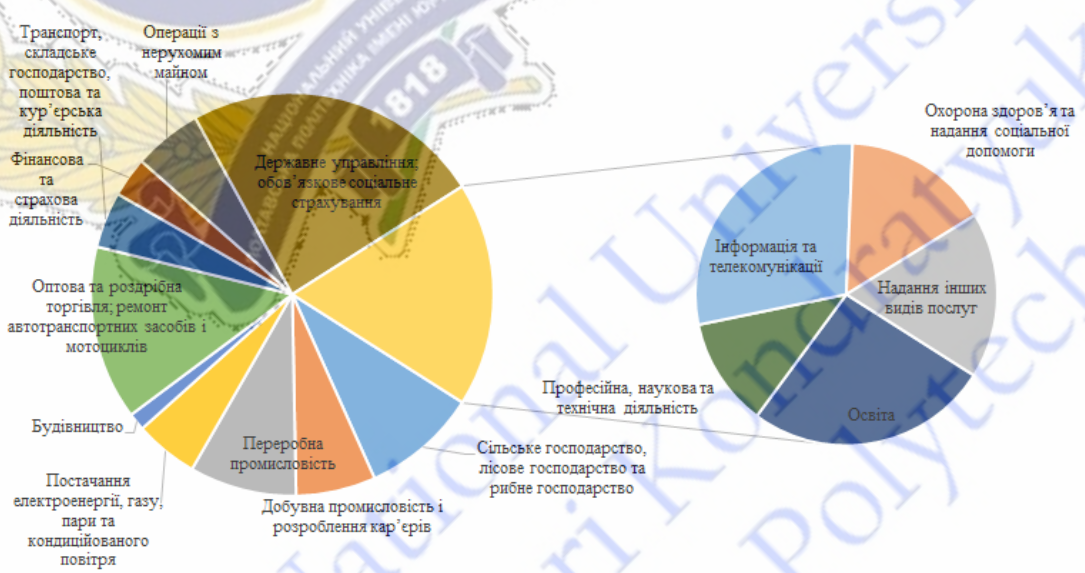

Рис. 2.6. Структура валової доданої вартості за видами економічної діяльності (2022 р., у фактичних цінах)

Джерело: побудовано автором на основі даних [106]

Специфіка представлених результатів безпосередньо пов'язана із війною рф проти України. У 2022 році в структурі валової доданої вартості найбільша частка припадає на галузь державного управління та оборони і становить 24%.

Це пояснюється, в першу чергу, нормами грошового забезпечення для військовослужбовців.

Галузь сільського, лісового та рибного господарства склала 9,3%. Якщо порівнювати цей показник із аналогічними показниками в країнах Європейського Союзу, то він є достатньо високим через переважання низької за вмістом доданої вартості продукції, що випускається в галузі. Хоча Україна має конкурентні переваги в аграрній сфері, втім це можна розглядати як структурну диспропорцію.

Щодо операцій з нерухомим майном, то наведені дані дозволяють стверджувати, що ця галузь не є драйвером зростання для національної економіки. Водночас галузь інформації та телекомунікації є інноваційною та засвідчує стійке зростання у структурі валової доданої вартості.

У відповідності до проведеного аналізу, підтверджено зростання частки галузей, що становлять основу постіндустріальної економіки та є базисом розвитку цифрової економіки.

Ще одним показником, який дозволяє оцінити розвиток інформаційного середовища в умовах цифровізації економіки є внесок ІТ-сектору у формування валового внутрішнього продукту. Тому доцільним є аналіз та прогнозування динаміки зміни частки ІТ-сектору у ВВП України, оскільки саме ця частка і засвідчує обсяги цифрової економіки (рис. 2.7).

Дані рисунку 2.7 засвідчують, що частка цифрової економіки у ВВП України поступово буде зростати. Так, у 2011 році питома вага цифрової економіки у ВВП України становила 3%, у 2017 році зросла до 4%, а у 2022 році, навіть попри війну, цей показник досяг позначки 5,5%. Водночас, у гривнях обсяг ВВП у ІТ-секторі зріс помітніше – від 34,3 млрд грн у 2011 році до 187 млрд грн у 2021 році. На рисунку 2.3 також проілюстровано прогноз до 2027 року, прорахований із використанням поліноміального тренду другого ступеня, який дозволяє робити оптимістичні прогнози. Тобто у 2024 році частка ІТ-сектору у ВВП України має досягнути 6%.

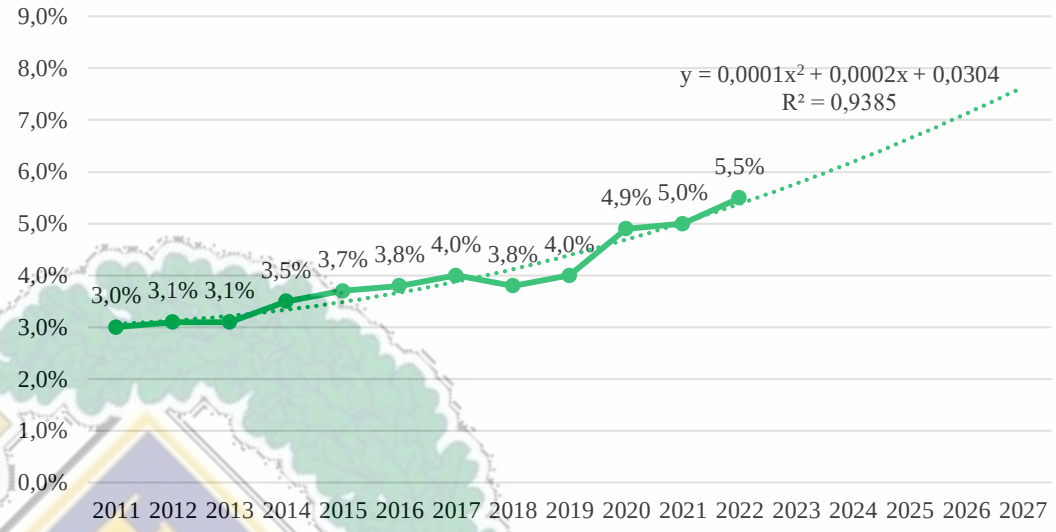

Рис. 2.7. Динаміка зміни частки ІТ-сектору у ВВП України (фактичне та прогнозне значення з використанням поліноміального тренду другого ступеня)

Джерело: розраховано автором на основі даних [107]

Окреслена тенденція підтверджується розрахунками експертів ініціативи «Цифрова адженда України» [105], які відображають прогнози показників цифровізації економіки України (див. табл. 2.1).

Доречно також розглянути песимістичний прогноз з використанням степеневої лінії тренду, яка є найбільш адекватною з урахуванням величини коефіцієнта детермінації (рис. 2.8).

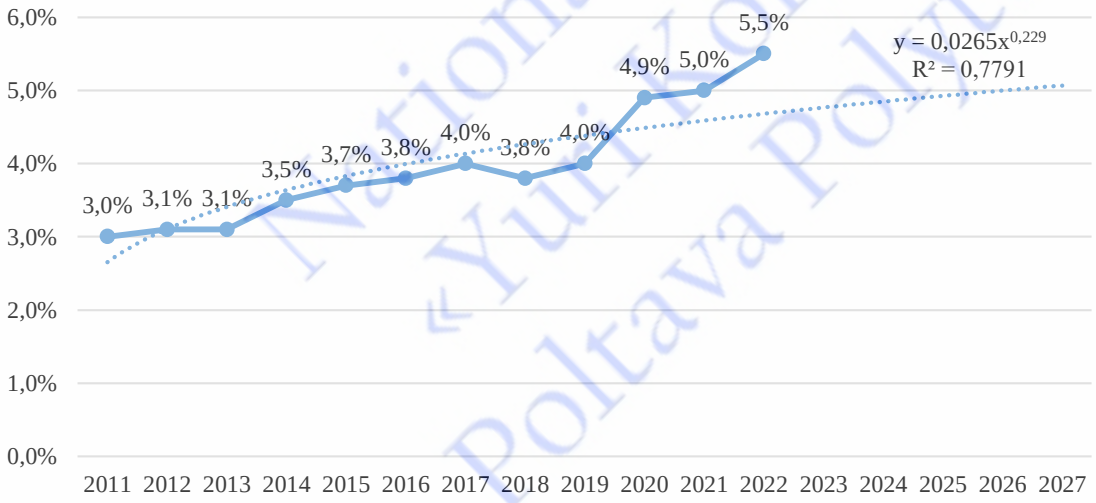

Рис. 2.8. Динаміки зміни частки ІТ-сектору у ВВП України (фактичне та прогнозне значення з використанням степеневої лінії тренду)

Джерело: розраховано автором на основі даних [107]

Згідно з поданими даними (рис. 2.8), у 2024 році частка ІТ-сектору у ВВП України знаходитиметься на рівні 2020 року та становитиме 4,9%. Водночас значення коефіцієнта детермінації, який виступає величиною достовірності апроксимації, підтверджує вищий рівень ймовірності оптимістичного сценарію розвитку цифрової економіки в Україні. Ця гіпотеза підтверджується й аналітичними даними щодо динаміки експорту ІТ-послуг.

Попри повномасштабну війну, ІТ-сфера стала єдиною сферою експорту, яка характеризується позитивною динамікою. Так, за 2022 рік експортна виручка ІТ-послуг зросла на 5,85% і склала 7,3 млрд дол. Це на 406 млн дол. більше, ніж у 2021 році. Тенденції зміни ІТ-експорту протягом 2021–2022 років подано на рисунку 2.9.

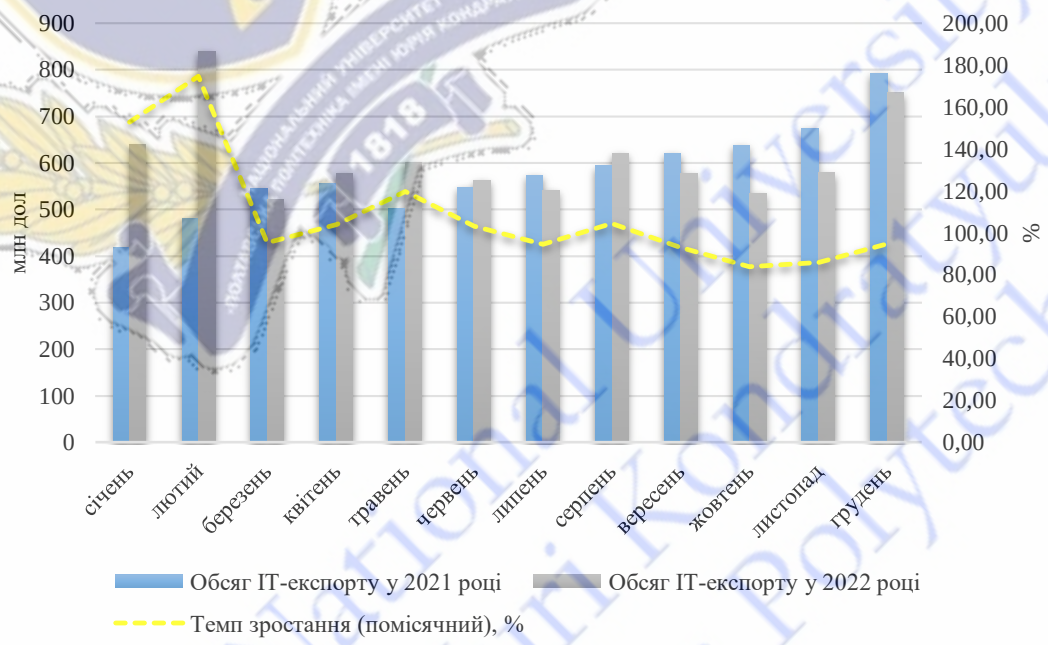

Рис. 2.9. Тенденції зміни обсягу ІТ-експорту в Україні протягом 2021–2022 років

Джерело: побудовано автором на основі даних [106]

Стійкість цифрового сектору найбільш помітна в кризових умовах. Відповідно, цифрова економіка може стати фактором стійкості економіки та надійним джерелом податкових надходжень, оскільки вона менше залежна від

фізичних активів, ніж промисловість чи сільське господарство. Інформаційні технології здатні значно підвищити ефективність майбутнього процесу відбудови. Йдеться не лише про розвиток IT-сектору та застосування цифрових технологій в інших галузях для підвищення ефективності виробництва, але й про цифрові рішення для розподілу міжнародної допомоги та контролю за її використанням, що дозволить знизити корупційні ризики.

Для порівняння рівня цифрової економіки України з країнами Європейського Союзу доцільно проаналізувати частку IT-сектора у ВВП цих країн, використовуючи офіційні дані Євростату. На рисунку 2.10 представлено відсоток сектору ІКТ у ВВП країн ЄС за 2011 рік.

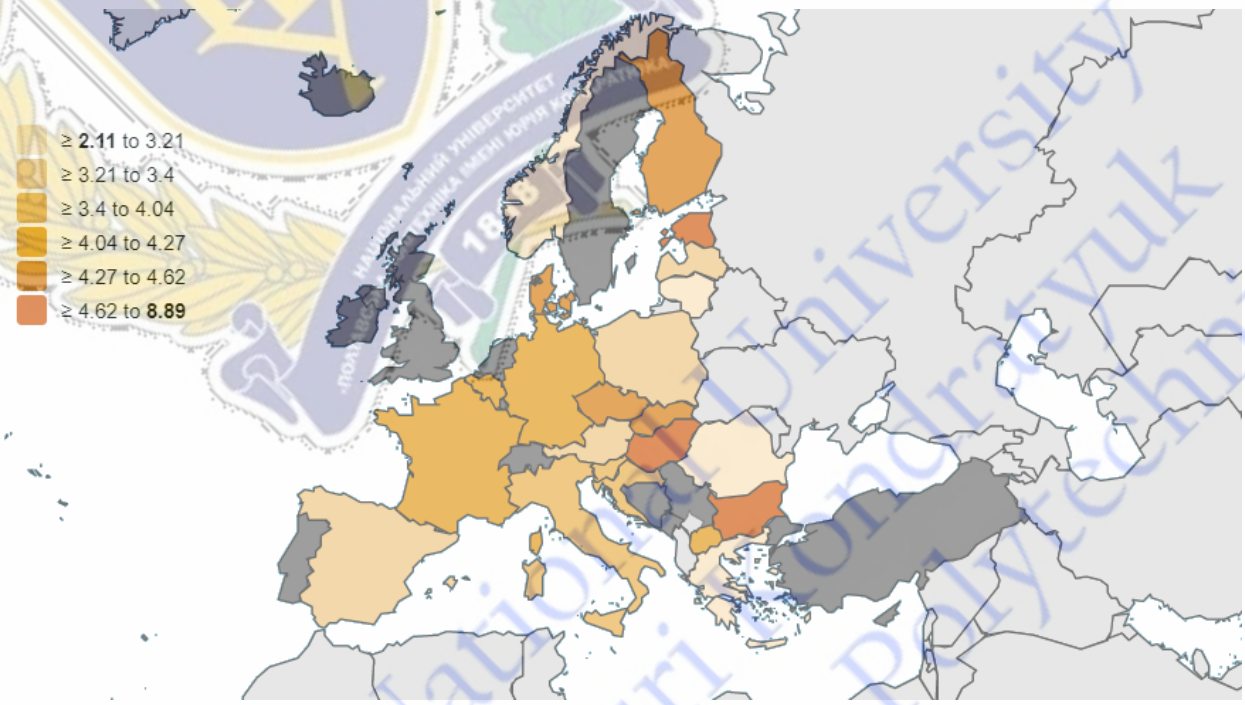

Рис. 2.10. Інфографіка частки сектору ІКТ у ВВП країн Європейського Союзу у 2011 році

Джерело: побудовано автором на основі даних [108]

Згідно з наведеними даними що відсоток сектору інформаційно-комунікаційних технологій у ВВП країн ЄС у 2011 році коливався в межах від 2,11% до 8,89%. Найвищий рівень показника спостерігався на Мальті – 8,89%, найнижчий, на рівні 2,11% – у Греції. При цьому, середнє значення склало 4,06%.

Для порівняння в Україні у 2011 році питома вага цифрової економіки у ВВП становила 3%.

Аналізуючи відсоток сектору інформаційно-комунікаційних технологій у ВВП країн ЄС у 2020 році, слід зазначити, що нижня межа піднялася до 3,23% і саме цього рівня досягла Греція. Водночас верхня межа показника склала 8,14% (Мальта) (рис. 2.11). Середнє значення показника зросло до 5,01%. Це свідчить про те, що відбувається активний розвиток економік країн Європейського Союзу у напрямку їх інформатизації та цифровізації.

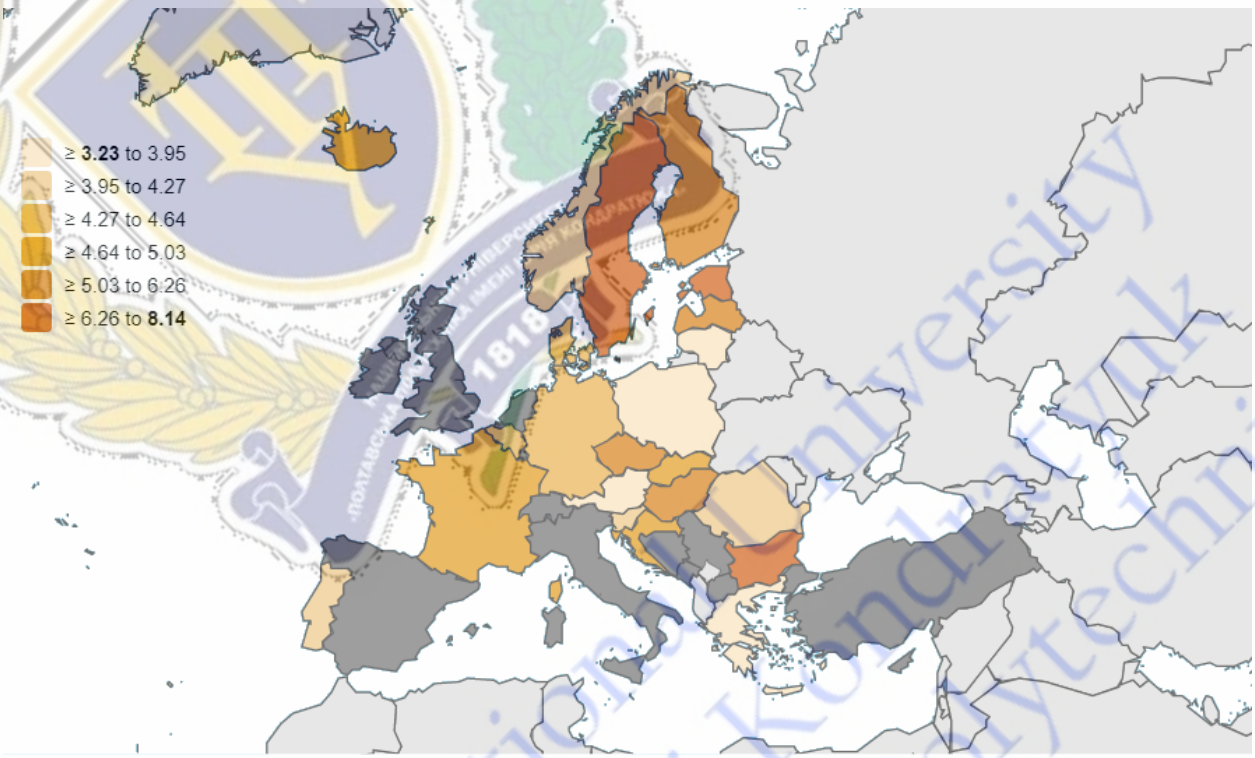

Рис. 2.11. Інфографіка частки сектору ІКТ у ВВП країн Європейського Союзу у 2020 році

Джерело: побудовано автором на основі даних [108]

В Україні у 2020 році питома вага цифрової економіки у ВВП становила 4,9%. Це свідчить про позитивну динаміку процесу цифровізації економіки України та максимального наближення показника до середнього по Європейському Союзу. Доцільно відмітити, що у сфері фінансових послуг,

послуг зв'язку, логістики національні суб'єкти господарювання застосовують цифрові технології на рівні зі світовими конкурентами.

Незважаючи на війну, Україна продовжує активно розвивати цифрову економіку з метою якнайшвидшої синхронізації з цифровою екосистемою ЄС шляхом приєднання до Єдиного європейського цифрового ринку. Ключовою метою Єдиного цифрового ринку Європейського Союзу є усунення бар'єрів і створення єдиних правил для поширення онлайн-послуг. Зокрема, у сферах цифрового маркетингу, телекомунікацій та електронної комерції, підвищення рівня кібербезпеки мереж та інформаційних систем. Згідно з оцінками провідних вітчизняних економістів інтеграція до Єдиного цифрового ринку ЄС може забезпечити зростання ВВП України до 12%, а рівень експорту товарів до країн-членів ЄС – до 17%, послуг – до 12,2%. Таким чином, доєднання України до ринків ЄС матиме не лише євроінтеграційні, але й економічні переваги.

Водночас, стрімкий розвиток процесів цифровізації став джерелом не тільки нових можливостей, а й ризиків і загроз, насамперед інформаційної безпеки національної економіки [81]. Поряд із традиційними загрозами, такими як промислове шпигунство, навмисне та ненавмисне розголошення співробітниками конфіденційної інформації та комерційної таємниці, недобросовісні дії конкурентів, зокрема заподіяння шкоди діловій репутації, втручання третіх осіб в інформаційні системи та мережі, порушення цілісності баз даних, тощо, з'являється низка додаткових загроз інформаційним ресурсам і технологіям в економіці, методи діагностики та реагування на які ще не до кінця розроблені [109]. Це, насамперед, загрози, пов'язані з кібератаками, розголошенням персональних даних, впливом шпигунських програм і вірусів, фішингом, загрозами, пов'язаними з оновленням комп'ютерних програм тощо. В умовах постійного зростання кіберризиків та кіберзагроз важливо відслідковувати рівень кібербезпеки інформаційного середовища в Україні, виокремлювати основні проблеми розвитку національної системи кіберзахисту та визначати напрями їх вирішення.

Зростання конфліктів у кіберпросторі правомірно датувати 2013 роком, коли була реалізована атака на вітчизняну енергосистему з виведенням її з ладу. З цього часу кількість кібератак невпинно зростає. За офіційними даними Ради національної безпеки і оборони України, лише за 2019 рік відбулося 480 кібератак на сферу державного управління та об'єкти стратегічного значення. Хронологія найбільших атак на інформаційні системи в країні представлено на рисунку 2.12.

Рис. 2.12. Хронологія найбільших кібератак на інформаційні системи України за 2014 – 2017 рр.

Джерело: побудовано автором на основі даних [110, 111]

Враховуючи, що цифрова економіка базується на інформаційно-комунікаційних і цифрових технологіях, активізація процесів цифровізації господарської діяльності створює умови для збільшення випадків несанкціонованого використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж телекомунікацій, тобто розширюється спектр загроз інформаційному середовищу.

Отже, розвиток ІТ-технологій, поряд з безперечними перевагами, став причиною поглиблення ризиків та загроз в інформаційному середовищі, зокрема, кіберпросторі. Згідно з офіційними статистичними даними, рівень кіберзлочинності в Україні постійно зростає (рис. 2.13).

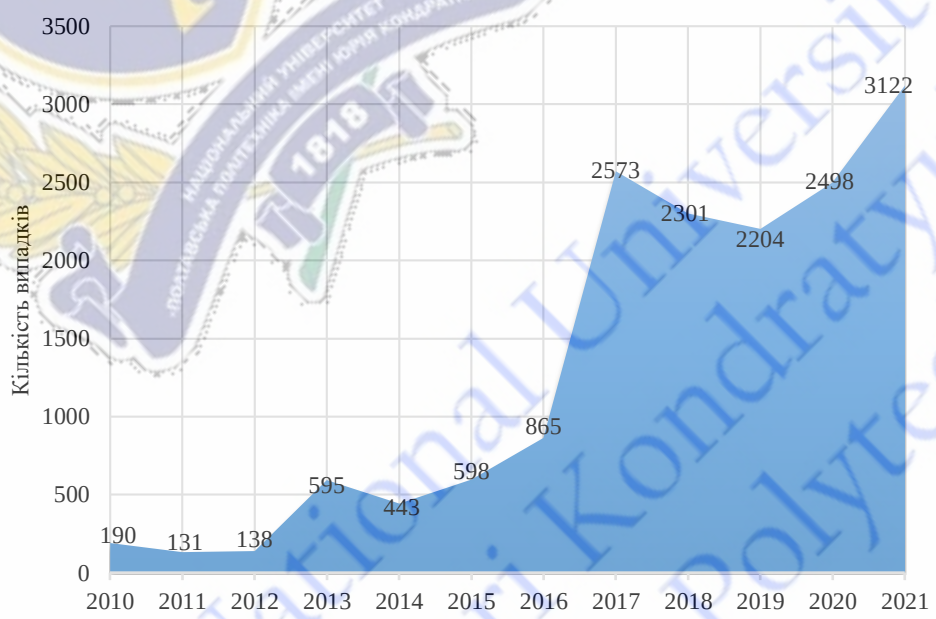

Рис. 2.13. Кількість кіберзлочинів в Україні у 2010 – 2021 рр.

Джерело: побудовано автором на основі даних [112]

Рівень кіберзлочинності в абсолютному вираженні характеризується значним зростанням і стабілізацією показників на високих рівнях. Суттєве збільшення кількості зареєстрованих у 2013 р. кіберзлочинів ряд науковців пов'язує з тим, що «зростання цього виду злочинів зумовлене щорічним зростанням користувачів Інтернет-ресурсу в Україні», інші пояснюють різницю

в даних щодо зареєстрованих злочинів з передачею права формування державної статистики про стан злочинності в державі від МВС до прокуратури України. У 2017 р. відбулося особливо помітне зростання рівня кіберзлочинності (більш ніж у чотири рази порівняно з 2013 р.). Це свідчить про специфічні риси досліджуваного виду злочинів, пов'язаних з особливостями комплексу факторів його детермінації: стрімке розгортання процесу інформатизації суспільства (упровадження мережі третього покоління (3G) операторами мобільного зв'язку), використання кібертехнологій як засобу злочинної діяльності, об'єктивне відставання в розвитку технічної складової правоохоронної системи тощо.

На думку вітчизняних і зарубіжних експертів, вирішення проблеми розслідування цього виду злочинів є непростим завданням для правоохоронних органів як у нашій країні, так і за кордоном. Вітчизняні та зарубіжні кримінологи відносять «комп'ютерну» злочинність до гіперлатентної (надприхованої). За різними оцінками, правоохоронним органам відомо лише про 10–20% цих злочинів [113].

Щодо світової статистики, то на початку 2020 року кількість кібератак у світі складала близько 5 тисяч за тиждень. На початку 2021 року їх абсолютний показник зріс до 200 тисяч [114]. Доцільно відмітити, що 19% усіх світових кібератак у 2021 році було направлено проти України (на першому місці – США), що підтверджує необхідність підвищення рівня захищеності інформаційного середовища національної економіки (рис. 2.14).

Для порівняння: частка Німеччини, Японії та Бельгії не перевищує 3% [115]. Таким чином, Україна посідає друге місце у світі за кількістю кібератак, спрямованих насамперед на об'єкти критичної інфраструктури країни, тобто такі галузі, як енергетика, фінанси, телекомунікації тощо, а також державні електронні інформаційні ресурси, порушення доступності і цілісності яких становить загрозу національним інтересам [116].

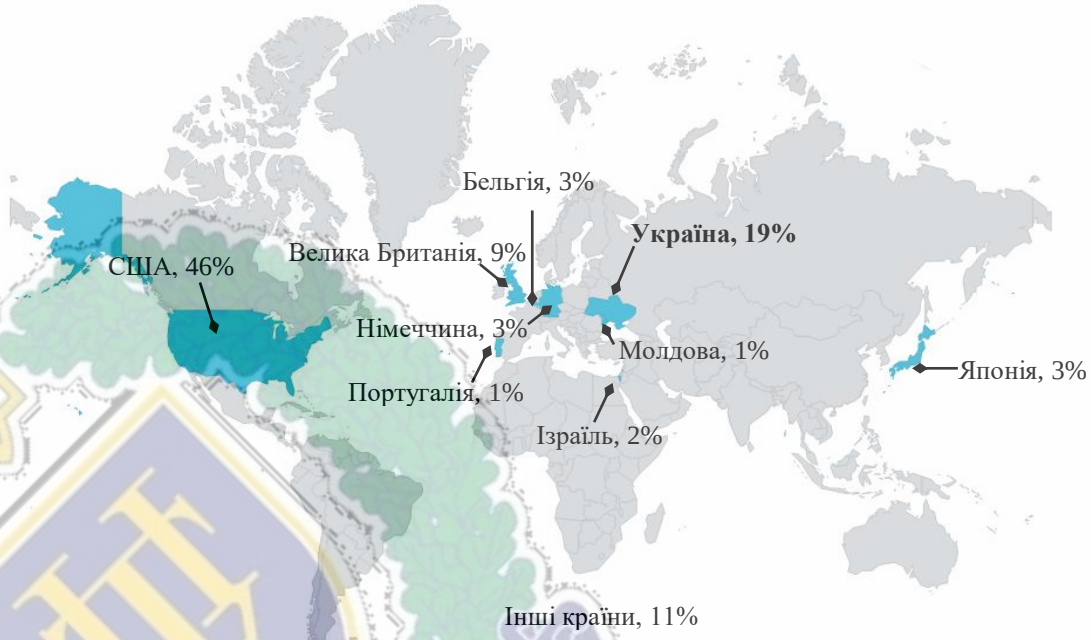

Рис. 2.14. Картосхема частки кібератак на країни світу у загальній їх кількості за 2021 рік

Джерело: побудовано автором на основі даних [115]

За даними компанії Microsoft, більшість кібератак у 2021 році було здійснено з території рф – 58% від загальної кількості зафіксованих атак. Друге місце серед країн, із територій яких здійснювали кібератаки, посіла Північна Корея (23%), а третє – Іран (11%) (рис. 2.15).

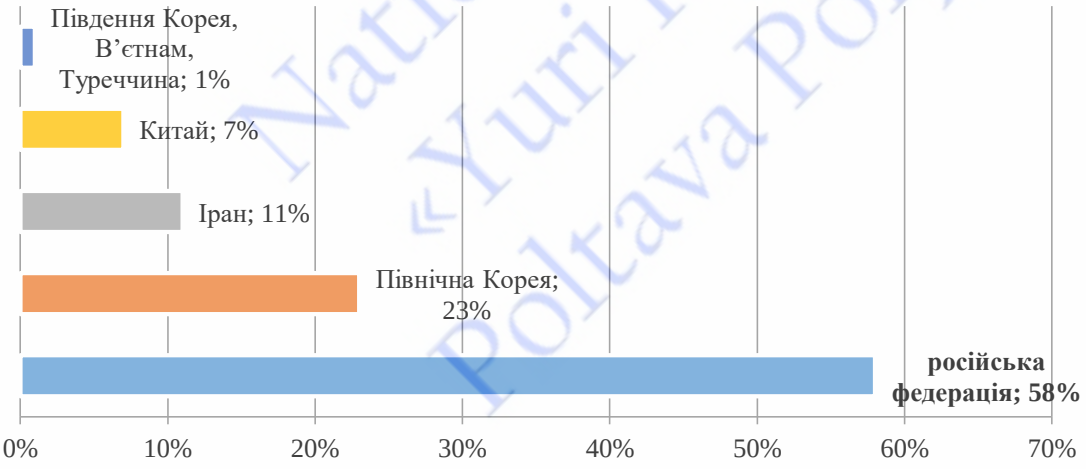

Рис. 2.15. Структура кібератак за країнами походження за 2021 рік

Джерело: побудовано автором на основі даних [115]

Державний сектор став головною мішенню для кіберзлочинців у 2022 році: кількість атак на інформаційну інфраструктуру цього сектора зросла на 95% у другій половині 2022 року в порівнянні з аналогічним періодом 2021 року (рис. 2.16). Останні роки Індія, США, Індонезія та Китай залишалися основними країнами-мішенями для кібератак. Разом на ці чотири країни припадає близько 40% від загальної кількості повідомлень про інциденти в державному секторі.

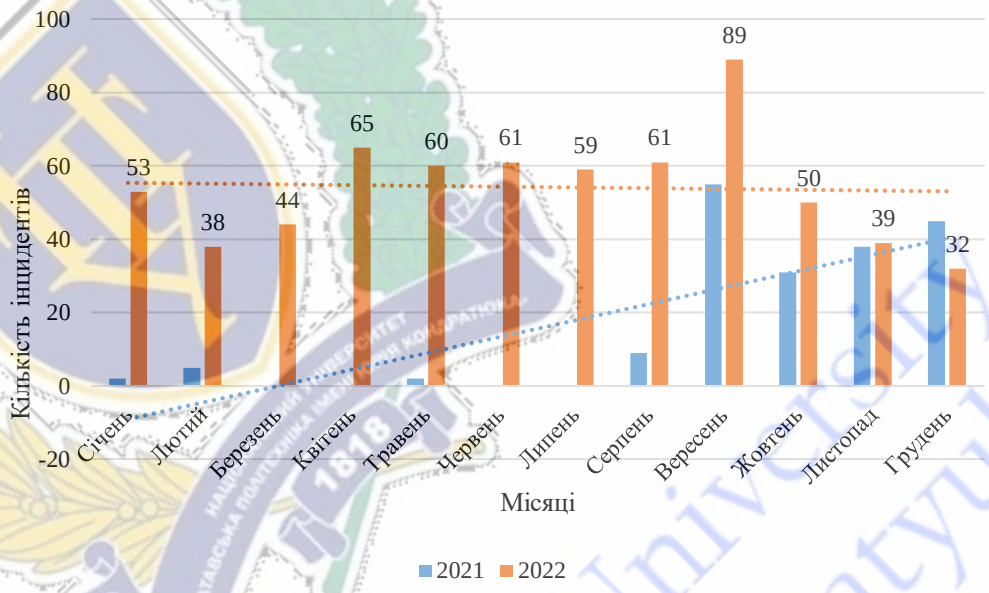

Рис. 2.16. Кількість кіберінцидентів, спрямованих на державний сектор, зафіксованих за 2021–2022 рр.

Джерело: побудовано автором на основі даних [117]

Зростання рівня цифровізації, спричинене COVID-19, не лише збільшило площу атак для зловмисників, але й дозволила країнам використовувати кібервійну як інструмент для нападу на інші країни [118].

Повномасштабне вторгнення російської федерації в Україну супроводжувалося скоординованими кібератаками на державні установи та об’єкти критичної інфраструктури. Водночас, більш ніж на 600% зросла кількість кібератак на росію як підтримка Україні з боку активістів.

З початку 2022 року російська федерація розпочинає кібервійну проти України – інтенсивність кібератак зросла: тільки за січень виявлено 6,8 млн

підозрілих подій інформаційної безпеки, виявлено 25,5 тис. потенційних кіберінцидентів і припинено 121 кібератаку. Для порівняння, у квітні 2021 року фахівці Служби безпеки України виявили 1,5 млн підозрілих подій і запобігли 53 критичним кіберінцидентам [119]. У січні-лютому 2022 року на об'єкти критичної інфраструктури та державні інформаційні ресурси України було здійснено 436 кібератак, порівняно з 64 за аналогічний період 2021 року. Найбільш масштабніші з них наведено на рисунку 2.17.

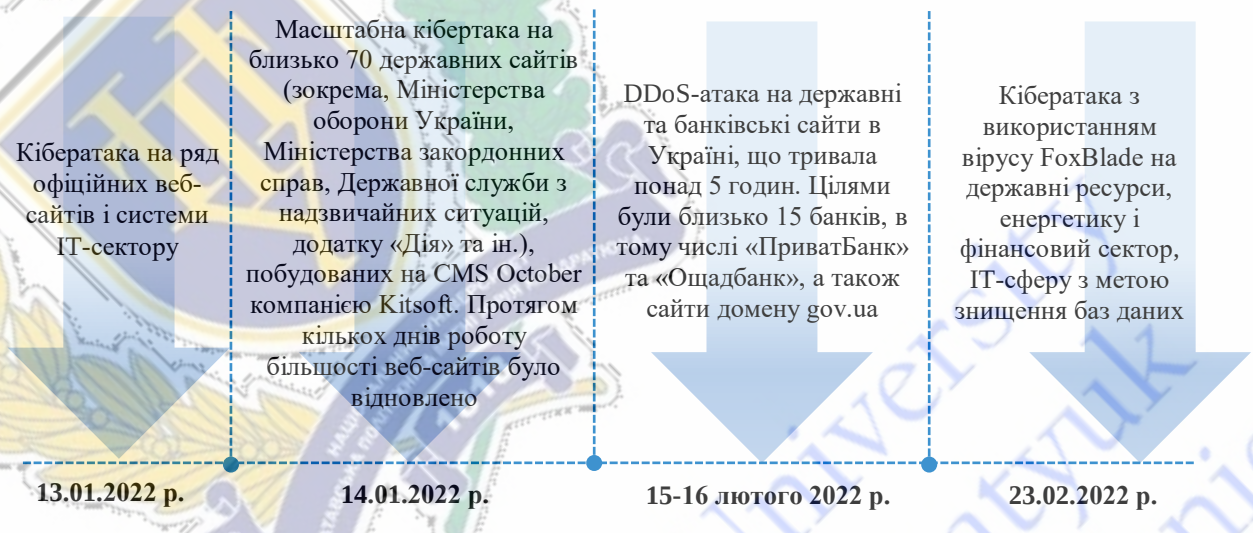

Рис. 2.17. Кібератаки на об'єкти критичної інфраструктури та державні інформаційні ресурси України у січні–лютому 2022 року

Джерело: побудовано автором на основі даних [110, 112, 114, 115]

За даними Державної служби спеціального зв'язку та захисту інформації України [120], з початку військової агресії рф за одну добу зафіксовано критичну кількість DDoS-атак: 271. За період березень-травень 2022 року продовжувалися кібератаки на офіційні державні ресурси та сайти українських онлайн-медіа, енергетичний сектор, логістичну інфраструктуру.

Основними видами кібератак, що становлять найбільшу загрозу інформаційній безпеці та кібербезпеці національної економіки, є цільові кібератаки, DDoS-атаки, інсайдерські атаки, програми-вимагачі, фішинг.

Програми-вимагачі або шифрувальники здійснюють шифрування інформації на девайсах компанії, що може призвести до повної зупинку бізнесу. В окремих випадках інформація не підлягає відновленню. Інсайдерські атаки є одними з найскладніших видів кіберзагроз, оскільки безпосередньо пов'язані з людським фактором. Інсайдером зазвичай виступає співробітник компанії, який наносить шкоду як цілеспрямовано, так і випадково. Цей вид кібератаки складно передбачити [121].

Фішинг є однією з найефективніших та найпоширеніших атак. Полягає в поширенні кіберзловмисником листів зі шкідливими файлами або посиланнями, які при відкритті заражають ПК. З цього розпочинається проникнення в мережу організації. DDoS-атаки, цільові кібератаки,– це атаки на обчислювальну систему з метою доведення її до відмови, створення таких умов, за яких користувачі системи взагалі не мали можливості отримати доступ до системних ресурсів, що надаються, або значно його обмежити.

Останній вид кібератак часто застосовується російським агресором для приховування деструктивних дій [122]. Зокрема, останню масштабну та тривалу DDoS атаку на українські банки та державні сайти було здійснено 15 лютого 2022 року. За офіційними даними жодного витоку даних, спотворення чи знищення елементів ІТ-інфраструктури, фінансових втрат не зафіксовано [123].

Перелічені види загроз інформаційній безпеці національної економіки спричиняють найбільші фінансові втрати. Так, за даними американської компанії McAfee, що спеціалізується на комп'ютерній безпеці, і Центру стратегічних і міжнародних досліджень (CSIS), глобальні економічні втрати внаслідок кібератак у 2020 році становили понад 1 трлн дол., що становило 1% світового ВВП. Порівняно з 2018 роком цей показник збільшився більш ніж на 50%. У 2021 році втрати від кібератак зросли до 4,2–6 трлн дол. (рис. 2.18). За прогнозами аналітиків у 2025 році абсолютна величина фінансових втрат від кіберзлочинності сягне 10,5 трлн дол.

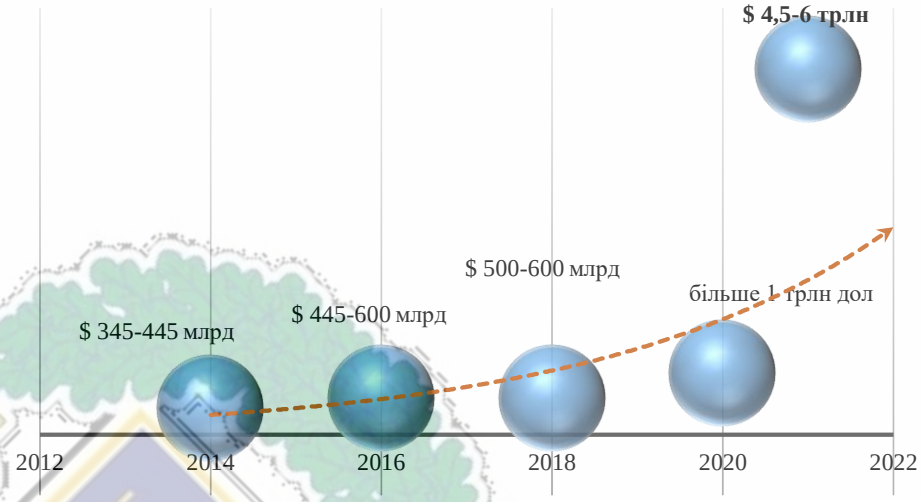

Рис. 2.18. Світові фінансові втрати від кібератак у 2014–2021 роках

Джерело: побудовано автором на основі даних [123]

Варто зазначити, що 2021 року було зафіксовано найвищий середній збиток від витоку даних за останні 17 років – 4,24 млн дол. Аналогічний показник за 2020 рік становив 3,86 млн дол. [124]. Найпоширенішою причиною витоку даних стали фішингові атаки. Крім прямих фінансових втрат, кібератаки спричиняють втрату робочого часу, а також втрату іміджу компанії [125]. Є й інші приховані витрати від кіберзлочинності – зокрема, зниження рівня задоволеності роботою співробітників.

Враховуючи актуальні виклики економічній безпеці України в інформаційній сфері, зростання негативних фінансових наслідків від реалізації кіберзагроз, необхідність визначення стратегічних напрямів протидії реальним та потенційним загрозам, у жовтні 2021 року була затверджена Стратегія інформаційної безпеки. Стратегією окреслено глобальні виклики та загрози інформаційній безпеці, зокрема зростання глобальних дезінформаційних кампаній, збільшення атак з боку російської федерації в інформаційному просторі, недостатній рівень медіаграмотності в умовах цифровізації. Також визначено основні напрями забезпечення інформаційної безпеки України, серед яких доцільно виокремити необхідність створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема, створення системи

боротьби з дезінформацією та інформаційними операціями, спрямованої на запобігання, виявлення та максимально швидке реагування на інформаційні загрози з боку держави та суспільства. Водночас, основою для розроблення превентивних заходів запобігання загрозам інформаційній безпеці та визначення ефективності від їх впровадження правомірно визначити проведення систематичного оцінювання рівня інформаційної безпеки.

2.2. Методичні засади оцінювання рівня інформаційної безпеки національної економіки

Проведені дослідження нормативно-правової бази та праць вітчизняних науковців [126–132] засвідчили відсутність загальноприйнятої методики оцінювання рівня інформаційної безпеки національної економіки. Певні методологічні підходи можна знайти у напрацюваннях щодо оцінювання інформаційної безпеки на мікрорівні, тобто суб'єктів господарювання.

Міжнародні стандарти ISO/IEC 27001 та ISO/IEC 27002 (до 2007 року мав назву ISO/IEC 17799) є основоположними в галузі управління інформаційною безпекою. Вони містять модель системи менеджменту, яка визначає загальну організацію процесів, класифікацію даних, системи доступу, інструкції з планування, обов'язки і відповідальність співробітників, оцінювання ризиків тощо в контексті інформаційної безпеки. Впровадження стандарту ISO/IEC 27001 дало змогу суб'єктам господарювання оцінювати свої ризики, впроваджувати засоби контролю для їхнього зниження, здійснювати контроль за ризиками, покращуючи, за потреби, захист інформації. Стандарт ISO/IEC 27002 застосовується з метою формування системи ефективного інформаційного захисту та удосконалення його методів.

На сьогоднішній день серія ISO/IEC 27000 охоплює понад 60 міжнародних стандартів, що включають усі аспекти інформаційної безпеки: від створення загального словника (ISO/IEC 27000), управління ризиками (ISO/IEC 27005),

безпеки у хмарних технологіях (ISO/IEC 27017 та ISO/IEC 27018) до методів судової експертизи, які застосовують для аналізу цифрових доказів і розслідування інцидентів (ISO/IEC 27042 та ISO/IEC 27043 відповідно) [126]. Вони дають можливість підприємствам постійно оновлюватися у боротьбі з кіберзлочинністю.

Побудова ефективної системи управління інформаційною безпекою на основі міжнародних стандартів серії ISO в сучасних інформаційно-комунікаційних системах і мережах є важливим завданням для кожного економічного суб'єкта. Для протидії зовнішнім атакам необхідно не лише мати ефективні засоби захисту, але й знати їх систему роботи, налаштування та слабкі місця операційних систем [127].

Аналіз наявних наукових напрацювань щодо діагностики рівня інформаційної безпеки на мікрорівні дозволяє окреслити наступні підходи. Так, Реверчук Н. [128] запропоновано оцінювати інформаційну безпеку підприємства з використанням показника продуктивності інформації, коефіцієнта інформаційної озброєності та коефіцієнт захищеності інформації. Ілляшенко С. [129] акцентує увагу на якісній стороні процесу інформаційного забезпечення суб'єкта господарювання. Ряд науковців [130] обґрунтовують доцільність використання для оцінювання рівня інформаційної безпеки п'яти показників, що характеризують інформаційно-аналітичне супроводження діяльності підприємства, захист комерційної інформації та безпеку документообігу, рівень ділової репутації та імідж продукції. Авторами роботи [131] доведено, що ефективне функціонування системи інформаційної безпеки ґрунтується на використанні імітаційного моделювання з метою прогнозування поведінки ініціаторів кіберінцидентів та розроблення комплексу превентивних заходів.

Одним із найбільш обґрунтованих є підхід, який ґрунтується на проведенні діагностики рівня інформаційної безпеки підприємства за трьома ключовими напрямами [132], кожен з яких передбачає розрахунок ряду відповідних показників:

– оцінювання програмно-технічної захищеності інформації, що ґрунтується на обчисленні коефіцієнта технічного захисту інформації, коефіцієнта програмної захищеності інформації, коефіцієнта фінансового захисту інформації, коефіцієнта фінансування інформаційних служб підприємства;

– оцінювання інформаційної надійності персоналу, що передбачає розрахунок коефіцієнта правової захищеності інформації, коефіцієнта досвіду роботи персоналу та коефіцієнта надійності персоналу, який забезпечує інформаційну безпеку підприємства, коефіцієнта підготовленості персоналу до розпізнавання загроз;

– оцінювання інформації, що надається особам, які приймають рішення, базується на обчисленні інформаційною службою підприємства коефіцієнта повноти інформації, коефіцієнта точності інформації, коефіцієнта суперечливості інформації, коефіцієнта своєчасності надання інформації, коефіцієнт надійності інформації.

Авторський колектив у складі Козубцова І., Чернонога О., Козубцової Л., Артемчука М., Нещерета І. обґрунтували пропозицій щодо вибору показників оцінювання функціонування системи захисту і кібербезпеки інформації в ІКТ спеціального зв'язку з точки зору її ефективності та здатності протидіяти кіберінцидентам [133]. Науковцями запропоновано в систему оцінювання включити показники, які дозволяють визначити здатність системи протидіяти вторгненню зловмисника до системи; загрозам конфіденційності та/або цілісності інформації; загрозам доступності інформації; шкідливим програмним засобам; спробам зловмисника щодо вторгнення до системи; махінаціям; наявності відомих вразливостей; збору інформації зловмисником; зловмисній інформації; іншим видам загроз.

Аналіз зарубіжних кейсів оцінювання рівня інформаційної безпеки суб'єктів господарювання та положень стандартів у галузі інформаційної безпеки, зокрема SP800-26 та SP800-53 (NIST), ISO/IEC 27001, ISO/IEC 21827, конструктивний огляд критеріїв, визначених SSE-CMM (Systems Security

Engineering Capability Maturity Model), TCSEC (Trusted Computer System Evaluation Criteria), ITSEC (Information Technology Security Evaluation Criteria), дозволяє узагальнити та виокремити наступні елементи для мікрорівня (табл. 2.2).

Таблиця 2.2

Напрямки та елементи оцінювання інформаційної безпеки суб'єктів господарювання

Напрям	Елемент оцінювання	Напрям	Елемент оцінювання
1	2	3	4
1. Захист даних	Організація захисту інформації	7. Кадрова безпека	Перевірка репутації
	План захисту інформації		Управління персоналом
2. Оцінка ризиків	Класифікація активів		Захист від третіх осіб
	Розподіл ресурсів	8. Реагування на інциденти	Тренінги з реагування
	Перегляд вимог до безпеки		Моніторинг інцидентів
	Оцінка ризиків		Звіти про інциденти безпеки
	Діагностика вразливості	9. Аудит та звітність	Функція створення цільової події аудиту
3. Управління конфігурацією	Оцінка змін конфігурації		Аудиторський моніторинг, аналітика та звітність
	Налаштування параметрів безпеки	10. Оцінка доступу та захист комунікацій	Управління рахунками
4. Обслуговування	Інструменти обслуговування		Керування паролями
	Дистанційне технічне обслуговування		Управління налаштуваннями
5. Підготовленість до непередбачуваних обставин	Тренування на випадок надзвичайних ситуацій		Контроль доступу
	Оновлення плану дій на випадок надзвичайних ситуацій		Функція попередження про використання системи
	Резервування комунікаційних послуг		Керування помилковими спробами доступу
	Резервне копіювання та відновлення інформаційних систем		Захищені шляхи комунікації
6. Фізичний захист	Управління фізичним доступом		Керування безпекою спільних системних ресурсів
	Керування доступом до носіїв інформації		Інструменти та технології для виявлення та запобігання вторгненням

Продовження табл. 2.2

1	2	3	4
	Контроль фізичного доступу		Захист від атак типу «відмова в обслуговуванні»
	Захист інформаційно-комунікативних технологій		Аварійне живлення
	Захист від дефектів програмного забезпечення та шкідливих програм		Функції керування сесіями

Джерело: систематизовано автором за даними [134–140]

Підсумовуючи проведений аналіз існуючих методичних підходів до оцінювання інформаційної безпеки на мікрорівні, доцільно відмітити, що вони грунтуються на визначенні здатності системи інформаційної безпеки протидіяти ризикам і загрозам, забезпечувати цілісність, конфіденційність та захищеність інформації, тобто відповідають основним цілям інформаційної безпеки. Таким чином, на основі розглянутих методик оцінки інформаційної безпеки суб'єктів господарювання правомірно сформовано алгоритм оцінювання рівня інформаційної безпеки національної економіки як базису отримання достовірного результату та формування якісних висновків (рис. 2.19).

На першому етапі відбувається визначення стратегічних цілей інформаційної безпеки з урахуванням інтересів держави (захищений інформаційний простір України, забезпечення зростання цифровізації національної економіки на безпекових засадах та ін.), регіонів (ефективне функціонування системи стратегічних комунікацій, зростання частки ІТ-сектору у ВРП та ін.), суб'єктів господарювання (високий рівень інформаційної достатності для прийняття управлінських рішень, можливість використання цифрових досягнень з метою максимізації прибутку та ін.) та громадян (підвищення рівня медіакультури та медіаграмотності, дотримання конституційних прав на вільне вираження своїх поглядів і переконань, захист приватності та ін.).

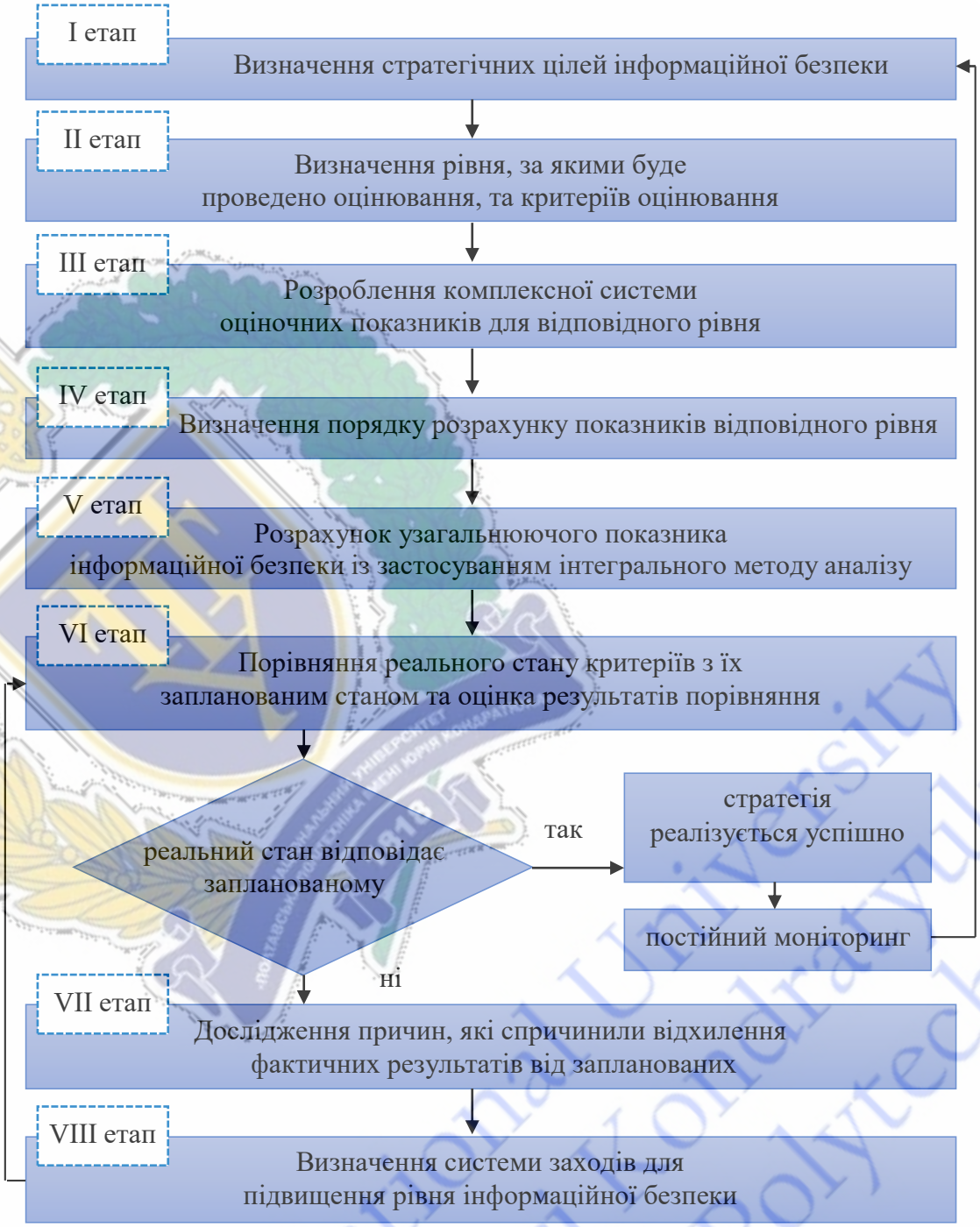

Рис. 2.19. Алгоритм оцінювання рівня інформаційної безпеки національної економіки

Джерело: розроблено автором

Другий етап передбачає визначення рівнів, за якими буде проведено оцінювання інформаційної безпеки, та критеріїв оцінювання. Враховуючи визначених суб'єктів безпеки, доцільно проводити діагностику на макро-, мезо-, мікро- та нанорівнях.

В загальному розумінні критерії – це ознака, на основі якої проводиться оцінка якості економічних об’єктів та процесів, порівняння альтернатив, класифікація об’єктів і явищ. Таким чином, в контексті предмета дослідження під критерієм слід розуміти ознаку чи сукупність ознак, на підставі яких визначається сучасний рівень інформаційної безпеки та здатність до його підвищення.

В межах третього етапу проводиться розроблення та затвердження системи оціночних показників для відповідного рівня, а також визначаються причинно-наслідкові зв’язки показників, напрямів реалізації та критеріїв їх оцінки. Підбір показників є досить важливим, оскільки від їх об’єктивності та всебічності буде залежати достовірність результатів оцінювання рівня інформаційної безпеки.

На четвертому етапі визначаються алгоритми розрахунку оціночних показників для кожного рівня, специфіка яких буде залежати від належності показників до якісних чи кількісних. У випадку наявності якісних індикаторів для приведення їх до кількісного вигляду правомірно застосовувати метод квантування. Розрахунок узагальнюючого показника інформаційної безпеки із застосуванням інтегрального методу аналізу проводиться в рамках п’ятого етапу. При цьому узагальнюючий показник відображає підсумкові результати синергетичної дії чинників, які характеризують інформаційну безпеку на різних рівнях (макро-, мезо-, мікро- , нанорівень).

Наступним етапом є порівняння реального стану критеріїв з їх запланованим станом, а також оцінка результатів порівняння. Якщо реальний рівень відповідає запланованому, то заходи спрямовуються на підтримку чи підвищення. В протилежному випадку відбувається перехід до сьомого етапу, на якому здійснюється дослідження причин незадовільного рівня інформаційної безпеки. Заключний етап передбачає визначення системи заходів для підвищення інформаційної безпеки за окресленими раніше рівнями (макро-, мезо-, мікро-, нанорівень).

Виходячи з обґрунтованого значення інформаційної безпеки в системі національної безпеки, взаємозв’язку процесів цифровізації національної

економіки і необхідністю підвищення рівня захищеності інформаційного простору, з метою доведення гіпотези щодо існування взаємообумовлених впливів між системою інформаційної безпеки та національною економікою, актуалізується питання оцінювання рівня інформаційної безпеки на макрорівні. Враховуючи законодавчу визначеність стратегічних цілей інформаційної безпеки держави, необхідним постає розроблення збалансованої системи оціночних показників (третій етап згідно розробленого алгоритму оцінювання рівня інформаційної безпеки).

В Україні на сьогодні немає загальноприйнятої методики, яка б дозволила оцінити рівень інформаційної безпеки на макрорівні. Водночас, розроблено ряд світових індексів, які спрямовані на оцінювання ефективності інформаційної політики країн. Зокрема, Індекс свободи преси (Press Freedom Index, PFI), розроблений міжнародною недержавною організацією Репортери без кордонів (Reporters sans frontières, RSF), який дозволяє визначити рівень свободи преси, відкритості й прозорості інформаційного середовища та розраховується для 180 країн. Рейтинг формується на основі результатів анкетування журналістів, науковців й інших спеціалістів в усьому світі, та передбачає присвоєння балів від 0 до 100. Ця оцінка розраховується на основі двох компонентів: кількісний підрахунок зловживань щодо журналістів у зв'язку з їх роботою та засобів масової інформації; якісний аналіз ситуації в кожній країні на основі відповідей спеціалістів зі свободи преси. Якісний аналіз ґрунтується на п'яти контекстуальних показниках, які характеризують інформаційну політику країни в напрямку забезпечення прозорості й відкритості національного інформаційного середовища поряд із захистом інтересів громадян: політичний контекст, правова база, економічний контекст, соціокультурний контекст і безпека [141]. Показники PFI дають можливість оцінити сприятливість регуляторного середовища для забезпечення інформаційної стійкості держави і доступу усіх суб'єктів до достовірної та об'єктивної інформації, рівень ефективності державної підтримки (в тому числі економічної) функціонування

незалежних ЗМІ, що, безперечно, характеризує окремі аспекти інформаційної безпеки національної економіки.

Також існує ряд індексів, які містять індикатори, що характеризують рівень впровадження інформаційно-комунікаційних технологій в економічну систему та їх доступність для економічних суб'єктів усіх рівнів (особа, домогосподарство, суб'єкт господарювання): Індекс соціального прогресу (Social Progress Index, SPI), Індекс розвитку е-урядування (E-Government Development Index, EGDI), Глобальний індекс інновацій (Global Innovation Index, GII) та Рейтинг світової цифрової конкурентоспроможності (World Digital Competitiveness Rankings, WDCR). Так, SPI, спрямований на оцінювання рівня задоволення потреб суспільства, містить 54 індикатори, які згруповані за трьома напрямками: задоволення базових людських потреб, забезпечення основ благополуччя (серед яких доступ до інформації та комунікацій) та забезпечення кожній особі можливості реалізації власного потенціалу [142]. EGDI містить три субіндекси (індекс онлайн-сервісів, індекс телекомунікаційної інфраструктури, індекс людського капіталу) і дає змогу оцінити готовність національних урядів використовувати інформаційно-комунікаційні технології з метою надання якісних інформаційних і державних послуг населенню та бізнесу. Слід відмітити, що як додаток до Індексу розвитку е-урядування використовується Індекс електронної участі (E-Participation Index, EPI). Рейтинг EPI оцінює електронну участь відповідно до трирівневої моделі: використання інтерактивних послуг для надання інформації урядами громадянам, взаємодія та консультації з громадянами та участь громадян в процесах ухвалення державних рішень [143]. У 2020 році у рейтингу EPI Україна піднялася на 29 позицій та посіла 46 місце зі 193 країн. Це стало можливим завдяки реалізації ідеї «держави в смартфоні» та створення Міністерством цифрової трансформації України застосунку «Дія».

Ще один комплексний показник, який дозволяє оцінити рівень розвитку та впровадження інформаційних технологій в економічну систему – Глобальний індекс інновацій [144], який розраховується з 2007 року у рамках спільного проєкту Всесвітньої організації інтелектуальної власності (World Intellectual

Property Organization), Корнельського університету (Cornell University) та Міжнародної бізнес-школи INSEAD. Рейтинг оцінює рівень інноваційного розвитку, ефективність інноваційної екосистеми за даними 132 країн світу. GII включає близько 80 показників та розраховується як зведена сума оцінок двох груп індикаторів: Innovation Input – наявні ресурси й умови для формування інновацій; Innovation Output – досягнуті практичні результати реалізації інновацій.

WDCR, розроблений дослідницьким центром у Швейцарії (IMD World Competitiveness Center), спрямований на оцінювання рівня цифровізації національних економік на основі 54 критеріїв, обєднаних у три групи: готовність до цифрового майбутнього (здатність бізнесу до швидкої адаптації в нових умовах та IT-інтеграція, ставлення до адаптації), цифрові знання (кадри, освіта та концентрація наукових знань) та цифрові технології (нормативно-правове регулювання процесів цифровізації, капітал і технологічна інфраструктура). Одним із головних висновків, які зробили розробники рейтингу на основі результатів дослідження, що головним пріоритетом для державного та приватного секторів у країнах з цифровою економікою є розроблення та впровадження дієвих заходів з кібербезпеки [145]. Забезпечити конкурентоспроможність, в тому числі цифрову, не можливо без високого рівня кібербезпеки та інформаційної безпеки країни в цілому.

Тому поряд з індексами, які дозволяють оцінити рівень ефективності інформаційної політики, що безпосередньо впливає на інформаційну безпеку країни, правомірно окреслити ряд глобальних індексів, що дозволяють визначити можливості країни у сфері кіберзахисту, оцінити рівень її кіберпотужності, зокрема спроможності регуляторних заходів і засобів досягти стратегічних цілей кібербезпеки як невід'ємної складової інформаційної безпеки [146]. Так, у 2020 році Центром науки та міжнародних відносин Роберта та Рене Бельфера (Belfer Center for Science and International Affairs) вперше опубліковані результати розрахунку Національного індексу кіберпотужності (National Cyber Power Index, NCPI), який оцінює ефективність державної стратегії у напрямі

запобігання кіберзагрозам, реагування на правопорушення та боротьби з ними, а також рівень ефективності робочої сили й інновацій у сфері кібербезпеки [147].

NCPI ґрунтується на визначенні рейтингу 30 країн у контексті семи національних цілей та включає Індекс кібернамірів (Cyber Intent Index, CII) та Індекс кіберможливостей (Cyber Capability Index, CCI). Індекс кібернамірів базується на розрахунку 32 індикаторів, які згруповані за національними цілями: спостереження, захист, контроль, розвідка, торгівля, правопорушення і норми. Індекс кіберможливостей передбачає оцінювання 27 індикаторів можливостей, об'єднаних у вісім груп: докази атак; національний онлайн-контент; національні кіберструктури; зменшення кібервразливості; приватний сектор, торгівля та інновації; зв'язок; робоча сила; законодавство та державна політика.

Національний індекс кіберезпеки (National Cyber Security Index, NCSI), розроблений Фондом академії електронного врядування Естонії, дозволяє оцінити готовність країн до запобігання кіберзагрозам й управління кіберінцидентами. NCSI включає 12 індикаторів за напрямами: моніторинг та аналіз кіберзагроз, освіта та підвищення кваліфікації у сфері кіберзахисту, розробленість політики з кібербезпеки, внесок у глобальну кібербезпеку, захист основних послуг у кіберпросторі, захист цифрових сервісів, захист персональних даних, послуги електронної ідентифікації, кіберкризове управління, реагування на кіберінциденти, боротьба з кіберзлочинністю і військові кібероперації [148].

Міжнародним союзом електрозв'язку (International Telecommunication Union, ITU) у 2014 році був розроблений Глобальний індекс кібербезпеки (Global Cybersecurity Index, GCI), який характеризує здатність протистояти кібератакам та забезпечувати роботу об'єктів критичної цифрової інфраструктури національної економіки. GCI містить 25 індикаторів за п'ятьма напрямами: правовий (рівень розробленості законодавчої бази у сфері кібербезпеки), організаційний (національні стратегії кібербезпеки), технічний (рівень реалізації технічних можливостей кіберзахисту через національні й галузеві агенції), розбудова потенціалу (інформаційне забезпечення, освіта і наявні стимули для розвитку потенціалу кібербезпеки), співробітництво (рівень розвитку

партнерства у сфері кібербезпеки). Розрахунок індикаторів, що використовуються для визначення Глобального індексу кібербезпеки, базується на карті дерева розвитку кібербезпеки та бінарних варіантах реагування [149].

Динаміка позицій України у зазначених рейтингах подана в таблиці 2.3.

Таблиця 2.3

Позиції України у глобальних рейтингах, які характеризують рівень інформаційної безпеки національної економіки

Рейтинг / Роки	Press Freedom Index	Social Progress Index	E-Government Development Index	Global Innovation Index	World Digital Competitiveness Rankings	Global Cybersecurity Index	National Cyber Security Index
2013	126	-	-	71	54	-	-
2014	127	62	87	63	50	-	-
2015	129	62	-	64	59	70	-
2016	107	63	62	56	59	59	24
2017	102	88	-	50	60	58	26
2018	101	64	82	43	58	54	29
2019	102	80	-	47	60	-	28
2020	96	63	69	45	58	79	25
2021	97	48	-	49	54	78	24
2022	106	52	46	57	-	-	-

Джерело: складено автором на основі даних [141–145, 147, 148]

Аналізуючи позиції України у світових рейтингах, правомірно зробити наступні висновки. Згідно з даними Індексу свободи преси, у 2022 році Україна посіла 106 місце серед 180 можливих. Міжнародна правозахисна організація «Репортери без кордонів» зниження рейтингу України пов’язує з військовою агресією рф, відмічаючи такі фактори як небезпечні умови для ЗМІ, високий рівень цензури на окупованих територіях та масову дезінформацію.

За офіційними даними, країна-агресор скоїла більше 500 злочинів проти представників преси та ЗМІ. Загинуло більше 60 українських та зарубіжних медійників, частина перебуває в ув’язненні. Лідерами рейтингу є Норвегія, Ірландія, Данія і Швеція [150].

Доцільно відмітити, що на початку травня 2023 року був опублікований «Індекс свободи преси 2023», згідно з яким Україна зайняла найкращу позицію

за часи незалежності, піднявшись на 27 пунктів і посівши 79 місце [151]. Головною причиною визначено економічну стабілізацію ЗМІ. У цьогорічному звіті також підкреслені катастрофічні наслідки інформаційного хаосу у нерегульованому світовому інформаційному онлайн-середовищі, де поширюються фейкові новини і пропаганда.

За рівнем соціального розвитку Україна у 2021 році посіла 48 місце, піднявшись на 15 позицій серед 163 країн із показником індексу 73,38 бали порівняно з 66,97 2019 року. У 2020 році, переважно через пандемію, погіршення доступу до необхідних медичних послуг та навантаження на системи охорони здоров'я, кількість країн, які входять до числа держав з дуже високим рівнем якості життя, високим рівнем якості життя та помірно високим рівнем якості життя – скоротилась із 104 до 71 [152]. У 2022 році відбулася втрата позицій (4 пункти) і Україна в рейтингу зайняла 52 місце із показником індексу 74,17. Це свідчить про позитивну динаміку країни в напрямку соціального розвитку. Втім ряд країн розвиваються більш динамічно.

У 2020 році Україна посіла 69-те місце у рейтингу країн з найвищим рівнем розвитку електронного урядування, піднявшись на 13 позицій у порівнянні із 2018 роком. У 2022 році Україна піднялася на 46 позицію завдяки зростанню таких складових як індекс он-лайн послуг та індекс телекомунікаційної інфраструктури. Дослідження «E-Government Survey 2020» показує, що Україна належить до групи країн із високим рівнем розвитку. Зростання рейтингу України значною мірою зумовлено впровадженням державних он-лайн сервісів та платформ, зокрема додатку «Дія». Очолюють рейтинг такі країни, як Данія, Фінляндія, Південна Корея.

В рейтингу Global Innovation Index порівнюється інноваційність економік 132 країн світу. Згідно зі звітом 2022 року найбільш інноваційними країнами визнано Швейцарію, США, Швецію, Велику Британію та Нідерланди. Україна в Глобальному інноваційному індексі 2021 року посідає 57 місце, ввійшовши до ТОП-3 країн економічної групи lower-middle income [153]. Динаміка позицій України у проаналізованих рейтингах представлена на рисунку 2.20.

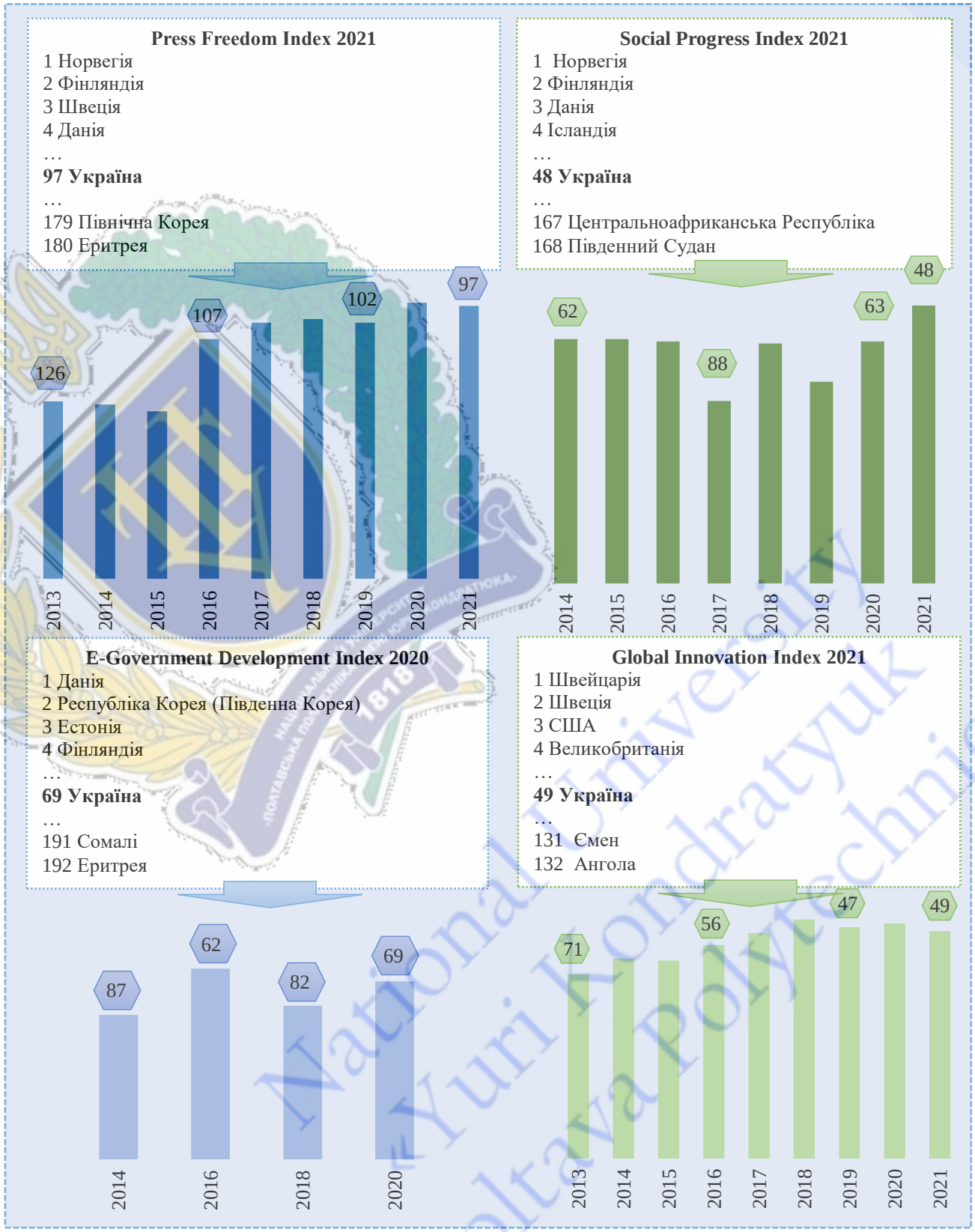

Рис. 2.20. Інфографіка позицій України у світових рейтингах, які характеризують інформаційну безпеку національної економіки

Джерело: побудовано автором на основі даних [141–145, 147–154]

Водночас, у рейтингу WDCR 2021 Україна займає останні позиції: 54 місце із 63 країн світу. Зазначена ситуація пояснюється низькими значеннями показників цифрових технологій і цифрової готовності. Щодо висновку, опублікованого за рейтингом 2022 року, лідируючу позицію займає Данія. Аналітиками відмічено необхідність підвищення захисту цифрової інфраструктури від кібератак у напрямі розвитку цифрової конкурентоспроможної економіки. Через обмежену надійність зібраних даних, неможливість підтвердження їх достовірності, Україна не включена до рейтингу 2022 року.

Рейтингова позиція України у Глобальному індексі кібербезпеки у 2016 р. склала 59 місце зі 175 країн, у 2017 році – 58 місце зі 194 країн, а у 2021 році – 78 місце. Тобто спостерігається зниження рівня індексу кібербезпеки. Причиною цього можна визначити активізацію кібератак з боку російської федерації на об’єкти критичної інфраструктури України. Водночас у рейтингу NCSI Україна займає лідируючі позиції серед 160 країн та входить у ТОП-30 держав з найвищим рівнем кібербезпеки.

Дані рисунку 2.21 підтверджують наявність потенційних можливостей підвищення рівня кібербезпеки національної економіки.

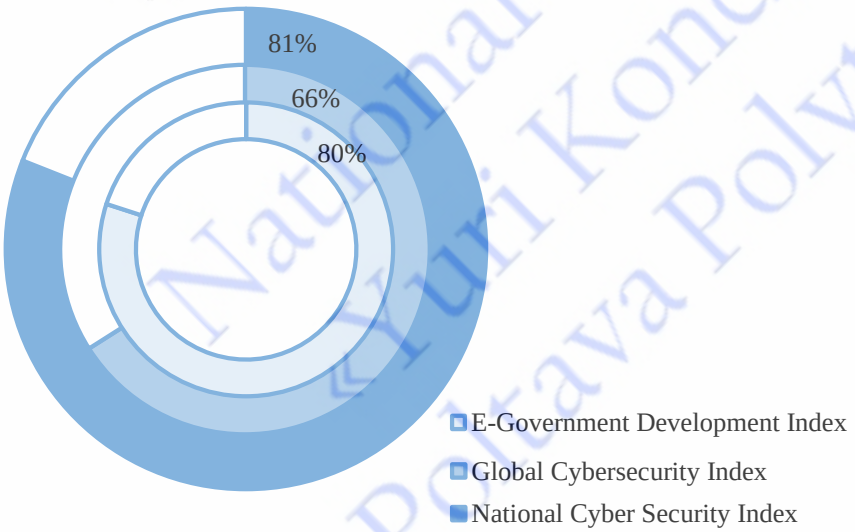

Рис. 2.21. Інфографіка відсоткових показників виконання Україною міжнародних рейтингів з кібербезпеки у 2022 році

Джерело: побудовано автором на основі даних [143, 147, 148]

Таким чином, окреслені рейтинги правомірно покласти в основу розрахунку інтегрального показника рівня інформаційної безпеки національної економіки. Ґрунтуючись на розробленому алгоритмі (див. рис. 2.19) представимо модель оцінювання, яка має бути реалізована на п’ятому етапі.

Для згортки часткових показників у інтегральний використовують ряд методів: розрахунок багатовимірної середньої, таксономічний метод, теорію нечітких множин. При проведенні економічних досліджень найчастіше використовується таксономічний метод, який має основну перевагу: дозволяє працювати з багатовимірними економічними об’єктами, які описуються досить великим спектром показників [155, с. 121]. За допомогою методу таксономії можна об’єднати значення декількох різнорідних показників, що характеризують рівень інформаційної безпеки національної економіки протягом кількох часових періодів та розрахувати інтегральний показник інформаційної безпеки національної економіки. Розрахунок здійснюється за наступним алгоритмом (рис. 2.22).

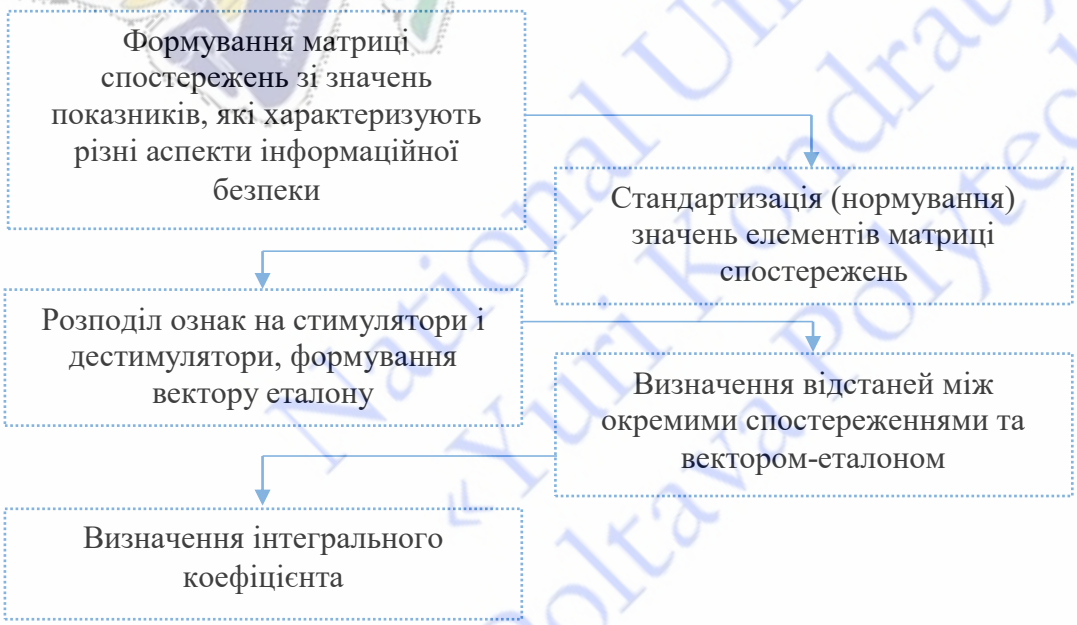

Рис. 2.22. Алгоритм розрахунку інтегрального показника інформаційної безпеки національної економіки з використанням таксономічного методу

Джерело: складено автором

При побудові інтегрального показника застосовують матрицю спостережень, складену зі значень показників, які характеризують різні компоненти інформаційної безпеки національної економіки, за які приймаємо місце України в міжнародних рейтингах і доцільність використання яких обґрунтовано.

Враховуючи, що місце України в міжнародних рейтингах є якісним показником, необхідно привести показники до кількісного виду. Стандартизація (нормування) вихідних даних передбачає вирівнювання дисперсії (кожна дисперсія стає рівною 1), а також значень ознаки (всі середні арифметичні дорівнюють нулю). Сутність методу нормування вхідних показників – це приведення їх до такого масштабу вимірювань, за якого «найкраще» значення показника дорівнює 1, а «найгірше» – 0. Використовуючи нормування в аспекті економічного дослідження, результатом є перехід від абсолютних значень показників до нормованих (стандартизованих) значень, що мають діапазон від 0 до 1, і вже за своєю величиною характеризують ступінь наближення до оптимального значення, що також можна інтерпретувати у відсотках: 0 відповідає 0%, 1 – 100%.

Під час формування ознакового простору (множини індикаторів) необхідно забезпечити інформаційну одновекторність показників. З цією метою відбувається розподіл ознак на стимулятори і дестимулятори. Зв’язок між інтегральним коефіцієнтом і показниками-стимуляторами прямий, а між інтегральним коефіцієнтом і показниками-дестимуляторами – обернений [156, с. 250–254].

Визначення інтегрального показника ґрунтується на застосуванні вагових коефіцієнтів, які дозволяють врахувати рівень впливу кожного індикатора. Отримані значення таксономічного інтегрального коефіцієнта показують тенденцію в змінах рівня інформаційної безпеки національної економіки. Чим ближче значення інтегрального показника до 1, тим рівень вищий.

Водночас для трактування результатів оцінювання рівня інформаційної безпеки національної економіки доцільно використати теорію нечітких множин.

Нечіткі описи застосовуються при складності розмежування понять «високого» і «максимального» рівня показника, або при необхідності проведення межі між «середнім» і «низьким» рівнями. У цьому випадку застосовується функція належності.

Загальновживаними функціями належності в теорії нечітких множин є трапицієвидні функції належності, аналітичне представлення яких забезпечує простоту і зручність виконання операцій над нечіткими множинами. Опис підмножин значень лінгвістичної змінної «рівень показника» здійснюють із використовуванням системи з п'яти функцій належності трапицевидної форми (стандартний п'ятирівневий 01-класифікатор).

У відповідності до п'ятирівневого нечіткого класифікатора, рівень інформаційної безпеки може характеризуватися наступними значеннями та знаходитися в одному з п'яти інтервалів (табл. 2.4).

Таблиця 2.4

Шкала оцінювання рівня інформаційної безпеки

Рівень безпеки / Значення	Дуже високий (безпечний) рівень	Високий (задовільний) рівень	Середній (незадовільний) рівень	Низький (небезпечний) рівень	Дуже низький (критичний) рівень
1-0,80					
0,80-0,60					
0,60-0,40					
0,40-0,20					
0,20-0					

Джерело: складено автором на основі [156, с. 250–254; 157]

Отже, на сьогодні питання формування інформаційної безпеки національної економіки знаходиться на стадії розроблення: відсутній єдиний підхід до аналізу стану та єдиних правил побудови системи оцінювання її рівня. Особливістю є наявність методичних підходів до оцінювання рівня інформаційної захищеності суб'єктів господарювання. Хоча і в цьому напрямку констатується відсутність комплексності.

З метою обґрунтованого та своєчасного визначення заходів із попередження й подолання негативних наслідків у випадку реалізації потенційних ризиків та загроз необхідним є здійснення моніторингу стану інформаційної безпеки. Перспективним напрямом має стати затверджена на державному рівні Методика розрахунку рівня інформаційної безпеки національної економіки з чітким переліком індикаторів та обґрунтованими пороговими значеннями.

2.3. Оцінювання інформаційної безпеки економіки України

Непередбачуваність і агресивність зовнішнього інформаційного середовища викликає необхідність розроблення ефективних інструментів забезпечення інформаційної безпеки національної економіки. Побудова економіко-математичних моделей оцінки, аналізу, прогнозування та управління інформаційною безпекою є актуальним завданням, що вимагає напрацювання підходів і методів вирішення. Розроблений у підпункті 2.2 методичний підхід до оцінювання рівня інформаційної безпеки національної економіки потребує апробації з метою підтвердження його якості та практичної значущості.

З урахуванням алгоритму розрахунку інтегрального показника інформаційної безпеки національної економіки (див. рис. 2.22), в першу чергу, необхідно сформувати матрицю спостережень, що складається зі значень обраних індикаторів – показників України в міжнародних рейтингах, які характеризують різні аспекти інформаційної безпеки національної економіки (Додаток Г, табл. Г.1). Формування множини індикаторів відбувалося за принципом репрезентативності (у підпункті 2.2 здійснено обґрунтування ряду глобальних індексів, показники яких характеризують інформаційну безпеку національної економіки) та принципом інформаційної доступності (використовувалися офіційні статистичні дані й публічні експертні оцінки). Оскільки матриця може бути представлена у схематичному чи табличному форматі, обрано останній варіант (табл. 2.5).

Таблиця 2.5

Макет матриці спостережень

	1	2	…	n
i_1	i_{11}	i_{12}	…	i_{1n}
i_2	i_{21}	i_{22}	…	i_{2n}
…	…	…	…	…
i_m	i_{m1}	i_{m2}	…	i_{mn}

Джерело: складено автором

Розмірність матриці спостережень становить $m \times n$ і залежить від кількості показників, введених у матрицю (i_m) та кількості періодів дослідження (n). Усі елементи матриці позначаються двома підрядковими індексами, з яких перший означає номер рядка, другий – номер стовпчика.

У відповідності до сформованої матриці інтегральний індекс інформаційної безпеки національної економіки об'єднує сім індикаторів.

$$I_i = \{i_{m1n}, i_{m2n}, i_{m3n}, i_{m4n}, i_{m5n}, i_{m6n}, i_{m7n}\} \quad (2.1)$$

де $i_{m1n}, i_{m2n}, i_{m3n}, i_{m4n}, i_{m5n}, i_{m6n}, i_{m7n}$ – позиції України у міжнародному рейтингу m в n періоді.

Враховуючи, що індикаторами інформаційної безпеки національної економіки визначено позиції України в міжнародних рейтингах, тобто якісні характеристики, відмінні за економічним змістом, необхідно привести їх до єдиної шкали вимірювання. Цей процес може ґрунтуватися на використанні різних методів, а саме методу функціональних залежностей, стохастичного методу, макроекономічних моделей, нелінійної динаміки та інших. У дослідженні стандартизацію (нормування) показників, тобто трансформацію у безрозмірні величини, здійснено з використанням розмаху варіації за формулою (2.2), наведеною нижче. Результати розрахунку подано в таблиці Г.2 Додатку Г.

$$i_{mn(\text{ст})} = \frac{i_{mn}}{i_{max} - i_{min}} \quad (2.2)$$

де i_{mn} – місце України у міжнародному рейтингу, що характеризує інформаційну безпеку національної економіки;

i_{max}, i_{min} – порогові значення і-го індикатора у діапазоні характеристичних значень.

На основі методу нормування відбулося узгодження кількісних показників і приведення їх до єдиного оптимального вигляду з діапазоном [0..1].

Враховуючи відсутність офіційних даних по показниках за окремі роки, необхідним виступає здійснення прогнозування з використанням методу згладжування. З метою забезпечення обґрунтованості та статистичної адекватності результатів, вибору оптимального виду рівняння при прогнозуванні величин, розраховано коефіцієнт детермінації R^2 для різних варіантів лінії тренду, що характеризує достовірність апроксимації: чим ближче значення R^2 до одиниці, тим надійніше лінія тренда апроксимує досліджуваний показник (Додаток Г, табл. Г.3). На основі отриманих результатів розраховані значення відсутніх показників (Додаток Г, табл. Г.4).

Наступним етапом апробації методичного підходу до оцінювання рівня інформаційної безпеки національної економіки є розподіл ознак на стимулятори і дестимулятори та визначення відстаней між окремими спостереженнями та вектором-еталоном (об'єктом-еталоном). Усі індикатори інформаційної безпеки національної економіки є стимуляторами і мають однакову спрямованість. Еталонний об'єкт являє собою вектор, компонентами якого є оптимальні значення кожного з показників досліджуваної системи [158, 159]. При використанні позицій України в міжнародних рейтингах як індикаторів інформаційної безпеки національної економіки об'єктом еталоном правомірно визначити перше місце у рейтингу. Нормування показників здійснено за наступною формулою.

$$i_{mn(\text{норм})} = 1 - i_{mn(\text{ст})} \quad (2.3)$$

Нормовані показники рівня інформаційної безпеки національної економіки наведено в таблиці Г.5 Додатку Г.

Розрахунок інтегрального коефіцієнту інформаційної безпеки національної економіки проводиться методом зважених сум за формулою:

$$I = \Sigma b_i * i_{mn(\text{норм})} \quad (2.4)$$

де b_i – вагові коефіцієнти складових інформаційної безпеки національної економіки;

$i_{mn(\text{норм})}$ – нормовані показники складових інформаційної безпеки національної економіки.

При цьому $0 \leq b_i \leq 1$, а $\Sigma b_i = 1$.

Для визначення вагових коефіцієнтів складників інформаційної безпеки національної економіки застосовано метод експертних оцінок. До експертного оцінювання було залучено групу експертів у складі 10 кандидатів наук та 10 докторів наук. На основі заповнених експертами анкет сформовано матрицю оцінок ранжируваних факторів (Додаток Д). Алгоритм визначення вагомості показників та рівня узгодженості думок наступний.

1. Розраховується сума оцінок по рядках (ΣS_j – сума оцінок кожного експерта) та по стовпцях (ΣS_i – сума оцінок експертів по кожному показнику). При цьому $\Sigma S_j = \Sigma S_i$.

2. Вагомість кожного показника (ваговий коефіцієнт) визначатиметься за формулою:

$$b_i = \frac{\bar{S}_i}{\sum \bar{S}_i} \quad (2.5)$$

де $\bar{S}_i$ – середня оцінка по i-му показнику;

$\sum \overline{S_i}$ – сума середніх оцінок експертів по показниках.

3. Для формування загальної оцінки щодо вагомості кожного показника необхідно визначити середнє арифметичне з оцінок по кожному фактору:

$$\bar{S} = \frac{\sum S_i}{j} \tag{2.6}$$

де $\sum S_i$ – сума оцінок експертів по кожному показнику;

j – кількість експертів.

3. Визначається відхилення від середньої $S_i - \bar{S}$ та квадрат відхилень $(S_i - \bar{S})^2$.

4. Для визначення рівня узгодженості оцінок експертів розраховується коефіцієнт конкордації:

$$W = \frac{12 \times \sum (S_i - \bar{S})^2}{j^2 \times (i^3 - i)} \tag{2.7}$$

де j – кількість експертів;

i – кількість показників.

На основі розрахунку коефіцієнта конкордації підтверджується чи спростовується гіпотеза щодо наявності згоди між фахівцями та достовірності результатів анкетування експертної групи. Коефіцієнт конкордації знаходиться в межах від 0 до 1. У випадку, коли значення коефіцієнта дорівнює 0 – узгодженості думок експертів немає; коли 1 – оцінки експертів характеризуються найвищим рівнем узгодженості [160].

$$W = \frac{12 \times 9972}{20^2 \times (7^3 - 7)} = 0{,}89$$

Розрахований коефіцієнт конкордації засвідчив високий ступінь узгодженості оцінок експертів, тобто метод експертної оцінки є достовірним і отримані вагові коефіцієнти (табл. 2.6) можна застосовувати в методиці оцінювання рівня інформаційної безпеки національної економіки.

Таблиця 2.6

Рівень вагомості складових інформаційної безпеки національної економіки

Складова	Коефіцієнт вагомості	Ранг
Press Freedom Index	0,10	3
Social Progress Index	0,10	3
E-Government Development Index	0,15	2
Global Innovation Index	0,10	3
World Digital Competitiveness Rankings	0,15	2
Global Cybersecurity Index	0,20	1
National Cyber Security Index	0,20	1

З урахуванням значимості окреслених складових інформаційної безпеки національної економіки, з використанням формули (2.4), визначено інтегральний показник інформаційної безпеки економіки України (табл. 2.7).

Таблиця 2.7

Визначення інтегрального показники рівня інформаційної безпеки національної економіки України за 2013 – 2021 роки з урахуванням вагових коефіцієнтів

Роки / Складові	2013	2014	2015	2016	2017	2018	2019	2020	2021
1	2	3	4	5	6	7	8	9	10
Press Freedom Index	0,0300	0,0294	0,0283	0,0406	0,0433	0,0439	0,0433	0,0467	0,0461
Social Progress Index	0,0620	0,0620	0,0620	0,0613	0,0460	0,0607	0,0509	0,0613	0,0706
E-Government Development Index	0,0824	0,0824	0,0921	0,1018	0,0940	0,0863	0,0913	0,0964	0,0964
Global Innovation Index	0,0462	0,0523	0,0515	0,0576	0,0621	0,0674	0,0644	0,0659	0,0629

Продовження табл. 2.7

1	2	3	4	5	6	7	8	9	10
World Digital Competitiveness Rankings	0,0214	0,0310	0,0095	0,0095	0,0071	0,0119	0,0071	0,0119	0,0214
Global Cybersecurity Index	0,1200	0,1200	0,1200	0,1326	0,1402	0,1443	0,1314	0,1186	0,1196
National Cyber Security Index	0,1700	0,1700	0,1700	0,1700	0,1675	0,1638	0,1650	0,1688	0,1700
Інтегральний показник інформаційної безпеки національної економіки, %	53,20	54,70	53,34	57,34	56,04	57,83	55,36	56,95	58,69

Джерело: розраховано автором

Динаміка розрахованого інтегрального індексу інформаційної безпеки економіки України представлена на рисунку 2.23.

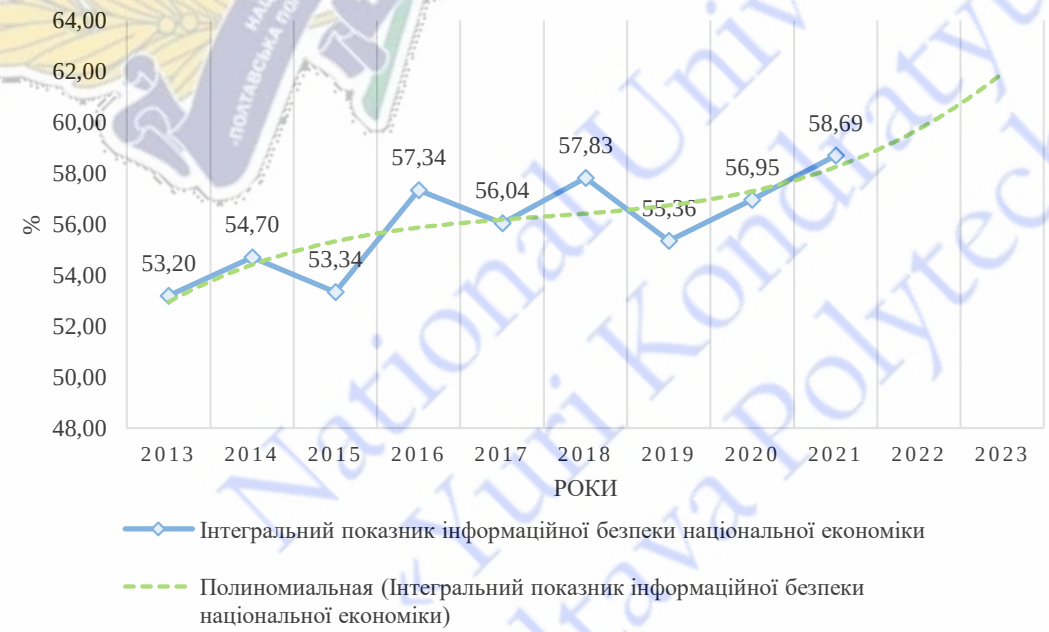

Рис. 2.23. Динаміка рівня інформаційної безпеки національної економіки України у 2013 – 2021 роках

Джерело: побудовано автором

При максимальному значенні рівня інтегрального показника інформаційної безпеки країни у 100%, найбільший спостерігався 2021 р. Падіння рівня інформаційної безпеки у 2015 році пов'язане з військовою агресією російської федерації на сході країни та активізацією атак в інформаційному просторі, а у 2019 році – з пандемією COVID-19 та активізацією кіберзлочинів [161].

Оптимальною зоною для рівня інформаційної безпеки правомірно визначити показник вище 80% (80–100%), задовільний 60–80%, незадовільний – 40–60%, небезпечний – діапазон значень 20–40%, критичний – менший за 20% (0–20%). За весь аналізований період 2013–2021 рр. рівень інформаційної безпеки знаходився на незадовільному рівні (40–60%), але не виходячи з меж безпечної зони. Водночас, прогнозована позитивна динаміка інтегрального показника, описана поліноміальною лінією тренда, підтверджується активізацію України в напрямку впровадження заходів підвищення рівня інформаційної безпеки національної економіки [162].

Зазначена позитивна динаміка пов'язана, зокрема, з удосконаленням вітчизняного законодавства у сфері інформаційної безпеки та кібербезпеки, як її невід'ємної складової. Також розширюється співпраця з міжнародними організаціями у сфері кібербезпеки. У вересні 2021 року Державна служба спеціального зв'язку та захисту інформації України уклала угоду з Агенством з кібербезпеки та безпеки інфраструктури США, що передбачає: координацію дій із захисту критично важливих об'єктів інформаційної інфраструктури та вдосконалення системи реагування на кіберінциденти; використання позитивного досвіду США щодо організації взаємодії державних органів та бізнесу у сфері кібербезпеки; обмін досвідом у межах системи управління ризиками, що забезпечить національну стійкість України до кіберзагроз; реалізацію проєктів міжнародної технічної допомоги з побудови мережі галузевих та регіональних операційних центрів безпеки (Security Operation Centers) і груп реагування (CSIRT), передбачених Стратегією кібербезпеки України.

На початку квітня 2022 року Україна увійшла до складу Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) як учасник-контрибутор. Приєднання України до складу CCDCOE надає можливість обмінюватися досвідом щодо виявлення та протидії сучасним кіберзагрозам, розвивати можливості спільного реагування на кібератаки, а також проводити операції із захисту та стримування в кіберпросторі.

Розвиток міжнародного співробітництва для зміцнення кіберстійкості економічного простору України є пріоритетом для запобігання глобальним кіберзагрозам, забезпечення високого рівня якості розслідування кіберзлочинів, затримання та переслідування зловмисників, а також подолання проблем кібербезпеки.

Водночас є напрями у сфері кібербезпеки, які негативно впливають на позиції України у розглянутих рейтингах і потребують вдосконалення. Зокрема, поточний низький рівень внеску в глобальну кібербезпеку, недостатній рівень захисту цифрових сервісів і нерозвиненість напряму військових кібероперацій.

Слід зазначити, що з початку 2022 року ведеться активна діяльність щодо подолання окреслених проблемних аспектів: Україна стала активним учасником міжнародного співробітництва у сфері кібербезпеки; триває процес формування кібервійська [163], що відповідає за інформаційну безпеку, захист критичної інфраструктури і розвідку.

Ураховуючи досягнення України, правомірно визначити її рівноправним учасником на міжнародній арені у сфері інформаційної та кібербезпеки. Перспективними завданнями мають стати подальше вдосконалення систем захисту інформації об'єктів критичної інфраструктури на основі найкращих світових практик та координація дій з міжнародними організаціями щодо протидії загрозам, пов'язаним із розвитком цифрової економіки та інформаційного суспільства.

Комплексний та комунікаційний аспекти системного підходу у дослідженні передбачають, з одного боку, визначення інформаційної безпеки національної економіки як самостійного елементу національної безпеки, а з

іншого – як інтегрованої складової будь-якої іншої безпеки, зокрема економічної. Тому наступним етапом дослідження є доведення взаємозв'язку між інформаційною та економічною безпекою. Інтегральний показник рівня економічної безпеки розраховується на основі Методичних рекомендацій щодо розрахунку рівня економічної безпеки України [157]. У дослідженні використані оприлюднені офіційні дані Міністерства економіки України [164], узагальнені в Додатку Е. Проведений розрахунок відхилення середнього значення інтегрального показника рівня економічної безпеки України та субіндексів від максимального й мінімального значень засвідчив відсутність різких коливань рівня економічної безпеки протягом досліджуваного періоду. Рівень економічної безпеки України є стабільно незадовільним.

Вводиться гіпотеза, що між фактором I (рівнем інформаційної безпеки національної економіки) та показником E (рівнем економічної безпеки) існує лінійна стохастична залежність $E = aI + b$. Для визначення параметрів a і b моделі за методом найменших квадратів розв'язується система нормальних рівнянь:

$$\begin{cases} a\sum_i I_i^2 + b\sum_i I_i = \sum_i I_i E_i \quad (i = \overline{1,n}); \\ a\sum_i I_i + bn = \sum_i E_i \quad (i = \overline{1,n}); \end{cases} \tag{2.8}$$

де a, b – параметри рівняння;

I_i – інтегральний показник інформаційної безпеки національної економіки в i-й період;

E_i – інтегральний показник економічної безпеки України в i-й період;

$n = 8$ – кількість спостережень.

Дані, необхідні для визначення коефіцієнтів цієї системи, наведено в таблиці 2.8.

Таблиця 2.8

Вихідні дані економетричної моделі взаємозалежності інформаційної безпеки національної економіки та економічної безпеки

Роки	E	I	E_I	I^2	E_{Ii}	$(I_i - E_{Ii})^2$	$(E_i - \overline{E})^2$
2013	47	53,20	2500,34	2830,10	53,63798656	44,06286562	0,0625
2014	45	54,70	2461,57	2992,27	54,03264443	81,58866537	2025
2015	44	53,34	2347,11	2845,52	53,67597501	93,62449231	1936
2016	48	57,34	2752,27	3287,76	54,72521394	45,22850256	2304
2017	48	56,04	2689,72	3140,00	54,38298293	40,7424711	2304
2018	49	57,83	2833,69	3344,35	54,85424772	34,27221633	2401
2019	49	55,36	2712,42	3064,23	54,20435214	27,0852812	2401
2020	48	56,95	2733,65	3243,42	54,62333183	43,86852456	2304
Σ	378,00	444,76	21030,76	24747,65	156,4607346	49079,64613	142884

Джерело: складено автором

Отже, система нормальних рівнянь має вигляд

$$\begin{cases} 24747{,}65a + 444{,}76b = 21030{,}76 \\ 444{,}76a + 8b = 378 \end{cases}$$

Її розв'язок a = 0,8462, b= -350,182.

Отже, рівняння регресії має вигляд E = 0,8462I – 350,182

Аналізуючи коефіцієнти рівняння регресії, можна зробити висновок про те, що підвищення інформаційної безпеки на 1% сприяє зростанню рівня економічної безпеки країни на 0,85%.

Для оцінки адекватності прийнятої економетричної моделі експериментальним даним використаємо критерій Фішера. Для визначення розрахункового значення критерію Фішера обчислюємо значення $(E_i - E_{Ii})^2$, $(E - \overline{E})^2$, де E_i – значення змінної E в i-тий рік, E_{Ii} – значення змінної E в i-тий рік, визначене із рівняння регресії $E_i = aI_i + b$, $\overline{E}$ – середнє значення змінної E (див. табл. 2.8).

Визначимо коефіцієнт детермінації та індекс кореляції:

$$R^2 = 1 - \frac{\sum (E_i - E_{Ii})^2}{\sum (E_i - \overline{E})^2} = 0{,}67$$
$$R = \sqrt{R^2} = 0{,}8 \qquad (2.9)$$

Фактичне значення критерію Фішера становитиме:

$$F = \frac{R^2}{1 - R^2}(n - 2) = 12{,}5 \qquad (2.10)$$

Табличне значення F-критерію для ймовірності p = 0,95 і числа ступенів вільності $k_1 = m = 1$, $k_2 = n–m–1$ дорівнює 4,96. Оскільки фактичне значення перевищує табличне, то модель є адекватною [162]. Деталізовані результати кореляційно-регресійного аналізу взаємозалежності інформаційної безпеки національної економіки та економічної безпеки України наведено в Додатку Ж. Графічна інтерпретація результатів дослідження взаємозв'язку рівнів економічної та інформаційної безпеки України представлена на діаграмі розсіювання (рис. 2.24).

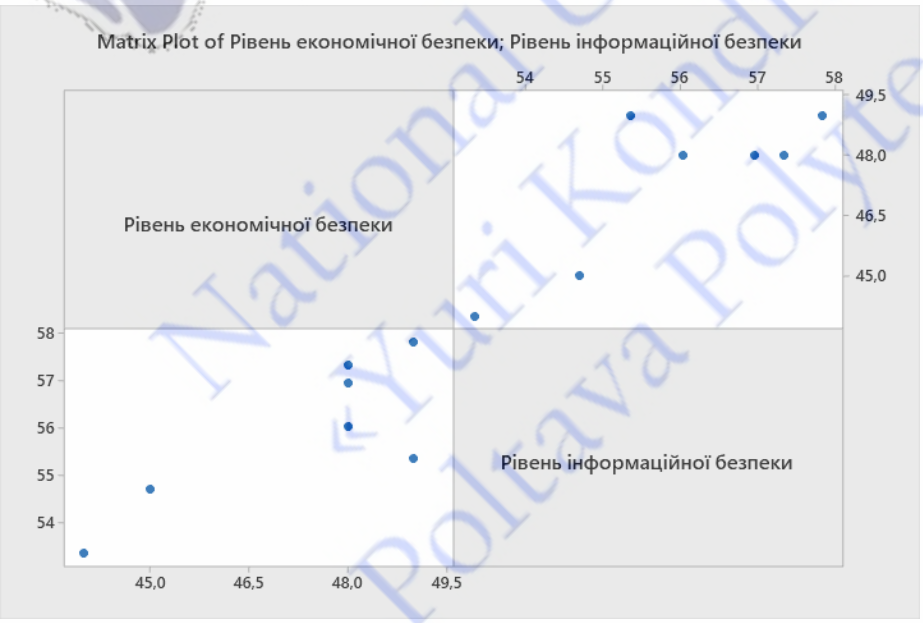

Рис. 2.24. Взаємозв'язок інформаційної безпеки національної економіки та економічної безпеки України

Джерело: побудовано автором

Отриманий результат підтверджує наявність прямої кореляції між інформаційною безпекою національної економіки та економічною безпекою: при зростанні рівня інформаційної безпеки рівень економічної безпеки також буде підвищуватися. Водночас, розкид рівня економічної безпеки є достатньо значним по відношенню до певного значення інформаційної безпеки національної економіки. Тому кореляція є середньою, оскільки на рівень інтегрального показника економічної безпеки впливають й інші фактори, виражені її субіндексами [162].

Таким чином, інформаційна та економічна безпека мають потенціал в аспекті забезпечення синергетичних ефектів. Забезпечення формування інформаційного середовища національної економіки на засадах безпекоорієнтованості є базисом реалізації національних інтересів, що створює нові можливості для зміцнення безпеки економіки України в умовах посилення впливу внутрішніх і зовнішніх дестабілізуючих чинників, та вимагає провадження інтегрованої державної політики.

Загрози інформаційній безпеці виступають деструктивними факторами розвитку національної економіки. Тому наступним етапом дослідження є визначення впливу інформаційної безпеки на рівень розвитку національної економіки. Рівень економічного розвитку країн визначається обсягом валового національного продукту (ВНП), або обсягом валового внутрішнього продукту (ВВП), або рівнем ВВП на душу населення.

У дослідженні рівень розвитку національної економіки виражено рівнем ВВП в розрахунку на тисячу осіб. Чисельність населення взято в середньому за рік. Вводиться гіпотеза, що між фактором I (рівнем інформаційної безпеки) та показником E (рівнем розвитку національної економіки) існує лінійна стохастична залежність. Алгоритм визначення впливу ґрунтується на формулах 2.8 – 2.10, а вихідні дані для розрахунку представлені в таблиці 2.9.

Таблиця 2.9

Вихідні дані економетричної моделі впливу інформаційної безпеки на рівень розвитку національної економіки

Роки	E	I	EI	I^2	Eіі	$(I_i - E_{ii})^2$	$(E_i - \overline{E})^2$
2013	31,9887	53,2	1701,80	2830,24	53,63832	468,7060461	1084,18239
2014	35,83	54,70	1960,18	2992,27	54,03264443	331,190659	1284,075556
2015	46,2102	53,34	2465,01	2845,52	53,67597501	55,73779644	2135,382584
2016	55,8535	57,34	3202,58	3287,76	54,72521394	1,273029429	3119,613462
2017	70,2243	56,04	3935,07	3140,00	54,38298293	250,9473265	4931,45231
2018	84,192	57,83	4868,85	3344,35	54,85424772	860,703709	7088,292864
2019	94,5898	55,36	5236,06	3064,23	54,20435214	1630,984399	8947,230264
2020	100,4325	56,95	5719,73	3243,42	54,62333183	2098,479888	10086,68706
2021	131,9072	58,69	7741,63	3444,52	55,079994	5902,419582	17399,50941
Σ	651,23	503,45	36830,92	28192,30	489,22	11600,44	56076,43

Джерело: складено автором

Отже, система нормальних рівнянь має вигляд

$$\begin{cases} 28192{,}30a + 503{,}45b = 36830{,}92 \\ 503{,}45a + 9b = 651{,}23 \end{cases}$$

Її розв'язок a = 1,0779, b= 18,467.

Отже, рівняння регресії має вигляд E = 1,0779I + 18467.

Аналізуючи коефіцієнти рівняння регресії, можна зробити висновок про те, що підвищення інформаційної безпеки на 1 сприяє зростанню рівня розвитку національної економіки країни на 1,08.

На основі використання критерію Фішера доведено адекватність прийнятої економетричної моделі. Результати кореляційно-регресійного аналізу взаємозалежності введених в модель показників наведено в Додатку И. Графічна інтерпретація результатів дослідження впливу інформаційної безпеки національної економіки на рівень розвитку економіки України представлена на рисунку 2.25.

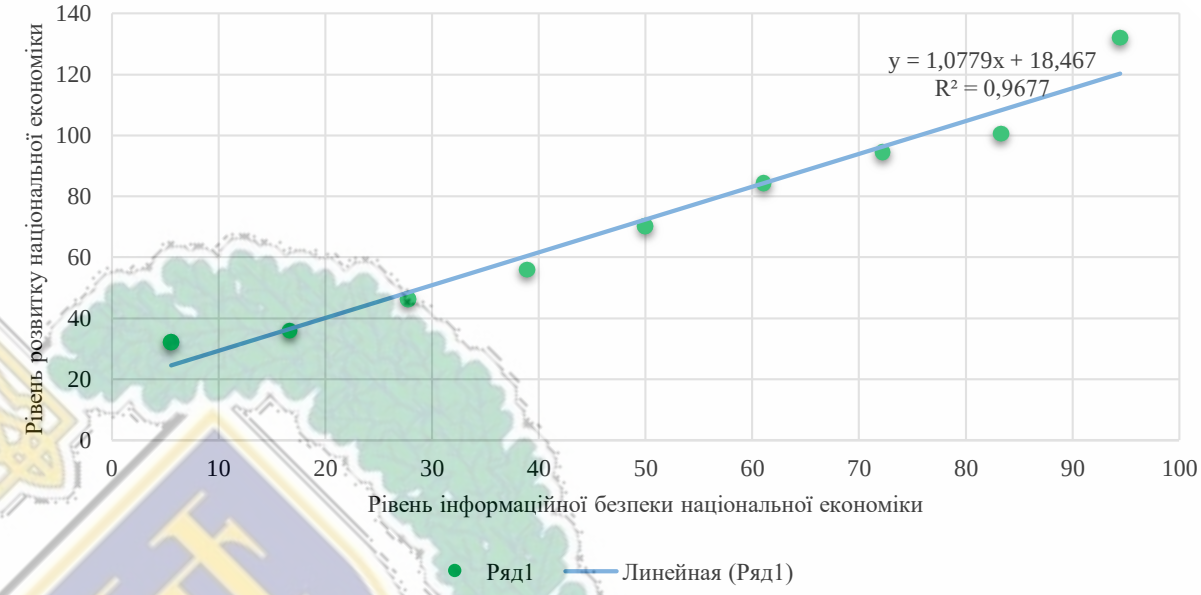

Рис. 2.25. Вплив інформаційної безпеки національної економіки на рівень розвитку економіки України

Джерело: побудовано автором

Отриманий результат підтверджує наявність прямої кореляції між інформаційною безпекою та рівнем розвитку національної економіки: при зростанні рівня інформаційної безпеки рівень розвитку національної економіки також буде підвищуватися.

З урахуванням результатів проведеного інтегрального оцінювання інформаційної безпеки національної економіки доцільно відмітити необхідність затвердження на державному рівні Методики розрахунку рівня інформаційної безпеки з чітким переліком індикаторів та обґрунтованими пороговими значеннями. Проведене оцінювання рівня інформаційної безпеки на основі показників, які лежать в основі світових рейтингів, може стати підґрунтям для вказаної методики. Зокрема, субіндексами інтегрального показника інформаційної безпеки доцільно визначити: розробленість державної політики у сфері інформаційної безпеки; моніторинг та аналіз загроз інформаційному середовищу; освіта та підвищення кваліфікації у сфері захисту інформаційного, в тому числі кіберпростору; внесок у глобальну інформаційну безпеку, захист цифрових сервісів та основних послуг у кіберпросторі, послуг електронної

ідентифікації, захист персональних даних; боротьба з кіберзлочинністю та військові кібероперації.

Встановлений у процесі дослідження взаємозв'язок між інформаційною безпекою національної економіки та економічною безпекою України, обґрунтований вплив інформаційної безпеки на рівень розвитку національної економіки підтверджує необхідність провадження інтегрованої державної політики. Перспективним залишається питанням обґрунтування методів захисту інформації, зокрема на об'єктах критичної економічної інфраструктури.

Висновки до розділу 2

1. На основі проведеного компаративного аналізу рівня цифровізації економіки України з країнами Європейського Союзу встановлено максимальне наближення показника національної економіки до середнього по ЄС. У сфері фінансових послуг, послуг зв'язку, логістики національні суб'єкти господарювання застосовують цифрові технології на рівні зі світовими конкурентами. Проведене за оптимістичним та песимістичним сценаріями прогнозування динаміки зміни частки ІТ-сектору у ВВП України, яка засвідчує обсяги цифрової економіки, дозволяє обґрунтовано констатувати посилення процесів цифрової трансформації.

2. Доведено, що в кризових умовах високу стійкість демонструє саме цифровий сектор. З початку повномасштабного вторгнення рф українська ІТ-галузь стала однією з найстабільніших сфер національної економіки – це єдина галузь, обсяг експорту якої виріс у 2022 році. Відповідно цифрову трансформацію національної економіка правомірно вважати детермінантою стійкості, стабільності та адаптивності.

3. Обґрунтовано, що поряд з традиційними загрозами інформаційній безпеці національної економіки процеси цифровізації стали джерелом виникнення ряду додаткових загроз інформаційним ресурсам і технологіям в

економіці, методи діагностики і протидії яким поки що не відпрацьовані в повній мірі. Це вимагає інтеграції безпекових аспектів економічних та інформаційних процесів.

4. Розроблено методику комплексного оцінювання рівня інформаційної безпеки національної економіки, яка передбачає розрахунок та визначення конструктивної валідності інтегрального індексу інформаційної безпеки національної економіки на основі системи індикаторів (у тому числі, індикаторів цифрової, інституційної, кіберспроможності національної економіки та характеризують рівень і міру її відповідності домінуючим світовим тенденціям розвитку цифрової економіки). За аналізований період рівень інформаційної безпеки національної економіки знаходився на незадовільному рівні, але не виходячи з меж безпечної зони. Для прогнозування динаміки інтегрального показника використано модель поліноміальної апроксимації, що підтвердила позитивні зрушення в напрямку підвищення рівня безпеки інформаційного середовища в Україні.

5. На основі використання економетричного аналітичного інструментарію встановлено залежність між рівнем інформаційної безпеки національної економіки та економічної безпеки України, вплив інформаційної безпеки на рівень розвитку національної економіки. Обґрунтоване доведення діалектичного взаємозв'язку між показниками актуалізує необхідність усунення загроз та деструктивних факторів розвитку національної економіки на основі формування безпекоорієнтованого інформаційного середовища.

Основні результати дослідження відображені у наукових працях автора [81, 109, 118, 122, 125, 146, 162].

РОЗДІЛ 3
НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ЕКОНОМІКИ УКРАЇНИ

3.1. Концепти забезпечення інформаційної безпеки національної економіки в умовах цифровізації

У сучасних умовах цифровізація стає головною глобальною тенденцією економічного розвитку, докорінно змінюючи структуру національної економіки і перетворюючи на якісно новий стан, у якому домінують цифрові технології. Як зазначалося у попередніх розділах, це пов'язано з тим, що трансформація економічних відносин на цифрових засадах визначає низку суттєвих переваг для економічної діяльності: оптимізація витрат за рахунок економії на просуванні товарів і послуг; прискорення бізнес-процесів завдяки скороченню часу, що витрачається на комунікацію; скорочення часу реакції на зміни ринку; автоматичне опрацювання та аналіз даних; скорочення операційних витрат; постійне створення інноваційних продуктів; максимальна адаптація послуг, що надаються, до потреб і вимог споживачів.

Саме тому розвиток національної економіки все більше ґрунтується на технологіях та знаннях, що робить їх основною продуктивною силою, а цифрові дані та новітні технологічні досягнення в галузі ІКТ стають ключовим фактором виробництва.

В Україні в умовах розвитку Індустрії 4.0 та впровадження принципів Індустрії 5.0 (екологічності, стійкості та адаптивності) процес цифровізації реального сектору економіки активно продовжується. Інноваційні технології, зокрема хмарні технології, сучасні способи отримання та аналізу великих масивів даних (Big Data), робототехніка, криптовалюта та технологія блокчейн, краудсорсинг, штучний інтелект тощо змінюють сектори національної

економіки. Структура національної економіки в умовах цифрової трансформації та інформаційного суспільства характеризується набуттям некласичних, нестійких і змінюваних форм. Процеси цифровізації руйнують межі між біологічними, фізичними та цифровими сферами, сприяють виникненню принципово нових підходів до провадження діяльності суб'єктами національної економіки.

Становлення Індустрії 4.0 й прискорена цифровізація національної економіки України, виступаючи драйверами економічних перетворень, зумовили появу специфічних деструктивних феноменів (інформаційних війн, інформаційного тероризму, масштабних відкритих та прихованих кібератак), сила впливу і масштаби яких посилилися в умовах повномасштабної війни.

Архітектоніку національної економіки в умовах цифрової трансформації з урахуванням можливостей щодо створення валової доданої вартості, отримання вигід економічними суб'єктами та можливих ризиків і загроз, спричинених процесами цифровізації, представлено на рисунку 3.1.

У відповідності до логіки, конструкції та контенту представленої авторської моделі національної економіки, правомірно стверджувати, що в умовах цифровізації можливості розвитку національної економіки, стійкість до модифікованих ризиків і загроз безпосередньо залежать від захищеності інформаційного середовища національної економіки, тобто інформаційної безпеки.

Отже, активне впровадження цифрових технологій Індустрії 4.0, поширення принципів Індустрії 5.0 сприяли виникненню принципово нової форми організації та функціонування національної економіки. Окреслені ризики і загрози національній економіці в умовах цифрової трансформації робить релевантною проблему захисту інформаційного середовища економічних суб'єктів усіх рівнів. З огляду на наведену аргументацію постає необхідною наукова інтерпретація концептів забезпечення інформаційної безпеки національної економіки в умовах цифровізації.

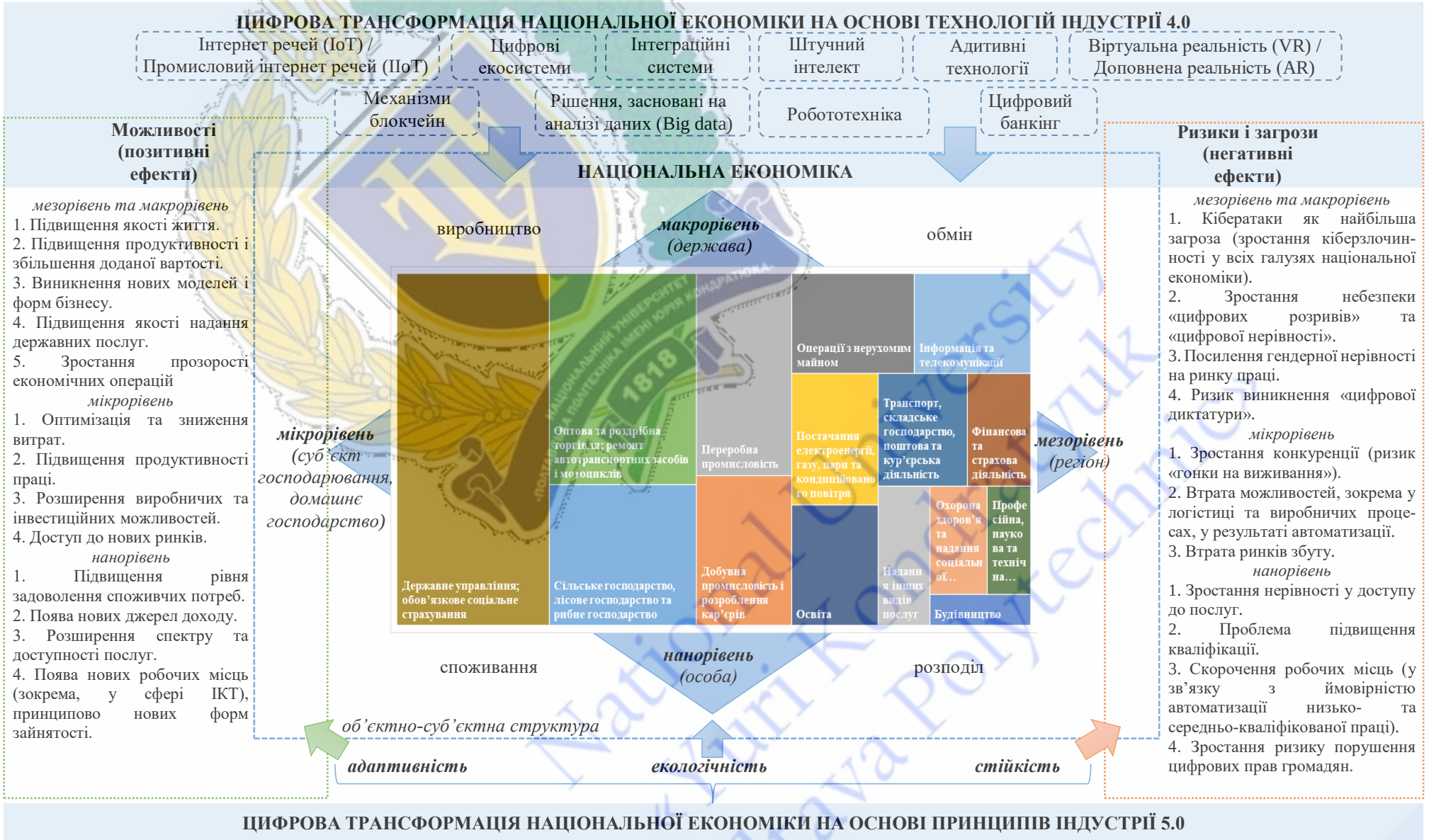

Рис. 3.1. Архітектоніка національної економіки в умовах цифрової трансформації (авторська розробка)

Проблема забезпечення безпеки інформаційного середовища є пріоритетною на національному і міжнародному рівні в останні десятиліття. Трансформація світової економіки у цифровий формат, її віртуалізація, зміна форм організації економічних відносин спричинили появу нових викликів. Зловживання інформацією може призвести до технологічних аварій, воєнних конфліктів, дезорганізувати державне управління, економічну систему та спричинити багато інших небезпек. Тому інформаційну безпеку правомірно визначити невід'ємною складовою кожної сфери національної безпеки, яка спрямована на захист національних інтересів, в тому числі економічних, від деструктивного впливу потенційних і реалізованих інформаційних загроз, мінімізацію збитків через недостовірну та неповну інформацію, незаконне заволодіння інформацією та її використання.

В умовах посилення впливу внутрішніх і зовнішніх дестабілізуючих чинників, реалізації безпрецедентних загроз усім складовим національної безпеки, спричинених військовою агресією російської федерації забезпечення інформаційної безпеки національної економіки, що передбачає функціонування інформаційного середовища економіки України на засадах безпекоорієнтованості, є базисом реалізації національних інтересів, що створює нові можливості для зміцнення безпеки національної економіки.

Існуючі підходи до забезпечення безпеки національної економіки, в тому числі інформаційної, базуються на використанні відповідного інструментарію, кожному з підходів властиві свої переваги та обмеження, втім жоден не визнаний досконалішим порівняно з іншими. Наявність кількох підходів до забезпечення безпеки національної економіки є виявом контекстуальності постмодерністської методології економічної безпекології, для якої характерні гнучкі дослідницькі стратегії. Головним є виконання такої вимоги: підходи різними шляхами, з використанням різних інструментів мають надавати однаковий за змістом (хоча різний за формою) опис процесу забезпечення безпеки національної економіки.

Зміст кожного з підходів до забезпечення безпеки національної економіки розкривається за допомогою його концептів. Концепт підходу розглядається як

елемент структурованого знання про дії з забезпечення безпеки, який відображає певний фрагмент (аспект) забезпечення безпеки і сприяє категоризації цього знання. Концепти підходу об'єктивізують його онтологічну складову, пояснюють його процесуальність і дозволяють встановити предметно-логічні зв'язки різних ракурсів ідеї.

Концепти будь-якого підходу до забезпечення інформаційної безпеки національної економіки мають бути операціоналізовані. Операціоналізація концептів підходу «переводить» його принципи та теоретичні конструкції в практичну площину через формування сукупності прийомів, процедур та алгоритмів, і в такий спосіб регламентує дії дослідника.

Таким чином, під концепцією забезпечення інформаційної безпеки національної економіки мається на увазі система концептів відносно методологічного підходу, цілей, методів, принципів, технологій забезпечення інформаційної безпеки держави, здійснення практичних завдань і застосування інструментів на рівні країни в цілому, регіонів та окремих суб'єктів господарювання, що мають забезпечити інформаційну безпеку національної економіки. При цьому концепти базуються на положеннях нової парадигми використання можливостей, які пов'язані з розвитком інформаційних технологій та попередження й запобігання новим загрозам інформаційній безпеці національної економіки шляхом захисту інформації, забезпечення цілісності, достовірності, доступності державних інформаційних ресурсів, інформації з обмеженим доступом, в тому числі тієї, що циркулює на об'єктах економічної інформаційної інфраструктури та визначає подальший безпечний розвиток держави шляхом створення системи безпеки комп'ютерних систем обробки економічних даних (КСОЕД) та враховують зовнішні і внутрішні загрози, реалізовані внаслідок військової агресії російської федерації.

В основу авторської концепції забезпечення інформаційної безпеки національної економіки правомірно покладено синергетичний підхід, з урахуванням того, що система інформаційної безпеки економіки України є

складною, нерівноважною, нелійнійною, з елементами самоорганізації системою [165].

Синергетичний підхід у загальному розумінні передбачає загальний кооперативний ефект, який досягається за рахунок взаємодії різних, зазвичай складних систем, що складаються з великої кількості елементів, між якими існує значна кількість взаємозв'язків. Якщо в простих системах існує єдиний причинно-наслідковий зв'язок, то в складних системах причини часто відокремлені від наслідків у часі та просторі [166, с. 28–42]. Поведінка складних систем має низку властивостей, яких немає у простих систем.

Синергетичний підхід застосовується науковцями у сфері безпекології. Зокрема, Л. О. Корчевська окреслюючи принципи економічної безпеки суб'єктів господарювання поділяє їх на п'ять груп за цільовим, функціональним, структурним, процесним та системним напрямами, що дає змогу сформувати теоретичне підґрунтя для синергетичного управління економічною безпекою [167].

Синергетика вивчає стан складних систем у сфері нестійкої рівноваги, точніше, динаміку їхньої самоорганізації. Синергетика (або синергізм) в економічній науці – це процес самоорганізації економічної системи з утворенням в її підсистемах стійких коливань певних змінних, що змінюють траєкторію і якість її розвитку [168]. Цей методологічний підхід означає визнання того, що економіка як синергетична система здатна до незворотного якісного розвитку, що забезпечується системним синтезом технологічних, економічних, організаційних, екологічних, соціальних, управлінських чинників із врахуванням автохвильових й автокаталітичних явищ [169].

Таким чином, синергетичний підхід до забезпечення інформаційної безпеки національної економіки являє собою сукупність принципів, що ґрунтуються на розгляді інформаційної безпеки національної економіки як складної систем, здатної до самоорганізації [170].

Основними принципами синергетичного підходу для забезпечення інформаційної безпеки національної економіки є наступні:

– об’єктами застосування підходу є складні відкриті нелінійні системи;

– передумовою самоорганізації системи є її нестійкий стан, що передбачає можливість коливань (флуктуацій);

– наявні альтернативні варіанти розвитку системи, що визначаються в точках вибору стратегія (траєкторія) подальшого розвитку (точки біфуркації);

– майбутній стан системи (атрактор) притягує, змінює, формує, організовує поточний стан системи і відіграє роль мети [171].

Враховуючи наукові напрацювання щодо методології синергетичного підходу основними категоріями синергетики правомірно виділити наступні:

– відкритість – наявність постійної взаємодії із зовнішнім середовищем, що передбачає, у тому числі, обмін інформацією;

– нелінійність – наявність динамічних процесів, різних варіантів реагування на ризики і загрози зовнішнього середовища;

– нерівноважність – характеризує відсутність рівноважного стану;

– самоорганізація – здатність системи до оптимального функціонування, самостійної відбудови, відновлення та якісних змін;

– флуктуація – випадкове відхилення основних показників від середнього значення, що здатне привести до утворення нової структури і системної якості;

– біфуркація – наявність різних напрямів розвитку відкритої нелінійної системи;

– атрактор – мета, ціль, стійкий стан системи, який є бажаним [168–172].

Враховуючи принципові положення синергетичної парадигми забезпечення інформаційної безпеки національної економіки має ґрунтуватися на її сприйнятті як самоорганізованої системи, зміна якої відбувається під впливом як внутрішніх механізмів, так і зовнішніх детермінант. Забезпечення інформаційної безпеки національної економіки передбачає досягнення захищеності та стійкості інформаційного середовища національної економіки в умовах деструктивних феноменів, тобто формування безпекоорієнтованого інформаційного середовища.

Таким чином, концепти синергетичного підходу до забезпечення інформаційної безпеки національної економіки полягають у наступному.

1. Захист національних економічних інтересів є першочерговим в умовах військової агресії російської федерації, а також поглиблення процесів глобалізації, євроінтеграції та зростання рівня відкритості економіки України. В умовах цифровізації виникають не лише нові виклики та загрози, але й невичерпні можливості, пов'язані з розвитком IT-технологій, які необхідно всебічно використовувати у процесі забезпечення інформаційної безпеки національної економіки.

2. Процеси цифровізації обумовлюють трансформацію структури національних економік. Базовими передумовами впровадження нових підходів до розвитку національної економіки України є такі ключові умови й чинники:

– цифрова трансформація є стратегічним напрямом підвищення стійкості національної економіки в умовах воєнного стану;

– трансформація факторів виробництва в цифрову форму під впливом активного розвитку інформаційної економіки: основними факторами виробництва стають інформація та інформаційні технології, а володіння інформаційними ресурсами спряє якісній зміні економічної системи, характеру економічних відносин між економічними суб'єктами;

– структурні зміни на мікро- та макроекономічному рівнях (створення підприємств у цифровому просторі без наявності матеріальних активів; формування інформаційної індустрії);

– технологічні інновації, роботизація, новітні інформаційні технології зробили доступними ряд послуг, покращили якість життя суспільства та спричинили кардинальну структурну зміну економіки;

– поглиблення тенденцій глобалізації економіки, що відбувається у світі та, зокрема, країнах Європейського Союзу та призводить до підвищення вимог до фінансової стійкості суб'єктів господарювання, зростання конкуренції на вітчизняному та світовому ринках;

– зростання ролі та значення інновацій у господарській діяльності, що проявляються у появі принципово нових продуктів, тенденції мінімізації «живого» спілкування на тлі поступового перенесення значної частини операцій у віртуальний простір [170; 173, с. 36–44].

3. В процесі визначення напрямів забезпечення інформаційної безпеки національної економіки необхідно враховувати особливості функціонування економічної системи України в умовах воєнного стану.

В умовах ведення інформаційних і гібридних війн формування інформаційної безпеки національної економіки є необхідною умовою захисту національних економічних інтересів, забезпечення захищеності державних інформаційних ресурсів, інформації з обмеженим доступом, в тому числі тієї, що циркулює на об'єктах економічної інформаційної інфраструктури і є базисом національної безпеки країни [162, 174]. Світовий досвід свідчить про те, що країна, яка прагне до отримання максимальної віддачі від перетворень в інформаційно-комунікаційній сфері, повинна максимально приділяти увагу питанням інформаційної безпеки.

В Україні цифровізацією динамічно охоплюється освіта та управління, сфера послуг і торгівля, фінансовий сектор, освіту та управління, і позитивні результати цих процесів для бізнесу і держави набувають особливої значущості. Переваги цифрової економіки очевидні: інклюзивність, динамічність, зниження вартості платежів (в он-лайн режимі вартість послуг є нижчою), відкриття нових джерел доходу тощо. Окрім цього, у підприємств з'являється можливість вийти на глобальний ринок та підвищити рівень доступності до товарів і послуг у будь-якій країні. За необхідності будь-який інноваційний продукт може бути модифікований під додаткові потреби замовника і в стислі терміни, навіть за умови просторової віддаленості об'єктів виробничої системи [175].

При цьому вплив цифровізації на перспективи розвитку національної економіки є дуальним: водночас із виникненням нових можливостей загострюються «традиційні» і формується низка нових ризиків, пов'язаних, в

першу чергу, з інформаційною безпекою національної економіки, основними серед них є такі:

– ризик кіберзагроз, пов'язаний з проблемою захисту персональних даних;

– «цифрове рабство» (можливість використання даних про мільйони людей для управління їх поведінкою);

– «цифровий розрив», який пов'язаний з рівнем і умовами доступу до цифрового середовища в одній країні або в різних країнах [170].

4. При розробці механізмів та інструментів формування безпекоорієнтованого інформаційного середовища національної економіки як основи її інформаційної безпеки доцільно використовувати економіко-математичні методи, адекватні особливостям функціонування об'єкта дослідження, що характеризуються рядом властивостей: наявність взаємозв'язку й динаміки, різновекторних інтересів економічних суб'єктів, нестаціонарність і багатоаспектність процесів, в основу яких покладено принципи: самоорганізації, рефлексії та обмеженої раціональності.

Водночас, система принципів забезпечення інформаційної безпеки національної економіки має включати також загальносистемні принципи, що дозволить синтезувати різні методи та інструменти, а саме: принцип системності (врахування усіх факторів, здатних вплинути на рівень інформаційної безпеки національної економіки), принцип синергізму (передбачає врахування міжсистемної взаємодії між елементами системи інформаційної безпеки національної економіки); принцип потенційної з'єднуваності (полягає в наявності можливості формування тимчасових цілісностей самодостатніх систем у системний комплекс внаслідок перехрещення інтересів економічних суб'єктів); принципи, що сприяють цифровій трансформації економічної системи (принцип достатності та адекватності відповідної законодавчої бази, принцип наявності цифрової інформаційно-комунікативної інфраструктури); принцип компромісу (узгодженість економічних інтересів суб'єктів усіх рівнів із зовнішнім середовищем); принцип суб'єктності (сприйняття зовнішнього середовища та значення інформаційної безпеки через призму різновекторних

інтересів економічних суб'єктів), принцип економічної доцільності (ефект від заходів забезпечення інформаційної безпеки національної економіки не повинен перевищувати витрати на їх реалізацію) [170, 176, 177].

5. Як методологічний базис для розробки векторів та орієнтирів забезпечення інформаційної безпеки національної економіки слід використовувати синергетичний підхід. В основі цього підходу лежать положення концепції синергетики, яка свідчить, що оптимального стану можливо досягнути за умови нерівноважності системи і наявності процесів самоорганізації [178, с. 112]. Стан нерівноваги правомірно визначити як момент переходу в якісно новий стан, за якого інформаційна безпека національної економіки здатна досягнути більш високого рівня.

Синергетичний підхід передбачає забезпечення інформаційної безпеки національної економіки відповідно з урахуванням глобальних цифрових трендів. Мова йде про те, що у періоди нестабільності можуть виникати паралельні структури, які несуть в собі інформаційні та кіберзагрози. За певних обставин вони можуть характеризуватися стійким характером і спричинити вихід системи на неоптимальну траєкторію розвитку.

В цих умовах, з метою забезпечення інформаційної безпеки національної економіки, основу регуляторних процесів у країні має становити оптимальне поєднання ринкових регуляторів та економічно обґрунтованої державної політики. Мета цього управління полягає у тому, щоб активізувати наявні внутрішні резерви шляхом незначного резонансного впливу та зміцнити інформаційну безпеку на всіх рівнях національної економіки [170].

Використання синергетичного підходу до формування безпекоорієнтованого інформаційного середовища національної економіки дозволить більш повно реалізувати можливості державної політики.

6. Забезпечення підтримки національної економіки, її стабілізації в умовах воєнного стану, а також розвитку та підвищення конкурентоспроможності у післявоєнний період передбачає, зокрема, стимулювання розвитку е-освіти, е-медицини, е-демократії, е-торгівлі, е-платежів, а також активне впровадження

новітніх інформаційних технологій та, водночас, ефективних систем захисту інформації у сфері безпеки і правопорядку. Натомість низький рівень покриття України цифровою інфраструктурою та її вразливість до кіберризиків (шахрайських дій і несанкціонованого втручання) вимагає законодавчого потребує надійних систем захисту.

7. Інформаційну безпеку національної економіки правомірно розглядати з точки зору системного підходу. Система інформаційної безпеки національної економіки має ґрунтуватися на дієвому інституційному забезпеченні та бути спрямованою на захист національних економічних інтересів [34]. Базуючись на ефективному інституційно-організаційному та інституційно-правовому забезпеченні, система інформаційної безпеки національної економіки повинна забезпечувати взаємодію складових і суб'єктів у процесі вирішення завдань щодо зміцнення безпеки національної економіки.

8. Формування безпекоорієнтованого інформаційного середовища національної економіки як базису інформаційної безпеки вимагає наявності відповідного наукового, аналітичного, інституційного та фінансового забезпечення, що має забезпечувати реалізацію заходів адміністративного й економічного характеру, спрямованих на забезпечення національних економічних інтересів з урахуванням чинного законодавства України. Механізм формування безпекоорієнтованого інформаційного середовища має передбачати заходи превентивного реагування на виникнення відхилень від ключових параметрів / індикаторів, що характеризують виконання завдань реалізації національних економічних інтересів, тобто, бути адаптивним до змін зовнішнього середовища, що має забезпечити конкурентоспроможність національної економіки та її стійкість до ризиків і загроз [170].

9. Теоретичні передумови формування безпекоорієнтованого інформаційного середовища національної економіки мають ґрунтуватися на основі міждисциплінарного підходу з урахуванням ключових положень концепцій та теорій безпекології (концепція забезпечення економічної безпеки держави); теорій державного регулювання (неокласична теорія, інституційна

економічна теорія, концепція асиметричності інформації, несприятливого вибору і ризику опортуністичної поведінки); сучасних економічних концепцій та теорій (еволюційна теорія, теорія поведінкової економіки); концепцій менеджменту та маркетингу (концепція стратегічного менеджменту, концепція менеджменту як економічних стосунків, концепція синергії, концепція ситуаційного управління, стратегія активної адаптації до зовнішнього середовища, стратегія маркетингу партнерських відносин), інших концепції та теорій.

Таким чином, можна зробити висновок про те, що запропоновані концепти синергетичного підходу до забезпечення інформаційної безпеки національної економіки кардинально відрізняються від існуючих по розглянутих структурних характеристиках та можуть бути основою для побудови концептуальної моделі механізму формування безпекоорієнтованого інформаційного середовища як основи інформаційної безпеки національної економіки (рис. 3.2).

Синергетичний підхід до забезпечення інформаційної безпеки національної економіки правомірно визначити методологічною орієнтацією у практичній діяльності, яка ґрунтується на використанні сукупності ідей, понять і методів дослідження та управління складною, відкритою, нерівноважною, нелінійною, з елементами самоорганізації системою інформаційної безпеки економіки України [170]. В основі формування безпекоорієнтованого інформаційного середовища національної економіки є максимальний захист та задоволення інтересів держави, суб’єктів господарювання і громадян. На забезпечення інтересів зацікавлених груп мають бути спрямовані зусилля суб’єктів забезпечення інформаційної безпеки національної економіки.

Наведені ключові концептуальні положення стосуються основних аспектів формування безпекоорієнтованого інформаційного середовища та мають стати теоретичним базисом для подальшої розробки методології забезпечення інформаційної безпеки національної економіки.

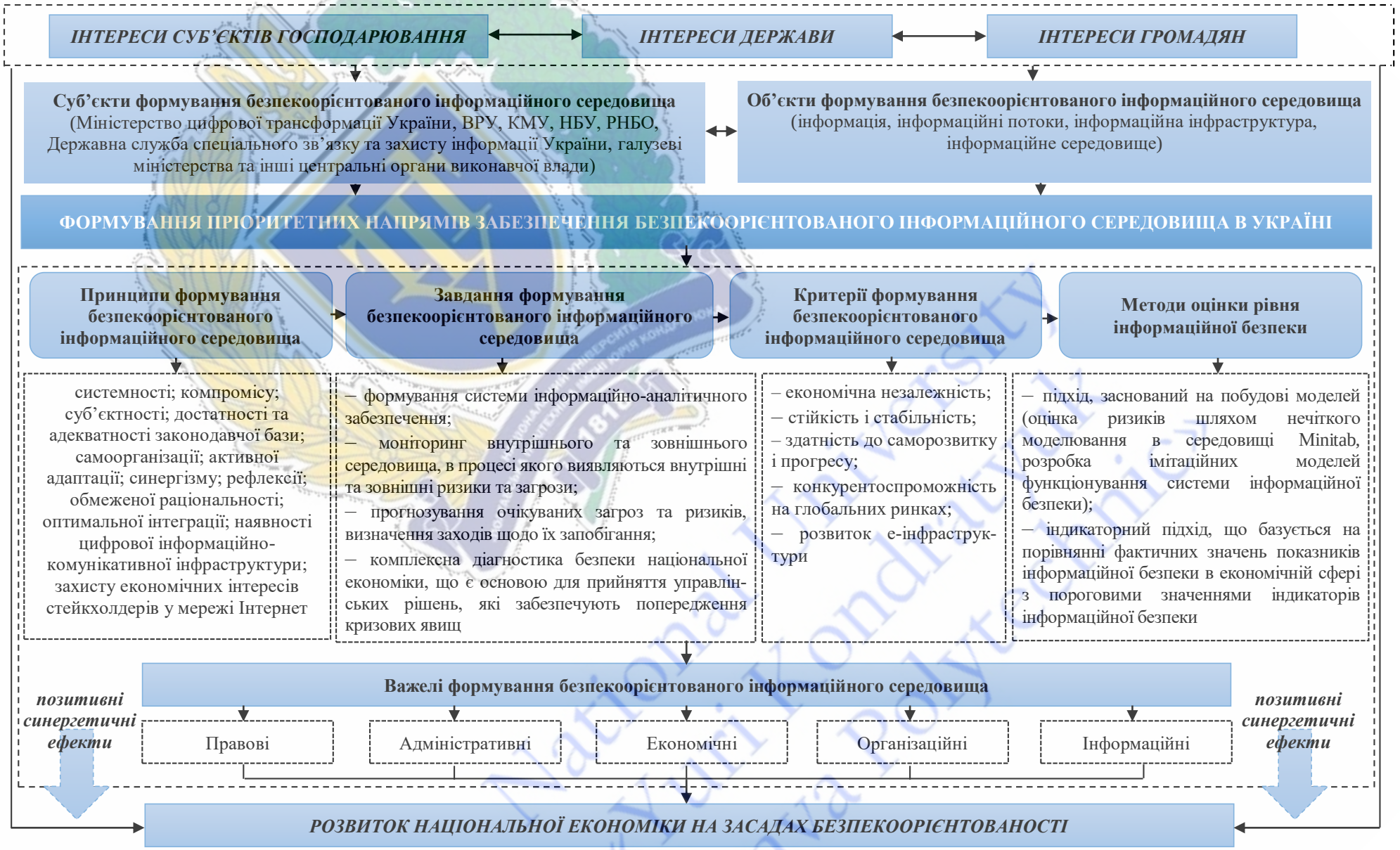

Рис. 3.2. Концептуальна модель механізму формування безпекоорієнтованого інформаційного середовища в Україні

Джерело: розроблено автором

Узагальнюючи вищезазначене, правомірно відмітити, що основними положеннями пропонованого синергетичного підходу до формування безпекоорієнтованого інформаційного середовища в Україні є наступні.

1. Процеси самоорганізації в системі інформаційної безпеки національної економіки характеризують невизначеність та нестабільність як національного, так і світового ринку в цілому. Застосування синергетичного підходу дає можливість визначити позитивні та негативні наслідки системної взаємодії різних чинників, серед яких можливо виділити організаційно-економічні, інституційні, політичні, управлінські, інноваційні, психологічні, соціальні тощо.

2. Використання синергетичної парадигми, на противагу «класичним» підходам в управлінні, передбачає реалізацію цільового випливу на процеси самоорганізації в динамічних системах, якою є система інформаційної безпеки національної економіки. Отже, на сьогодні в процесі регулювання з боку держави виникає потреба використання підходів теорії управління, тобто формування такої системи інформаційної безпеки національної економіки, яка б генерувала позитивні синергетичні ефекти.

3. Заходи регулювання процесів формування безпекоорієнтованого інформаційного середовища мають включати елементи синергетичного підходу, що визначає процес управління не в досягненні локальної «стійкості» чи «стабільності», а у забезпеченні траєкторії розвитку, що відповідає глобальним тенденціям розвитку інформаційної економіки, у визначенні та формуванні вектору цього розвитку.

4. Відсутність можливості прогнозувати поведінку суб’єктів нерівноважних систем вимагає створення альтернативних методів прогнозування їх динаміки. При цьому, в умовах воєнного стану національна економіка характеризується нерівноважністю та нестабільністю, що обумовлює наявність значної кількості варіантів подальшого її розвитку. Отже, формування безпекоорієнтованого інформаційного середовища має враховувати синергетичну парадигму розвитку економіки України.

Окреслені концепти синергетичного підходу стали базисом для побудови концептуальної моделі механізму формування безпекоорієнтованого інформаційного середовища в Україні, реалізація якої дозволить досягнути позитивних синергетичних ефектів в процесі трансформації та розвитку національної економічної системи.

3.2. Компаративний аналіз систем інформаційної безпеки та модернізація структур захисту інформації в Україні

Залежність економічних суб'єктів від інформаційних систем та їх послуг спричиняє зростання їх уразливості до інформаційних загроз. Зростання взаємодії суспільних і приватних мереж, спільне використання інформаційних ресурсів спричиняють збільшення труднощів в управлінні доступом і забезпеченні гарантій послуг та безпеки інформаційно-комунікаційних систем і мереж. Цифровізація господарської діяльності створює умови для зростання випадків несанкціонованого використання комп'ютерних мереж і систем, тобто збільшення кіберзлочинності [179].

Загрози інформаційній та кібербезпеці змінили парадигму економічних відносин кілька десятиліть тому, оскільки здатні спричинити значні прямі і непрямі втрати. В умовах сьогодення першочерговою ціллю для кіберзлочинців є фінансові послуги, конфіденційні дані, транзакції, інформація про облікові записи клієнтів та приватні персональні дані. Забезпечення високого рівня інформаційної безпеки національної економіки ґрунтується на захищеності кожного економічного суб'єкта в інформаційному середовищі. Тому постає доволі суттєва проблема щодо визначення порядку формування вимог та виконання заходів із забезпечення кіберзахисту та інформаційної безпеки суб'єктів національної економіки.

У цьому аспекті питання впровадження ефективних систем захисту інформації є пріоритетним для суб'єктів національної економіки. Забезпечення інформаційної безпеки національної економіки полягає в можливості

своєчасного виявлення економічними суб'єктами каналів втрат інформації, потенційних загроз і рівня їх важливості, типів суб'єктів викрадення інформації, способів їх дій; оперативному реагуванні на реальні та потенційні загрози; забезпеченні відшкодування збитків; запобіганні економічному й промисловому шпіонажу.

За наявними оцінками експертів IT-сфери та проведеним аналізом публікацій і статей з відкритих джерел, типологія систем інформаційної безпеки та кібербезпеки суб'єктів світового ринку тримається в таємниці. При цьому відомо, що зазначені системи використовуються для перевірки безпеки власних комунікаційних систем і їх побудова доволі розгалужена і не однотипна з визначеними зв'язками між ними та об'єднаних єдиним керівництвом.

Проривні досягнення у штучному інтелекті, хмарних технологіях, інтернет-речах, продуктивності та природі обчислювальних засобів, можливостях зберігання обробки та передачі великих масивів даних та інформації (Big Data), засобах і технологіях їх реалізації вимагають принципово нових підходів до забезпечення інформаційної безпеки економічних суб'єктів. Можливості і вразливості сучасних інформаційно-комунікаційних та кібернетичних систем все більше залежать від зростання взаємозв'язків між ними в багатопараметричному, багатовимірному кіберпросторі та їх інформаційно-кібернетичного взаємопроникнення, взаємодії і взаємозалежності, тощо.

За цих умов трансформація поглядів на питання створення систем інформаційного захисту та, відповідно, розвиток їх структур та типологій в Україні відбувається під впливом розвитку технологій, змін у власному фінансовому безпековому середовищі, формах, способах та технологіях застосування засобів кібервпливу і нових досягнень в цьому [180].

В основі класичної типології систем захисту інформації лежить їх функціональне призначення (рис. 3.3).

Рис. 3.3. Типологія систем захисту інформації економічних суб'єктів за функціональним призначенням

Джерело: систематизовано автором на основі даних [180]

Системи захисту інформації можуть бути спрямовані на запобігання загроз, їх попередження, відновлення тощо. Водночас, постійна трансформація і поява нових модифікованих загроз інформаційній та кібербезпеці вимагає від суб'єктів національної економіки підвищувати ефективність та модернізувати існуючі систем захисту інформації.

В сучасних умовах економічні суб'єкти все більше наражаються на загрози безпеці завдяки широкому впровадженню фінансових онлайн-операцій і надання

послуг. Тому важливо забезпечити цілісність і конфіденційність інформації під час виконання будь-яких операцій у віртуальному середовищі.

Проведений аналіз діючих систем захисту інформації установ України (а саме, банківських та фінансових установ) засвідчує, засвідчує, що в цілому політика інформаційної та кібербезпеки проваджується всіма суб'єктами у відповідності до чинного законодавства України з урахуванням міжнародних стандартів з питань інформаційної безпеки та ґрунтується на положеннях Стратегії інформаційної безпеки, Стратегії кібербезпеки України, Закону України «Про основні засади забезпечення кібербезпеки України», Національних стандартів України з питань інформаційної безпеки (ДСТУ ISO/IEC 27000:2015, ДСТУ ISO/IEC 27001:2015, ДСТУ ISO/IEC 27002:2015), Постанови Правління Національного банку України «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» та ін.

Зазначеними вище нормативними документами та стандартами передбачені вимоги до мінімально необхідного пакету зі створення, впровадження, технічної підтримки та вдосконалення системи менеджменту інформаційної безпеки і кіберзахисту. При цьому, все більше організацій також усвідомлюють, що традиційних систем захисту інформації та ручних процедур вже недостатньо для виконання та підтримки політики інформаційної безпеки. В цьому контексті суб'єктам національної економіки України не забороняється нарощувати свої спроможності з питань інформаційної та кібербезпеки.

Сучасні структури систем захисту інформації та кібербезпеки мають відповідати міжнародним стандартам, стандартам Європейського Союзу та НАТО, передбачати застосування потужної лінійки інструментів, як на технологічному так і на програмному рівнях, використання розгалужених відповідних архітектур, методів захисту які спрямовані на упередження, виявлення та реагування на потенційні кіберзагрози.

Побудова систем захисту інформації в Україні має враховувати позитивний світовий досвід та ґрунтуватися на вимогах до інформаційної

безпеки, зазначених у міжнародно визнаних стандартах. Ці документи містять вимоги до систем захисту інформації (табл. 3.1), дотримання яких дозволяє забезпечити високий рівень інформаційної безпеки економічних суб'єктів.

Таблиця 3.1

Міжнародно визнані стандарти, що містять вимоги до побудови систем захисту інформації економічними суб'єктами

Стандарт безпеки	Зміст стандарту та вимоги до інформаційної безпеки
1	2
Payment Card Industry Data Security Standard (PCI-DSS), з англ. «стандарт безпеки індустрії платіжних карток» [181]	PCI-DSS визначає вимоги з захисту платіжних даних, які об'єднані у шість логічно пов'язаних груп, а саме: створення та обслуговування безпечної мережі за допомогою надійних систем; захист конфіденційних даних власника картки; створення прозорої програми керування вразливостями; застосування суворих заходів контролю доступу; здійснення моніторингу і тестування всіх мереж; постійна підтримка актуальної політики інформаційної безпеки.
Sarbanes-Oxley Act (SOX) [182]	Це кодекс США внутрішнього контролю над фінансовою звітністю компанії, яким передбачена демонстрація фінансових документів в автоматичному режимі. Зазначені автоматизовані рішення для баз даних допомагають застосовувати найкращі практики контролю версій спеціального програмного забезпечення. Зміни в базах даних перевіряються на відповідність політики безпеки і відповідному змістовному навантаженню, одночасно запобігаючи несанкціонованим змінам і змінам поза процесом.
Monetary Authority of Singapore-Technology Risk Management (MAS-TRM), з англ. «грошово-кредитне управління Сінгапуру – управління технологічними ризиками» [183]	Це рекомендації, які встановлюють правила для фінансових установ у Сінгапурі, та зосереджені на кіберстійкості, розробці спеціалізованого програмного забезпечення та хмарних обчисленнях. Це вимога до цифрової трансформації, яка визначає технологічні принципи управління ризиками, які відбуваються серед фінансових установ у всьому світі. Основні вектори регулювання здійснюється за наступними напрямками: соціальна інженерія серед співробітників правління та вищого керівництва установи (компанії); управління IT-проєктами; розробка та управління програмним забезпеченням; управління віддаленим доступом; використання власного цифрового пристрою замість офіційно наданого (концепція BYOD); безпека даних та інфраструктури; операції з кібербезпеки; кібернавчання; тестування на проникнення; інтернет-фінансові послуги.
General Data Protection Regulation (GDPR), з англ. «загальний регламент захисту даних» [184]	Регламент захисту даних який застосовується в усіх країнах-членах Європейського Союзу для гармонізації законів про конфіденційність даних. Цей Регламент встановлює правила та принципи, що стосуються захисту фізичних осіб щодо обробки персональних даних, а також правила, що стосуються вільного руху персональних даних.

Продовження табл. 3.1

1	2
Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), з англ. «Федеральний закон Грема-Ліча-Блілі» [185]	Закон про фінансову модернізацію, застосовується до фінансових установ США та регулює безпечне поводження з непублічною особистою інформацією, включаючи фінансову звітність та іншу особисту інформацію. До адміністративних, технічних та фізичних гарантій GLBA віднесено: забезпечення безпеки та конфіденційності записів та інформації клієнтів; захист від будь-яких можливих загроз, загроз безпеці цілісності даних; захист від несанкціонованого доступу до даних/інформації, які можуть нанести суттєві збитки або спричинити незручності для будь-якого клієнта; захист та моніторинг записів та інформації про клієнтів; створення та підтримання ефективної оцінки ризиків; визначення, впровадження та аудит конкретних заходів внутрішнього контролю безпеки, що захищають ці дані.

Джерело: систематизовано автором за вказаними даними

Систематизація нормативно встановлених вимог до інформаційної безпеки, зазначених у міжнародно визнаних стандартах Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes-Oxley Act (SOX), Monetary Authority of Singapore-Technology Risk Management (MAS-TRM), General Data Protection Regulation (GDPR) наведена в таблиці 3.2.

Таблиця 3.2

Систематизація нормативно встановлених вимог до інформаційної безпеки

Вимога (потреба)	Нормативні акти, що регулюють діяльність	Спроможність
1	2	3
Виявлення конфіденційних даних/оцінка ризиків, прогалин у безпеці і вразливості	PCI 2 PCI 6.1 MAS 2.0.1 MAS 2.0.5 SOX 302 SOX 404 GDPR Article 25/32/35	– виявлення активних служб баз даних і регламентованих даних, що зберігаються в базах, хмарних програмах; – оцінка ризиків вразливості баз даних, кожного активу, чутливості даних, недоліків конфігурації; – виявлення санкціонованих та несанкціонованих хмарних додатків до яких мають доступ користувачі, і оцінювання ризиків кожного з них.
Впровадження засобів контролю безпеки	PCI 3 PCI 6.6 PCI 7 PCI 8.5 PCI 11.5 MAS 5.1.2 MAS 5.1.7 (c/d/j) MAS 12.1.6	– брандмауер веб-програм (WAF) – захист загальнодоступних веб-програм; – віртуальне встановлення виправлень – компенсаційний контроль, що дозволяє блокувати вразливі місця веб-додатків; – самозахист програми під час виконання (RASP) – нейтралізує загрози у виробництві; – захист від захоплення облікового запису –

Продовження табл. 3.2

1	2	3
	SOX 302 SOX 404 GDPR Article 5/25/32	– пом'якшує зловмисні атаки АТО, не впливаючи при цьому на законних користувачів; – хмарна служба доставки додатків – захищає веб-сайти від DDoS-атак; – керування правами користувачів – допомагає реалізувати мінімальні привілеї та бізнес-доступ; – маскування даних – усуває використання конфіденційних даних у невиробничих системах, шляхом обмеження доступу.
Аудит, моніторинг і забезпечення доступу	PCI 10 PCI 12 MAS 5.1.2 MAS 5.1.7 (b, e, f, j) SOX 302 SOX 404 SOX 409 GDPR Article 25/32/33/34/35/44	– моніторинг активності баз даних і файлів збирає та записує доступ до баз даних і файлів, а також деталі активності; – сповіщення та блокування режиму доступу до регламентованих даних у баз даних і файлах з метою зменшення ризиків порушення даних; – попередньо визначені політики аудиту PCI та SOX забезпечують автоматизований журнал аудиту; – аудит доступу привілейованих користувачів, моніторинг усіх дій привілейованих користувачів, безпосередній доступ до сервера баз даних; – базові політики доступу до даних користувача.
Звітність	PCI SOQ SOX 302 SOX 404 SOX 409 GDPR Article 32/33/34	– попередня підготовка звітів для PCI, SOX та інших нормативних актів; – усунення людського ресурсу який схильний до помилок і забирає багато часу на підготовку звітів; – узгодження змін SOX показує аудиторам SOX, що зміни баз даних можна відстежити до схвалених запит на зміну квитка.

Джерело: складено автором за даними [181–185]

Дотримання систематизованих вимог дозволить економічним суб'єктам забезпечити безпеку та конфіденційність записів та інформації працівників, контрагентів та інших стейкхолдерів, цілісність даних; захист від несанкціонованого доступу до даних/інформації, які можуть нанести суттєві збитки; впровадження превентивних заходів протидії можливим ризикам.

Водночас, в сучасних умовах системи захисту інформації та кібербезпеки корпорацій і установ світового ринку обробляють та зберігають доволі потужний масив конфіденційних даних, таких як клієнт-транзакції, інформацію про облікові записи, персональні дані та інше. Ефективність їх функціонування ускладнюється постійною зміною обсягу, швидкості і різноманітності атак. Виникає необхідність використовувати нетрадиційні підходи до виконання заходів з безпеки.

Найпотужнішим на сьогоднішній день у світі превентивним інструментом захисту від інформаційних та кіберризиків правомірно визначити дистрибутив Kali Linux. Цей дистрибутив включає тестування на проникнення, криміналістику, зворотне проєктування та оцінку вразливості. Це кульмінація багаторічних удосконалень та результат безперервної еволюції від WHoppiX до WHAX, потім до BackTrack, і тепер до повноцінного дистрибутива тестування на проникнення. У Kali застосовується багато функцій Debian GNU/Linux і враховуються поради членів динамічного світового співтовариства, що працює над спеціальним програмним забезпеченням з відкритим кодом.

Враховуючи наявність традиційних та нетрадиційних інструментів забезпечення інформаційної безпеки, побудова ефективної системи захисту інформації повинна передбачати певну етапність (рис. 3.4).

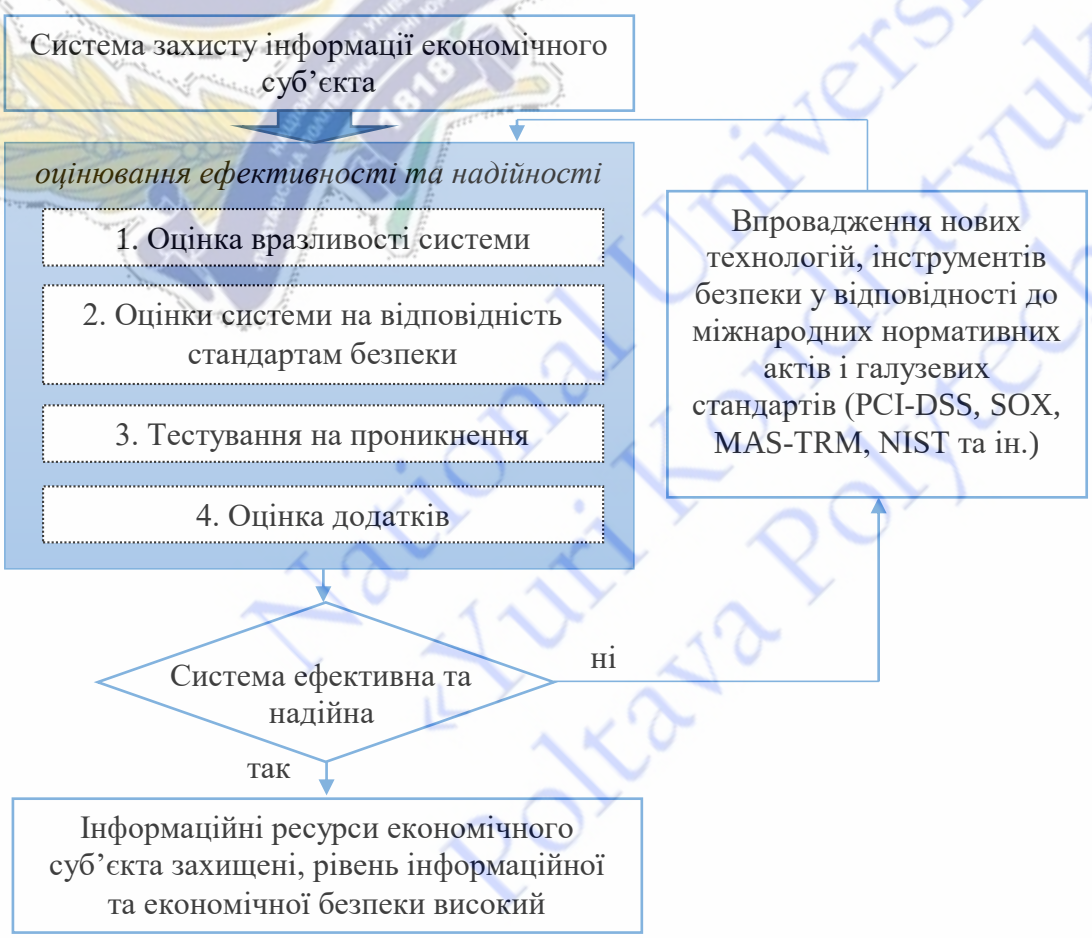

Рис. 3.4. Алгоритм побудови ефективної системи захисту інформації

Джерело: розроблено автором

Отже, згідно з запропонованим алгоритмом забезпечення ефективної системи захисту інформації можливе лише за умови систематичного її аналізу та оцінювання, що передбачає оцінку вразливості системи, оцінку системи на відповідність стандартам безпеки, тестування на проникнення та оцінку додатків.

Дослідження вразливості систем завдяки його простоті часто виконується на регулярній основі у досить досконалій розгалуженій архітектурі у рамках демонстрації рівня їхньої захищеності чи відповідності деяким стандартам безпеки. Утиліти, що використовуються для виявлення live-систем у цільовому оточенні, ідентифікують послуги, сканують деякі порти, та проводять їх аналіз з метою збору якомога більшої кількості інформації про систему. Потім зібрану інформацію перевіряють на відомі сигнатури вразливостей. Останні складаються з комбінацій фрагментів даних, які дозволяють розпізнати відомі проблеми безпеки. Тут використовується якомога більше відомостей, оскільки чим більше їх буде, тим точніше виявиться ідентифікація вразливості. Існує безліч показників, що становлять інтерес під час аналізу уразливостей систем. Серед них можна назвати такі – версія операційної системи, рівень patch, архітектура процесора, версія цільового програмного забезпечення.

Коли перевірка завершена, виявлені вразливості зазвичай пов’язують із стандартними ідентифікаторами, такими як CVE (Common Vulnerabilities and Exposures) [186], EDB-ID або кодами класифікації вразливостей, прийняті постачальниками інструментів сканування. Ця інформація разом із відомостями про оцінку вразливостей за методикою CVSS (Common Vulnerability Scoring System) [187] використовується для визначення рівня ризику. Всі ці відомості з урахуванням хибно позитивних та хибно негативних повідомлень про вразливості дають загальне уявлення, які потрібно враховувати, аналізуючи результати сканування.

Оскільки автоматизовані засоби використовують для виявлення вразливостей баз даних сигнатур, найменше відхилення від відомої сигнатури здатне змінити результат і, відповідно, обґрунтованість повідомлень про

виявлені уразливості. При цьому хибно позитивні результати вказують на те, чого немає, а хибно негативні, навпаки, приховують існуючі проблеми. Тому якість та можливості автоматичних сканерів уразливості безпосередньо залежать від застосовуваних базами даних сигнатур.

Наступним етапом є оцінка систем на відповідність стандартам безпеки. Подібні випробування систем доволі поширені, оскільки засновані на аналізі вимог, що визначаються державними та індустріальними стандартами, що поширюються на організації, як приклад PCI-DSS, DISA STIG, FedRAMP, FISMA. В даний час велика кількість організацій використовують Kali Linux як платформу саме для оцінки систем на відповідність стандартів безпеки.

Третій етап оцінювання ефективності та надійності систем захисту інформації передбачає тестування на проникнення. Традиційні тести на проникнення рідко починаються з визначення області перевірки. Натомість для них встановлюють певні цілі. Наприклад: «змоделювати наслідки компрометації внутрішнього користувача» або «з'ясувати, що трапилося б, якби організація потрапила під цілеспрямовану атаку, яку виконує зовнішній зловмисник». Ключовою відмінністю подібного аналізу є те, що в ході його виконання не тільки знаходять та оцінюють уразливості, але й ще використовують знайдені загрози для розкриття найгірших варіантів розвитку подій У ході тестування на проникнення не покладаються виключно на інструменти сканування систем на вразливості. Робота продовжується за допомогою дослідження уразливостей, застосування експлойтів або проведення випробувань для виключення хибно позитивних результатів, робиться все можливе для виявлення прихованих вразливостей. Подібне дослідження часто включає експлуатацію виявлених вразливостей, оцінку рівня доступу, який надають експлойти, та використання цього підвищеного рівня доступу як відправну точку для додаткових атак на цільову систему [179].

Незважаючи на складність та багатоплановість традиційного тестування на проникнення, хід такого дослідження можна впорядкувати, розбивши на кілька

кроків: збір інформації, виявлення вразливостей, експлуатація вразливостей, проникнення та вилучення даних, підготовка звітів.

Особливістю четвертого етапу – оцінки додатків – є той факт, що вивченню підлягає конкретна програма. Подібні перевірки стають все більш поширеними через специфіку додатків, що використовуються суб'єктами господарювання. Більшість з цих програм створено безпосередньо підприємствами та установами. Ряд додатків, які мають бути проаналізовані з позиції безпеки, включає:

1. Веб-додатки. Стандартні тести доволі часто дозволяють виявити базові проблеми веб-додатків.

2. Прикладні та серверні додатки, зокрема додатки для читання PDF-файлів або відео програм які використовують інтернет-ресурси. На сьогоднішній день зловмисники постійно вдосконалюють свої засоби ураження зазначених додатків на теренах інтернету, тому оцінка їх вразливості є беззаперечно необхідною.

3. Мобільні застосунки. Зі зростанням популярності мобільних пристроїв ці застосунки стають постійними предметами досліджень безпеки. Такі програми дуже швидко розвиваються і змінюються, тому в даній сфері методологія досліджень поки що не досягла достатньої зрілості, що веде до регулярної, практично щотижневої, появи нових методик.

Дослідження додатків можна проводити різними способами. Наприклад, для ідентифікації потенційних загроз є можливість застосувати автоматичні засоби, призначені для тестування конкретної програми. Ґрунтуючись на особливостях роботи додатків, подібні засоби намагаються знайти у них невідомі слабкості, замість того щоб покладатись на набір заздалегідь заданих сигнатур. Інструменти для аналізу програм повинні враховувати особливості їх тактики дій. Зокрема, поширеним є сканер уразливостей веб-додатків Burp Suite [188]. У ході дослідження програми він знаходить поля для введення даних, після чого застосовує різні атаки шляхом SQL-ін'єкцій, спостерігаючи в цей час за «поведінкою» додатка, з метою виявлення атак, які виявились успішними.

Існують і складніші сценарії аналізу додатків. Такі перевірки можуть бути виконані в інтерактивному режимі. При їх проведенні використовують моделі «чорної і білої скриньки».

Дослідження методом чорної скриньки: інструмент (або дослідник) взаємодіє з додатком, не володіючи спеціальними знаннями про нього або особливим доступом до нього, що перевищує можливості звичайного користувача. Наприклад, у випадку з веб-застосунком дослідник може мати лише доступ до функцій і можливостей, відкритих користувачеві, не авторизованому в системі. Будь-який обліковий запис буде таким самим, який звичайний користувач може зареєструвати самостійно. Це не дозволить атакуючому аналізувати функціонал, доступний лише привілейованим користувачам, облікові записи яких необхідно створювати адміністратору.

Дослідження методом білої скриньки: інструмент (або дослідник) часто має повний доступ до вихідного коду програми, доступ адміністратора до платформи, на якій воно виконується і т. д. Це гарантує виконання повного та ретельного аналізу всіх можливостей програми незалежно від того, де саме знаходиться функціональність, що досліджується. Мінус такого дослідження полягає в тому, що воно не є імітацією реальних дій зловмисника.

Водночас існує комбінований спосіб. Зазвичай такий алгоритм дослідження роботи додатку буде проводиться в залежності від поставленої мети. Якщо вона полягає у визначені того, що може статися з додатком, який виявиться предметом цілеспрямованої зовнішньої атаки, то, ймовірно, найкраще підійде тестування методом чорної скриньки. Якщо ж мета полягає в ідентифікації та усуненні як найбільшої кількості проблем з безпекою, за порівняно короткий час, то дослідження методом білої скриньки здатне виявитися ефективнішим.

В інших випадках можна застосувати гібридний підхід, коли дослідник не має повного доступу до вихідного коду програми для платформи, на якій воно виконується, але виданий йому обліковий запис підготовлений адміністратором і відкриває доступ до максимально можливої кількості функцій програми.

У випадку успішного проходження зазначених чотирьох етапів оцінювання система захисту інформації суб'єкта господарювання може вважатися надійною і забезпечувати високий рівень інформаційної та економічної безпеки. У протилежному випадку необхідним постає впровадження нових технологій, інструментів безпеки у відповідності до міжнародних нормативних актів і галузевих стандартів (PCI-DSS, SOX, MAS-TRM, NIST та ін.) з метою удосконалення існуючої системи захисту інформації.

Проведений компаративний аналіз систем інформаційної безпеки дозволяє обґрунтовано стверджувати, що перспективним напрямом підвищення ефективності систем захисту інформації та кібербезпеки в Україні є приведення їх у відповідність до міжнародно визнаних стандартів, стандартів Європейського Союзу та НАТО, застосування потужної лінійки інструментів як на технологічному, так і на програмному рівнях. Системи захисту інформації суб'єктів національної економіки мають ґрунтуватися на використанні розгалужених архітектур, методів захисту, які спрямовані на упередження, виявлення та реагування на потенційні кіберзагрози.

Враховуючи важливість впровадження систем захисту на мікрорівні, водночас необхідним для забезпечення інформаційної безпеки мезо- та макрорівня національної економіки є провадження ефективної державної політики.

3.3. Стратегічні орієнтири державної політики щодо забезпечення інформаційної безпеки економіки України

В сучасних умовах державна політика має бути спрямована на мінімізацію кібертероризму, у тому числі і міждержавного, що є одним із найбільших ризиків економічній безпеці країни, оскільки це ефективний сучасний інструмент ведення війн і відстоювання геополітичних інтересів. Рівень захисту України від цифрових загроз за міжнародним рейтингом The Network Readiness Index є

значно нижчим, ніж у європейських країнах, що вказує на загрозу корисному розвитку цифровізації, а також генерування трансграничних загроз країнам ЄС. Ігнорування цих загроз призводить до їх укорінення та тіньової інституалізації, що повністю нівелює вплив економічних регуляторів і потребує для вирішення більш системні заходи протидії. Це підтверджує необхідність безпекоорієнтованого управління економікою та формування нових підходів до забезпечення інформаційної безпеки держави в умовах сьогодення.

Розв'язання нагальних соціально-економічних проблем держави, пов'язаних з безпечним функціонуванням інформаційного середовища системи суспільних відносин передбачає обґрунтування стратегічних пріоритетів та розроблення концепції формування безпекоорієнтованого інформаційного середовища України в умовах воєнних та повоєнних викликів.

В умовах політичної та економічної нестабільності потрібно враховувати, що інформаційна безпека є категорією надбудови й обумовлена економічним розвитком держави [118]. Тому держава, при формуванні політики інформаційної безпеки національної економіки, повинна враховувати глобальні тенденції соціально-економічного розвитку, етап розвитку суспільства, дотримуватися комплексного підходу при розробленні та реалізації заходів. Отже, державна політика у сфері зміцнення інформаційної безпеки національної економіки передбачає цілеспрямовану діяльність органів державної влади та місцевого самоврядування з урахуванням стратегічних напрямів.

Формування стратегічних напрямів державної політики відбувається у відповідності до цільових стратегічних завдань та поставленої мети, що повинні бути законодавчо встановлені у базових нормативно-правових актах держави. Під час обґрунтування варіантів стратегічних рішень визначаються суб'єкти, відповідальні за запровадження заходів щодо реагування на загрози, та ресурсне забезпечення реалізації альтернативних напрямів державної політики.

З метою визначення стратегічних напрямів державної політики щодо зміцнення інформаційної безпеки національної економіки необхідно закцентувати увагу на обґрунтуванні основних положень Стратегії

інформаційної безпеки і Стратегії економічної безпеки України на період до 2025 року.

З огляду на особливості багаторівневої структури системи забезпечення інформаційної безпеки національної економіки доцільно використати метод аналізу ієрархій. Метод аналізу ієрархій був розроблений на початку 1990-х років американським вченим Т. Сааті. Цей метод дає змогу описати досліджувану систему та її проблему в термінах ієрархічної структури, дозволяє застосувати ряд засобів для встановлення впорядкованих пріоритетів та визначення інтенсивності взаємодії компонентів для досягнення головної мети, у результаті визначається кількісна оцінка пріоритетності елементів ієрархії.

Згідно з теорією систем, ієрархія є видом системи, що включає елементи, зруповані в незалежні підмножини (групи). На елементи i-ї групи впливають елементи групи $(i-1)$. У свою чергу елементи i-ї групи несуть вплив на елементи групи $(i+1)$ [189].

З метою порівняння та багатокритеріального ранжування критеріїв і заходів зміцнення інформаційної безпеки національної економіки пропонуємо рівні ієрархій (рис. 3.5).

Вищим рівнем ієрархії є мета – зміцнення інформаційної безпеки національної економіки.

На наступному рівні перебувають критерії: забезпечення стійкості національної економіки до інформаційних та кіберзагроз (X); розвиток інформаційного суспільства (Y); успішна адаптація суб'єктів господарювання до функціонування в умовах цифровізації (Z); підвищення рівня цифрової грамотності та інформаційної культури населення (R). Нижчий рівень становлять фактори, які впливають на досягнення цих критеріїв.

Для критерію X – це створення системи раннього виявлення, прогнозування та запобігання загрозам ($X1$), ефективна взаємодія державних органів при формуванні та реалізації державної політики ($X2$), запобігання поглибленню «цифрової нерівності» в національній економіці ($X3$), розвиток спроможностей протидії загрозам в інформаційному просторі ($X4$).

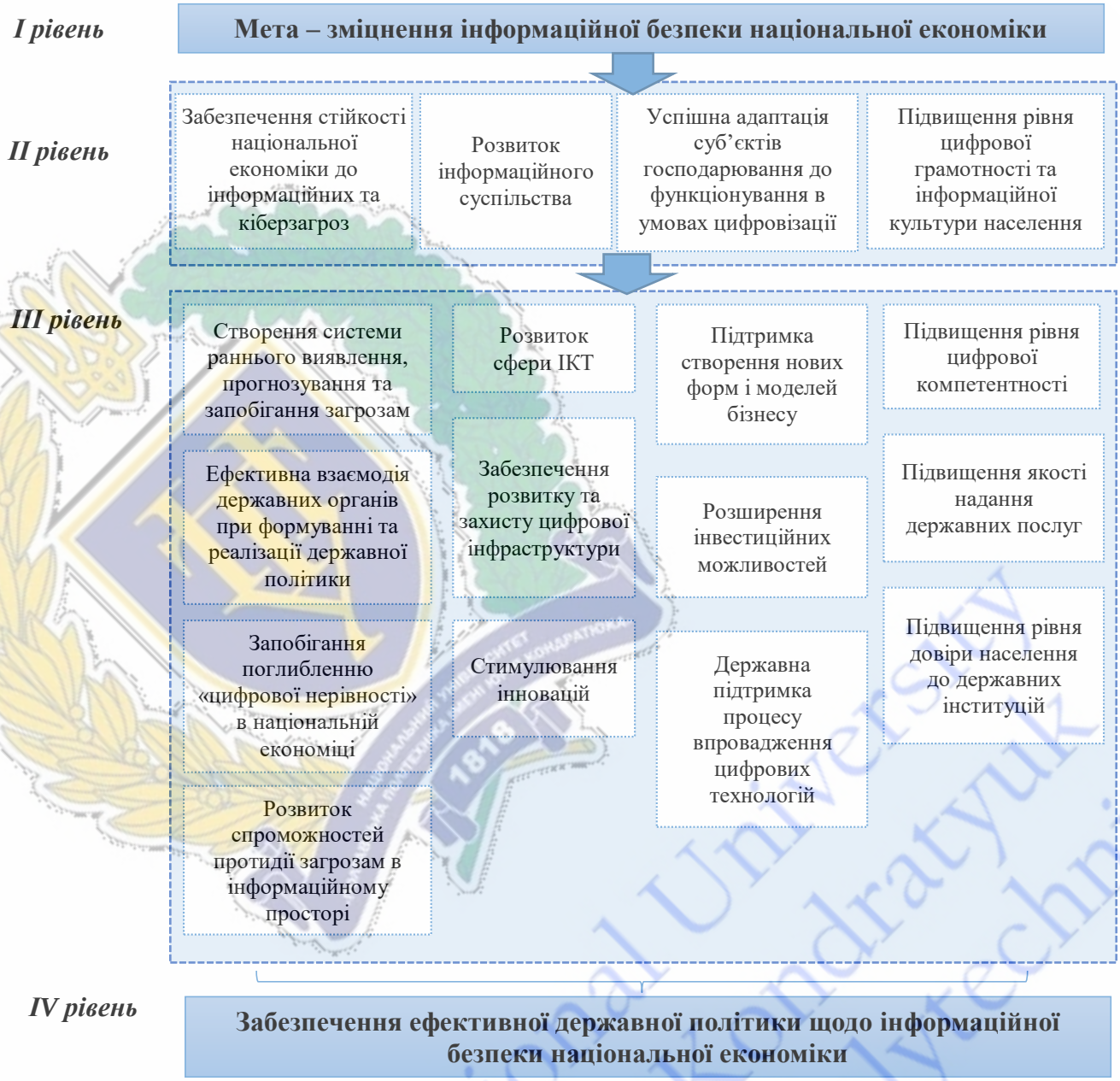

Рис. 3.5. Ієрархія визначення пріоритетних напрямів реалізації державної політики забезпечення інформаційної безпеки національної економіки на основі положень Стратегії інформаційної безпеки України та Стратегії економічної безпеки України на період до 2025 року

Джерело: розроблено автором

Для критерію *Y* – це розвиток сфери ІКТ (*Y1*), забезпечення розвитку та захисту цифрової інфраструктури (*Y2*), стимулювання інновацій (*Y3*).

Для критерію *Z* – це підтримка створення нових форм і моделей бізнесу (*Z1*), розширення інвестиційних можливостей (*Z2*), державна підтримка процесу впровадження цифрових технологій (*Z3*).

Для критерію R це підвищення рівня цифрової компетентності (R1), підвищення якості надання державних послуг (R2), підвищення рівня довіри населення до державних інституцій (R3).

Декомпозицію забезпечення інформаційної безпеки національної економіки з урахуванням окреслених критеріїв можна представити у схематичному вигляді (рис. 3.6).

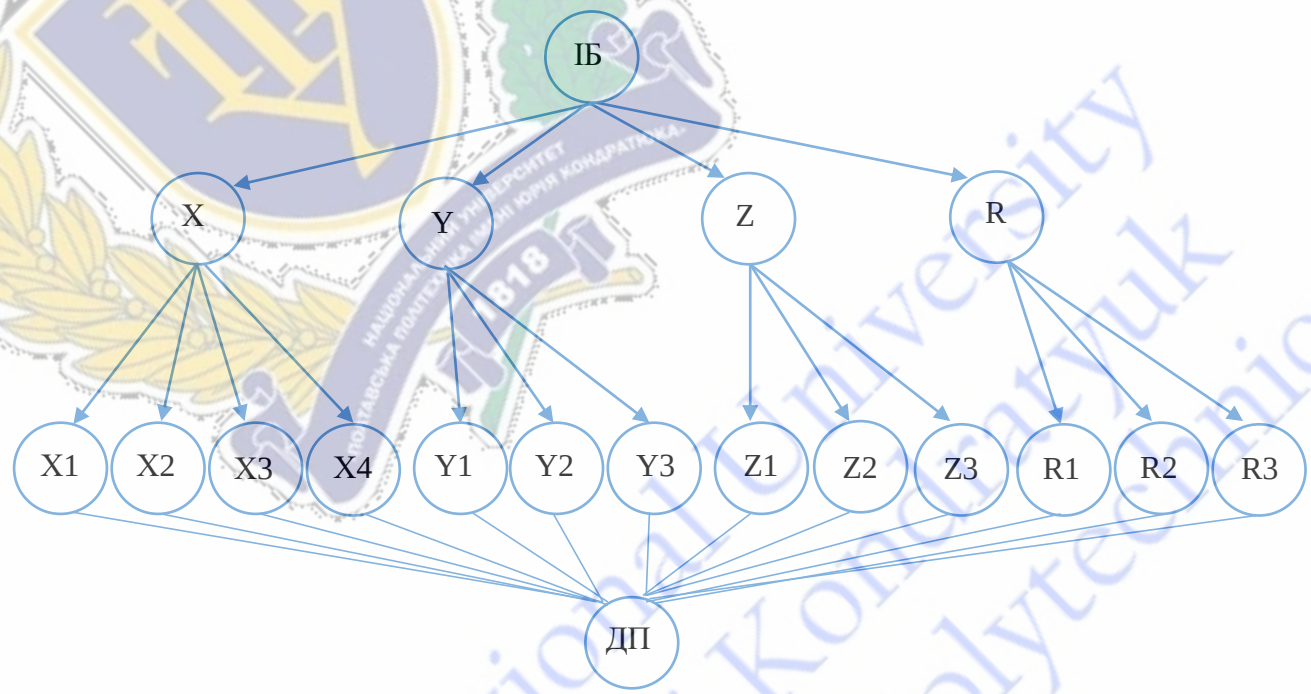

Рис. 3.6. Ієрархічна модель визначення стратегічних пріоритетів державної політики забезпечення інформаційної безпеки національної економіки

Джерело: побудовано автором

Першим етапом у застосуванні методу аналізу ієрархій є попарне порівняння всіх показників незалежно від змісту стратегій, яке виконується з використанням так званої шкали відношень Сааті (табл. 3.3).

Таблиця 3.3

Міра важливості	Визначення переваги одного об'єкту в порівнянні з іншим	Пояснення
1	Однакова значущість	Дві дії вносять однаковий вклад у досягнення цілі
3	Деяка перевага значущості одної дії над іншою (слабка значущість)	Досвід та судження дають легку перевагу одної дії перед іншою
5	Суттєва або сильна значущість	Досвід та судження дають сильну перевагу одної дії перед іншою
7	Дуже сильна або очевидна значущість	Перевага одної дії перед іншою дуже сильна. Її вищість практично очевидна
9	Абсолютна значущість	Свідчення на користь переваги одної дії над іншою абсолютно очевидно
2, 4, 6, 8	Проміжні значення між сусідніми оцінками шкали	Ситуація, коли необхідне компромісне рішення
Обернені величини наведених вище чисел	Якщо дії *i* при порівнянні з дією *j* приписується одно з наведених вище чисел, то дії *j* при порівнянні з *i* приписується обернене значення	Обґрунтоване припущення

Джерело: побудовано автором на основі даних [190]

Результати попарних порівнянь з використанням наведеної шкали заносяться у матрицю розмірністю m x m, де m – кількість параметрів оцінки. З формальної точки зору, заповнення експертом такої таблиці є відображенням його думки щодо впливу факторів другого рівня на мету аналізу – вибір найбільш ефективної стратегії [191].

Матриця попарних порівнянь для другого рівня має вигляд, наведений у таблиці 3.4.

Таблиця 3.4

Матриця попарних порівнянь другого рівня ієрархії

	X	*Y*	*Z*	*R*	Пріоритети	Нормалізовані пріоритети
1	2	3	4	5	6	7
Забезпечення стійкості національної економіки до інформаційних та кіберзагроз (*X*)	1	2	3	4	2,213	0,467
Розвиток інформаційного суспільства (*Y*)	1/2	1	2	3	1,316	0,278

Продовження табл. 3.4

1	2	3	4	5	6	7
Успішна адаптація суб'єктів господарювання до функціонування в умовах цифровізації (*Z*)	1/3	1/2	1	2	0,760	0,160
Підвищення рівня цифрової грамотності та інформаційної культури населення (*R*)	1/4	1/3	1/2	1	0,452	0,095
Всього					4,741	1,000

Джерело: розраховано автором

Перевагами використання методу аналізу ієрархій під час визначення пріоритетних напрямів реалізації стратегій є всебічне охоплення завдань і вказаних пріоритетів. Однією з головних переваг наведеного підходу у порівнянні з іншими методами визначення пріоритетних напрямів розвитку систем – інноваційність у підході до оцінювання структури проблеми на підставі чітко окреслених суджень та кількісної оцінки факторів.

Попарні порівняння використовуються для визначення найбільш прийнятних критеріїв вибору напрямів. Вибір напряму здійснюється на основі обраних критеріїв за чотирма компонентами, які попарно порівнюють за кожним із критеріїв за допомогою матриці. Сума нормалізованих пріоритетів дорівнює одиниці [191].

Узгодженість ієрархії напрямів забезпечення інформаційної безпеки національної економіки супроводжується визначенням індексу узгодженості всіх елементів. Порівняльна ефективність реалізації положень стратегій в наведеній матриці попарних порівнянь третього рівня ієрархії характеризується системою обраних пріоритетів (див. табл. 3.5–3.8). На їхній підставі ранжуються за пріоритетністю напрямки з найбільшим ефектом. Під час проведення оцінок пріоритетності напрямів бралися до уваги всі порівнянні елементи.

Отже, другим етапом використання методу аналізу ієрархій є попарне порівняння змісту чотирьох стратегічних альтернатів за кожним окремим показником. У результаті ми отримаємо десять матриць розмірністю n x n, де n - кількість стратегій, що аналізуються.

Для встановлення відносної пріоритетності третього рівня ієрархії (*X*) за напрямом забезпечення стійкості національної економіки до інформаційних та кіберзагроз будуємо матрицю попарних порівнянь за визначеними критеріями (табл. 3.5).

Таблиця 3.5

Матриця попарних порівнянь третього рівня ієрархії (*X*)

	X1	*X2*	*X3*	*X4*	Пріоритети	Нормалізовані пріоритети
Створення системи раннього виявлення, прогнозування та запобігання загрозам (*X1*)	1	2	3	4	2,213	0,467
Ефективна взаємодія державних органів при формуванні та реалізації державної політики (*X2*)	1/2	1	2	3	1,316	0,278
Запобігання поглибленню «цифрової нерівності» в національній економіці (X3)	1/3	1/2	1	2	0,760	0,160
Розвиток спроможностей протидії загрозам в інформаційному просторі (X4)	1/4	1/3	1/2	1	0,452	0,095
Всього					4,741	1,000

Джерело: розраховано автором

Сформуємо матрицю попарних порівнянь третього рівня ієрархії розвиток інформаційного суспільства (Y). Проводимо аналіз за визначеними критеріями третього рівня щодо кожного елемента-критерію (табл. 3.6).

Таблиця 3.6

Матриця парних порівнянь третього рівня ієрархії (*Y*)

	Y1	*Y2*	*Y3*	Пріоритети	Нормалізовані пріоритети
Розвиток сфери ІКТ (Y1)	1	2	3	1,817	0,540
Забезпечення розвитку та захисту цифрової інфраструктури (Y2)	1/2	1	2	1,000	0,297
Стимулювання інновацій (Y3)	1/2	1/3	1	0,550	0,163
Всього				3,367	1,000

Джерело: розраховано автором

Матрицю попарних порівнянь третього рівня ієрархії «успішна адаптація суб'єктів господарювання до функціонування в умовах цифровізації (Z)» та результати аналізу за визначеними критеріями подано в таблиці 3.7.

Таблиця 3.7

Матриця парних порівнянь третього рівня ієрархії (*Z*)

	Z*1*	Z*2*	Z*3*	Пріоритети	Нормалізовані пріоритети
Підтримка створення нових форм і моделей бізнесу (Z1)	1	2	3	1,817	0,540
Розширення інвестиційних можливостей (Z2)	1/2	1	2	1,000	0,297
Державна підтримка процесу впровадження цифрових технологій (Z3)	1/2	1/3	1	0,550	0,163
Всього				3,367	1,000

Локальні пріоритети для третього рівня ієрархії щодо критерію підвищення рівня цифрової грамотності та інформаційної культури населення визначені в таблиці 3.8.

Таблиця 3.8

Матриця парних порівнянь третього рівня ієрархії (*R*)

	R1	*R2*	*R3*	Пріоритети	Нормалізовані пріоритети
Підвищення рівня цифрової компетентності (R1)	1	2	3	1,817	0,540
Підвищення якості надання державних послуг (R2)	1/2	1	2	1,000	0,297
Підвищення рівня довіри населення до державних інституцій (R3)	1/2	1/3	1	0,550	0,163
Всього				3,367	1,000

Наступним етапом застосування методу аналізу ієрархій є поєднання локальних пріоритетів і розрахунок глобальних пріоритетів альтернатив щодо всієї ієрархії, що фактично є основним завданням методу аналізу ієрархій. У результаті цих дій отримується відсотковий розподіл пріоритетів між усіма n об'єктами, які порівнюються за сукупністю з m критеріїв.

Вектор локальних пріоритетів розраховується за наступним алгоритмом.

1. Для кожного рядка матриці попарних порівнянь розраховується середнє геометричне її елементів за формулою:

$$\bar{a}_i = \sqrt[n]{a_{i1}a_{i2}...a_{in}} \quad (3.1)$$

2. Визначається сума усіх середніх геометричних.

3. Кожне середнє геометричне ділиться на їх суму.

Таким чином, залежність зміцнення інформаційної безпеки національної економіки від факторів другого рівня ієрархії правомірно представити у наступному вигляді:

$$W = 0{,}467X + 0{,}278Y + 0{,}160Z + 0{,}095R \quad (3.2)$$

Залежність факторів другого рівня ієрархічної структури від факторів третього рівня представлено в наступному вигляді:

$X = 0{,}467X1 + 0{,}278X2 + 0{,}160X3 + 0{,}095X4$;

$Y = 0{,}540Y1 + 0{,}297Y2 + 0{,}163Y3$;

$Z = 0{,}540Z1 + 0{,}297Z2 + 0{,}163Z3$;

$R = 0{,}540R1 + 0{,}297R2 + 0{,}163R3$.

Отже, можна визначити залежність забезпечення інформаційної безпеки національної економіки від факторів третього рівня:

$W = 0{,}467(0{,}467X1 + 0{,}278X2 + 0{,}160X3 + 0{,}095X4) + 0{,}278(0{,}540Y1 +$
$+ 0{,}297Y2 + 0{,}163Y3) + 0{,}160(0{,}540Z1 + 0{,}297Z2 + 0{,}163Z3) + 0{,}095(0{,}540R1 +$
$+ 0{,}297R2 + 0{,}163R3)$;

$$W = 0{,}218X1 + 0{,}134X2 + 0{,}075X3 + 0{,}044X4 + 0{,}150Y1 + 0{,}082Y2 +$$
$$+ 0{,}045Y3 + 0{,}086Z1 + 0{,}048Z2 + 0{,}026Z3 + 0{,}051R1 + 0{,}028R2 + 0{,}015R3.$$

Систематизуємо отриманий результат у табличній формі (табл. 3.9 і 3.10).

Таблиця 3.9

Коефіцієнти при факторах третього рівня

Створення системи раннього виявлення, прогнозування та запобігання загрозам (X1)	0,218
Ефективна взаємодія державних органів при формуванні та реалізації державної політики (X2)	0,134
Запобігання поглибленню «цифрової нерівності» в національній економіці (X3)	0,075
Розвиток спроможностей протидії загрозам в інформаційному просторі (X4)	0,044
Розвиток сфери ІКТ (Y1)	0,150
Забезпечення розвитку та захисту цифрової інфраструктури (Y2)	0,082
Стимулювання інновацій (Y3)	0,045
Підтримка створення нових форм і моделей бізнесу (Z1)	0,086
Розширення інвестиційних можливостей (Z2)	0,048
Державна підтримка процесу впровадження цифрових технологій (Z3)	0,026
Підвищення рівня цифрової компетентності (R1)	0,051
Підвищення якості надання державних послуг (R2)	0,028
Підвищення рівня довіри населення до державних інституцій (R3)	0,015

Таблиця 3.10

Коефіцієнти при факторах третього рівня (впорядковані)

Підвищення рівня довіри населення до державних інституцій (R3)	0,015
Державна підтримка процесу впровадження цифрових технологій (Z3)	0,026
Підвищення якості надання державних послуг (R2)	0,028
Розвиток спроможностей протидії загрозам в інформаційному просторі (X4)	0,044
Стимулювання інновацій (Y3)	0,045
Розширення інвестиційних можливостей (Z2)	0,048
Підвищення рівня цифрової компетентності (R1)	0,051
Запобігання поглибленню «цифрової нерівності» в національній економіці (X3)	0,075
Забезпечення розвитку та захисту цифрової інфраструктури (Y2)	0,082
Підтримка створення нових форм і моделей бізнесу (Z1)	0,086
Ефективна взаємодія державних органів при формуванні та реалізації державної політики (X2)	0,134
Розвиток сфери ІКТ (Y1)	0,150
Створення системи раннього виявлення, прогнозування та запобігання загрозам (X1)	0,218

На підставі проведених обчислень правомірно стверджувати, що основними факторами, які впливають на забезпечення інформаційної безпеки

національної економіки є формування системи превентивного виявлення, запобігання та мінімізації деструктивних наслідків ризиків і загроз в інформаційному просторі, подальший розвиток сфери ІКТ в Україні та ефективна взаємодія державних органів при формування та реалізації державної політики з інформаційної безпеки.

Підсумовуючи розрахунки, доцільно відмітити, що використання методу аналізу ієрархій під час встановлення стратегічних напрямів реалізації положень Стратегії інформаційної безпеки та Стратегії економічної безпеки України на період до 2025 року дає змогу визначити домінантність задекларованих напрямів для ефективної реалізації стратегій.

Визначення стратегячних орієнтирів реалізації державної політики в контексті забезпечення інформаційної безпеки економіки України дозволяє зробити висновок, що в сучасних умовах необхідна переорієнтація державної політики. Неврегульованість в Україні на законодавчому рівні багатьох питань, що пов'язані з бурхливим розвитком інформаційно-комунікаційної сфери, з поширенням цифрових технологій набула ознак небезпеки, оскільки ускладнення комунікаційних процесів – підвищило якість ризиків і загроз, які виявилися настільки складними та всеосяжними, що їхній рівень зростає в логарифмічній прогресії, порівняно з можливістю протидіяти їм за допомогою чинного законодавства. На цьому тлі прогресує поява нового виду злочинності – організованої кіберзлочинності, що змушує державу виокремлювати навіть основні завдання протидії загрозам в інформаційно-комунікаційній сфері за такими напрямами: захист персональних даних; безпека інформаційних і комунікаційних систем, державних структур; захист робочого середовища і технологій. Розширення цифрових та індивідуалізація багатьох інших видів послуг підвищили ризик шахрайства для широкого кола користувачів або провайдерів до критичного рівня, а ризики витоку інформації потребують уваги держави до підвищення рівня захисту електронних систем даних [81].

Стратегічні орієнтири державної політики щодо забезпечення інформаційної безпеки економіки України, розроблені з урахуванням результатів апробованого у дослідженні методу ієрархій, наведено на рисунку 3.7.

Рис. 3.7. Стратегічні орієнтири державної політики забезпечення інформаційної безпеки національної економіки

Джерело: розроблено автором

В умовах цифровізації національної економіки відбувається інституціональна трансформація. Для досягнення стійкого соціально-економічного зростання необхідно аналізувати проблеми, ризики та наслідки, що виникають унаслідок цифрової трансформації в роботі з інформацією, у тому числі у зв'язку із забезпеченням інформаційної безпеки.

Відповідальність органів влади за впровадження ІКТ та електронно-обчислювальної техніки в усі сфери національної економіки зростає, а інформація та інформаційні ресурси стають вирішальними чинниками розвитку особистості, суспільства та держави. В цьому аспекті необхідно постійно і ретельно оцінювати як можливості, які цифровізація відкриває для розвитку суспільства і бізнесу, так і загрози, які вона несе, насамперед, для економічної безпеки держави, а тому безпеку може бути забезпечено виключно за умови інтегрального системного комплексного підходу.

Основне завдання державної політики в контексті зміцнення інформаційної безпеки національної економіки це створення відповідного політичного, економічного, соціального, правового середовища й інституційного забезпечення. Цей процес повинен супроводжуватися реалізацією відповідних орієнтирів зміцнення інформаційної безпеки, серед яких найактуальнішими правомірно визначити:

– розроблення конкретних механізмів, що упереджують загрози інформаційній безпеці національної економіки;

– удосконалення законодавчої бази та гармонізація українського законодавства із нормами ЄС;

– впровадження державними органами влади та органами місцевого самоврядування проєктів з цифровізації, зокрема розвитку цифрової інфраструктури з урахуванням потреб кожної громади;

– розвиток співпраці з міжнародними організаціями у сфері інформаційної та кібербезпеки;

– забезпечення чіткої координації та розподілу функціональних обовязків органів державної влади, відповідальних за реалізацію політики у сфері інформаційної безпеки.

Головними стратегічними орієнтирами під час формування напрямів забезпечення інформаційної безпеки національної економіки необхідно визначити: забезпечення економічної безпеки держави та реалізації національних економічних інтересів на засадах інформаційної захищеності; стимулювання розвитку галузі ІКТ з одночасним впровадженням ефективних систем захисту інформаційних активів; удосконалення нормативно-правової бази щодо реалізації державної політики інформаційної безпеки та її гармонізація зі стандартами ЄС.

Висновки до розділу 3

Виходячи з актуальності цифрової трансформації національної економіки представлено архітектоніку національної економіки з урахуванням можливостей щодо створення валової доданої вартості, отримання вигід економічними суб'єктами та можливих ризиків і загроз, спричинених процесами цифровізації. Однією з головних небезпек для функціонування національної економіки та національних економічних інтересів суб'єктів усіх рівнів (нанорівня, мікрорівня, мезорівня та макрорівня) в умовах інформаційного суспільства визначено зростання інтенсивності та масштабів кібератак, рівня кіберзлочинності. Відповідно, за авторським концептом стійкість та адаптивність національної економіки до модифікованих ризиків і загроз в умовах цифровізації, здатність до відновлення та розвитку безпосередньо залежать від захищеності інформаційного простору, тобто інформаційної безпеки.

2. Запропоновані концептуальні засади забезпечення інформаційної безпеки національної економіки в умовах цифровізації як сукупності теоретико-

методологічних положень щодо обґрунтування: методологічного підходу, цілей, принципів і методів, які відображають новий погляд на цей процес та передбачають використання цільового впливу держави на процеси забезпечення інформаційної безпеки національної економіки з метою використання можливостей, що надає цифрова трансформація національної економіки та попередження розгортання принципово нових загроз інформаційній безпеці держави. Концептуальні засади можна вважати теоретичним базисом для розроблення методології забезпечення інформаційної безпеки національної економіки в умовах цифровізації.

3. На основі використання синергетичної парадигми, що, на відміну від «класичних» підходів в управлінні, базується на здійсненні цільового випливу на процеси самоорганізації в динамічних системах, якою є система інформаційної безпеки національної економіки, запропоновано механізм формування безпекоорієнтованого інформаційного середовища. Реалізація розробленого механізму дозволить досягнути позитивних синергетичних ефектів у процесі трансформації та розвитку національної економічної системи.

4. Обґрунтовано, що забезпечення інформаційної безпеки на мікрорівні полягає в оперативній ідентифікації та своєчасному реагуванні на ризики і загрози економічним даним; створенні умов для відшкодування завданих збитків; уникненні економічного та промислового шпіонажу.

5. На основі проведеного компаративного аналізу систем інформаційної безпеки встановлено, що модернізація структур та топологій систем захисту інформації відбувається під впливом розвитку технологій, змін у власному безпековому середовищі, формах, способах та технологіях застосування засобів кібервпливу і нових досягнень в цьому. Зазначені заходи здійснюються у відповідності до міжнародних нормативних актів і галузевих стандартів (PCI-DSS, SOX, MAS-TRM, NIST та інші).

6. Основою розроблення та реалізації управлінських рішень в напрямку підвищення рівня інформаційної безпеки національної економіки визначено ефективне інформаційне забезпечення, яке є підґрунтям гнучкої й адекватної

реакції на зміни середовища функціонування економічних суб'єктів. Запропоновано алгоритм побудови ефективних систем захисту інформації, який передбачає оцінку вразливості системи, оцінку системи на відповідність стандартам безпеки, тестування на проникнення та оцінку додатків. Його дієвість буде залежить від спроможності адекватної ідентифікації ризиків на кожному з визначених етапів.

7. На основі методу ієрархій розвинуто методичні підходи до реалізації основних стратегічних цілей забезпечення інформаційної безпеки національної економіки, що дало змогу виділити структуру, положення та концепти задекларованих напрямів. Обґрунтовано, що основними факторами, які впливають на забезпечення інформаційної безпеки національної економіки є формування системи превентивного виявлення, запобігання та мінімізації деструктивних наслідків ризиків і загроз в інформаційному просторі з метою захисту інформації та зменшення її витоків; подальший розвиток сфери ІКТ в Україні; ефективна взаємодія державних органів при формування та реалізації державної політики з інформаційної безпеки.

Основні результати дослідження відображені у наукових працях автора [81, 118, 170, 179].

ВИСНОВКИ

Проведене дослідження дозволило обґрунтувати теоретичні положення й розробити методичні та практичні рекомендації щодо формування й забезпечення інформаційної безпеки національної економіки. Отримані теоретико-методичні та прикладні результати дають підстави для таких висновків.

1. Досліджено етимологію понять «безпека», «економічна безпека», «інформаційна безпека». Систематизовано наукові погляди до трактування категорії «інформаційна безпеки», що дозволило виокремити її специфічні ознаки та запропонувати авторське визначення дефініції «інформаційна безпека національної економіки» як стан захищеності інформаційного середовища, що забезпечує реалізацію національних економічних інтересів, стійкість об'єктів на макро-, мезо-, мікро- та нанорівнях до внутрішніх та зовнішніх, реальних та потенційних загроз, у тому числі, пов'язаних із активним розвитком IT-технологій. На основі системного та захисного підходів розроблено структурну модель інформаційної безпеки національної економіки із сукупністю її властивостей при взаємозв'язку із зовнішнім середовищем.

2. Поглиблено концептуальні засади дослідження інформаційної безпеки як невід'ємного елементу національної економіки в умовах цифровізації, що створює нові можливості для реалізації національних інтересів і зміцнення безпеки національної економіки та водночас є тригером виникнення нових ризиків та загроз. Систематизовано наукові підходи до ідентифікації ризиків та загроз інформаційній безпеці національної економіки, що дозволило удосконалити таксономію загроз доповненням їх розподілу за об'єктами дестабілізуючих дій, за ступенем детермінізму та за ймовірністю реалізації, та яку правомірно вважати базисом для формування напрямів запобігання, протидії, мінімізації негативного впливу від їх реалізації.

3. Дослідження інформаційної безпеки національної економіки на основі інституціонального підходу дозволило сформувати інституційну архітектоніку

інформаційної безпеки. Вивчення інституційного середовища, взаємозалежності, комплементарності інститутів, що формують систему інформаційної безпеки національної економіки стає домінуючою основою, що визначає системний базис нової, цифрової економіки на засадах посилення взаємозв'язків між окремими елементами системи. Обґрунтування інституційного забезпечення інформаційної безпеки національної економіки в розрізі його основних структурних елементів дало змогу окреслити основні проблеми інституційно-організаційного забезпечення інформаційної безпеки в Україні (зокрема відсутність спеціально уповноваженого органу, що суперечить сучасним тенденціям організації регуляторних процесів) та комплекс необхідних заходів з організації, взаємодії, інформування, контролю та інших функціонально-розпорядчих дій, завдяки виконанню яких національна економіка перебуватиме в безпеці.

4. Досліджено сучасні умови та тенденції розвитку інформаційного середовища в Україні та світі, ступінь охоплення процесами цифровізації національної та світової економік, рівень внеску ІТ-сектору у формування ВВП. Кореляції в отриманих результатах засвідчує вищу стійкість цифрового сектору в кризових умовах у порівнянні з іншими галузями економіки, ефективність застосування цифрових технологій як базису зниження рівня тіньової економіки та зменшення корупційних ризиків. Доведено, що стан інформаційного середовища в Україні характеризується зростанням численних загроз безпеці національної економіки: поряд з традиційними загрозами, таким як промислове шпигунство, навмисне і ненавмисне розголошення конфіденційної інформації та комерційної таємниці, втручання сторонніх осіб в інформаційні системи і мережі, порушення цілісності баз даних тощо, створюється ряд додаткових загроз, пов'язаних з кібератаками, впливом шпигунських програм і вірусів, фішингом тощо.

5. Запропоновано та апробовано методичний підхід до оцінювання інформаційної безпеки національної економіки, що ґрунтується на інтегральному методі та передбачає формування системи валідних індикаторів (у тому числі показників цифрової, інституційної, кіберспроможності національної економіки та характеризують рівень і міру її відповідності домінуючим світовим тенденціям

розвитку цифрової економіки) з використанням методів нормування і згладжування, визначення вагових коефіцієнтів складників інформаційної безпеки на основі методу експертних оцінок, розрахунок інтегрального індексу інформаційної безпеки та його прогнозування з використанням моделі поліноміальної апроксимації. З метою обґрунтованого трактування результатів апробації авторської методики оцінювання рівня інформаційної безпеки застосовано теорію нечітких множин (п'ятирівневий нечіткий класифікатор).

6. Установлено залежність і досліджено чутливість інтегральної оцінки інформаційної безпеки та рівня економічної безпеки, які мають потенціал в аспекті забезпечення синергетичних ефектів. Забезпечення формування безпекоорієнтованого інформаційного середовища є базисом реалізації національних інтересів, що створює нові можливості для зміцнення безпеки національної економіки в умовах посилення впливу внутрішніх і зовнішніх дестабілізуючих чинників, та підтверджує необхідність провадження інтегрованої державної політики.

7. Обґрунтовано концепти синергетичного підходу до забезпечення інформаційної безпеки національної економіки, які передбачають застосування сукупності ідей, понять і методів у дослідженні та забезпеченні інформаційної безпеки національної економіки як складної, відкритої, нерівноважної, нелінійної, з елементами самоорганізації системи. Розроблено механізм формування безпекоорієнтованого інформаційного середовища, що ґрунтується на положеннях нової парадигми використання можливостей, пов'язаних з розвитком інформаційних технологій та попередження й запобігання новим загрозам інформаційній безпеці національної економіки шляхом захисту інформації, враховує економічні інтереси суб'єктів усіх рівнів (макро-, мезо-, мікро- та нанорівня), та дозволить отримати позитивні синергетичні ефекти в напрямку зміцнення безпеки національної економіки в умовах впливу внутрішніх і зовнішніх дестабілізуючих чинників.

8. На основі порівняння та багатокритеріального ранжування критеріїв і заходів зміцнення інформаційної безпеки національної економіки розроблено

ієрархію пріоритетних напрямів реалізації державної політики. Забезпечення інформаційної безпеки національної економіки в сучасних умовах визначається головними цільовими стратегічними пріоритетами при формуванні напрямів забезпечення інформаційної безпеки національної економіки, якими є: забезпечення економічної безпеки держави та реалізації національних економічних інтересів на засадах інформаційної захищеності; стимулювання розвитку галузі ІКТ з одночасним впровадженням найбільш ефективних програмно-технологічних рішень для захисту інформації та зменшення її витоків, попередження зовнішніх і внутрішніх ризиків та загроз; удосконалення нормативно-правової бази щодо реалізації державної політики інформаційної безпеки та її гармонізація зі стандартами ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безручко Д. С. Ключові особливості інформації як економічної категорії. *Ефективна економіка* № 12, 2012. URL: http://www.economy.nayka.com.ua/?op=1&z=1630 (дата звернення 10.02.2022).

2. Коваленко Ю. О. Інформаційний ресурс у контексті теорії факторів виробництва. *Економіка промисловості*. 2011. № 4. С. 148–152.

3. Терехов В. І., Одягайло Б. М. Роль інформаційного фактора у формуванні переваг на європейських конкурентних ринках. *Вчені записки університету «КРОК»*. Серія: Економіка. 2018. Вип. 4. С. 36–44.

4. Бажал Ю. М. Інформаційна економіка. Роль інформації у формуванні ринкової економіки: монографія / за заг. ред. Івана Розпутенка; Нац. акад. держ. упр. при Президентові України. Ін-т підвищення кваліфікації керівних кадрів. Київ : К.І.С., 2004. С.34–57.

5. Akerlof George A. The Market for «Lemons»: Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics.* Aug. 1970. P. 488–500.

6. George A. Akerlof «The Economics of Caste and the Rat Race and other Woeful Tales». *Quarterly journal of economics*.1976. Vol. 90(4). P. 599–617.

7. Spence M. Market Signaling: Informational Transfer in Hiring and Related Processes. Cambridge, MA: Harvard University Press. 1974. 221 p.

8. Stiglitz J. E. Equilibrium in Product Markets with Imperfect Information. The American Economic Review. Papers and Proceedings of the Ninety. First Annual Meeting of the American Economic Association. 1979. Vol. 69 (2). P. 339–345.

9. Гринів Л. С., Кічурчак М. В. Національна економіка: навч. посіб. Львів: Магнолія 2006, 2009. 464 с.

10. Мочерний С. В., Ларіна Я. С., Устенко О. А., Юрій С. І. Економічний енциклопедичний словник: у 2 т. Т.1 / За ред. С. В. Мочерного. Львів: Світ, 2005. 616 с.

11. Круш П. В. Національна економіка. Київ: Каравела: 2008. 416 с.

12. Мельник А. Ф., Васіна А. Ю., Желюк Т. Л., Попович Т. М. Національна економіка: навч. посібник / за ред. А. Ф. Мельник. Київ: Знання, 2011. 463с.

13. Котикова О. І., Горобченко О. А., Олійник Т. Г., Крилова І. Г., Мельник І. О., Купчишина О. А. Національна економіка: навчальний посібник (у рисунках, схемах і таблицях). Миколаїв: Іліон, 2020. 196 с.

14. Merriam-Webster (nd). Національна економіка. У словнику Merriam-Webster.com. URL: https://www.merriam-webster.com/dictionary/national%20economy (дата звернення 10.02.2022).

15. Дмитренко А.В. Безпека інформаційного простору контролінгової інформації при здійсненні спільної діяльності. *Економіка та суспільство*. № 56. 2023. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3033 (дата звернення 10.05.2022).

16. CIS Controls Implementation Guide for SMEs. URL: CIS-Controls-Guide-for-SMEs.pdf (cisecurity.org).

17. Конституція України. URL: http://rada.gov.ua (дата звернення 10.02.2022).

18. Шипілова Л. М. Порівняльний аналіз ключових понять і категорій основ національної безпеки України: дис. канд. політ. наук: 21.01.01; Рада національної безпеки і оборони України, Ін-т проблем національної безпеки. Київ, 2007. 178 с.

19. Барановський О. І. Філософія безпеки: монографія: у 2 т. Київ: УБС НБУ, 2014. Т.1. 831 с.

20. Ліпкан В. А. Безпекознавство. Київ: Видавництво Європейського університету, 2003. 208 с.

21. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення 10.02.2022).

22. Solow R. M. A Contribution to the Theory of Economic Growth. *Quarterly Journal of Economics*. 1956. Vol. 70. P. 64–94.

23. Domar E. Capital Expansion, Rate of Growth and Employment. *Econometrica*. 1946. Vol. 14. No. 2. P. 137–147.

24. Pareto V., Priuli F. On the Economic Phenomenon: A Reply to Benedetto Croce. *Giornale Degli Economisti e Annali Di Economia*. 2012. Vol. 71(Anno 125). No. 2/3. P. 11–28. URL: http://www.jstor.org/stable/43828050 (дата звернення 15.05.2022).

25. Ласло Е. Інформація і узгодженість в природі та «ракова пухлина» неузгодженості людського світу. *Філософія освіти*. 2012. № 1–2. С. 131–137. URL: http://nbuv.gov.ua/UJRN/PhilEdu_2012_1-2_8 (дата звернення 15.05.2022).

26. Barro R. J., Xavier S.-i-M. Economic Growth. McGraw-Hill, 1995. 540 p. URL: https://crecimientoeconomico-asiain.weebly.com/uploads/1/2/9/0/1290958/[robert_j._barro_xavier_sala-i-martin]_economic_g_z-lib.org_.pdf (дата звернення 15.05.2022).

27. Юрків Н. Я. Економічна безпека реального сектора економіки України: стратегічні пріоритети і теоретико-методологічні засади забезпечення: монографія. Львів: ПАІС, 2012. 400 с.

28. Концепція економічної безпеки України / Керівник проекту В. М. Геєць. Київ : Логос, 1999. 56 с.

29. Варналій З. С., Буркальцева Д. Д., Саєнко О. С. Економічна безпека України: проблеми та пріоритети зміцнення: монографія. Київ: Знання України, 2011. 299 с.

30. Власюк О. С. Актуальні проблеми фінансової безпеки України в умовах посткризової трансформації: монографія. Київ: НІСД, 2014. 432 с.

31. Єпіфанов А. О., Пластун О. Л., Домбровський В. С., Болгар Т. М., Ващенко О. М. Фінансова безпека підприємств і банківських установ: монографія / за заг. ред. А. О. Єпіфанова. Суми: УАБС НБУ, 2009. 295 с.

32. Жаліло Я. А. Стратегія забезпечення економічної безпеки України. Пріоритети та проблеми імплементації. Стратегія національної безпеки України в контексті досвіду світової спільноти. Київ: Сатсанга, 2001. 224 с.

33. Стратегія інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 15.05.2022).

34. Онищенко С. В., Глушко А. Д. Концептуальні засади інформаційної безпеки національної економіки в умовах діджиталізації. *Соціальна економіка*. ХНУ, 2020. Вип. 59. с. 14–24.

35. Закон України «Про Концепцію Національної програми інформатизації». URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80 (дата звернення 15.05.2022).

36. Харченко Л. С., Ліпкан Н. А., Логінов О. В. й ін. Інформаційна безпека України: глосарій / заг. ред. Р. А. Калюжний. Київ: Текст, 2004. 135 с.

37. Авраменко А. В., Гасеський В. К. Інформаційна безпека в Україні як складова національної безпеки. *Зб. наук. праць УАДУ*. Київ: Вид-во УАДУ, 2012. № 18. С. 9–18.

38. Баранов О. П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. *Вісник Національної академії державного управління при Президентові України*. 2014. № 3. С. 60–65.

39. Петрик В. М., Галамба М. В. Інформаційна безпека України: поняття, сутність та загрози. *Юридичний журнал*. 2006. №11. С.49–52.

40. Ліпкан В. А. Теоретико-методологічні засади управління у сфері національної безпеки України: монографія. Національна академія внутрішніх справ України. Київ, 2005. 350 с.

41. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навч. посіб. / за заг.ред. П. В. Мельника. Ірпінь, 2000. 304 с.

42. Данільян О. Г., Дзьобан О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: навч. посіб. Харків: ФОЛІО, 2002. 285 с.

43. Литвиненко О. В. Інформаційні впливи та операції. Теоретико-аналітичні нариси: монографія. Київ: НІСД, 2003. 240с.

44. Яровенко Г. М. Системний підхід до формалізації поняття «Інформаційна безпека». *Причорноморські економічні студії*. 2018. № 34. С. 239–244.

45. Чередниченко В. Комунікативний менеджмент в стратегії розвитку підприємства. *Економіка та суспільство*. 2022. № 42. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1688 (дата звернення 06.07.2022).

46. Щебетун І. С. Модель місцевого самоврядування: поняття, взаємозв'язок з концепцією та системою місцевого самоврядування. *Правничий часопис Донецького університету*. 2013. № 1. С. 67–74.

47. English Oxford living Dictionaries. URL: https://en.oxforddictionaries.com/definition/challenge (дата звернення 06.07.2022).

48. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. і голов. ред. В. Т. Бусел. Київ; Ірпінь: ВТФ «Перун». 2005. 1728 с.

49. Мігус І. П., Лаптєв С. М. Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання. URL: http://www.economy.nayka.com.ua/?op=1&z=821 (дата звернення 06.07.2022).

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

51. Костюк Ж. С. Поняття ризику, небезпеки та загрози як базових категорій розкриття сутності економічної безпеки підприємства. *Вісник економіки транспорту і промисловості*. 2013. № 43. С. 143–149.

52. Добринь С. В., Шкляр Д. С. Визначення сутності та взаємозв'язку понять «ризик», «небезпека» та «загроза». *Агросвіт*. 2017. № 9. С. 48–52.

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

54. Пазєєва Г. М. Комплексна діагностика в забезпеченні економічної безпеки підприємств (на матеріалах транспортно-експедиційних підприємств

України): дис. канд. екон. наук : 21.04.02. Київ: Університет економіки та права «КРОК», 2017. 291 с.

55. Бойко І. В. Дефініції «ризик», «загроза», «небезпека» як об'єкти наукових досліджень у напрямі економічної безпеки підприємства. Приазовський економічний вісник. 2017. Вип. 5(05). С. 94–98.

56. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: монографія. Львів: Арал, 2008. 384 с.

57. Калініченко Л. Л. Кадрова безпека, як провідна складова в забезпеченні економічної безпеки підприємства. Економічна безпека в умовах глобалізації світової економіки: кол. моногр. у 2 т. Дніпропетровськ: «ФОП Дробязко С.І.», 2014. Т. 2. 349 с.

58. Романчик Т. В. Небезпека, загроза, ризик: аналіз термінологічного апарату теорії економічної безпеки. *Економічний вісник НТУУ «КПІ»*. 2020. С. 257–267.

59. Семенютіна Т. В. Економічні ризики, небезпеки, загрози: сутність та взаємозв'язок. *Економічний простір*. 2012. № 68. С. 106–113.

60. Ліпкан В. А. Національна безпека України: навчальний посібник. Київ: Кондор. 2006. 552 с.

61. Попович К. В. Етимологія та розвиток категорії «безпека». *Управління розвитком*. 2013. № 21. С. 58–61.

62. Ареф'єва О. В., Кузенко Т. Б. Планування економічної безпеки підприємств. Київ: Вид-во Європ. ун-ту, 2005. 170 с.

63. Варналій З. С. Економічна безпека: навч. посіб. Київ: Знання, 2009. 647 с.

64. Zaplatynskyi V. The new concept of the most general term "danger" . International scientific conference security, extremism, terorism. 13 – 14 December 2013. Podhájska Slovak Republic. Požiarnotechnický a expertízny ústav MV SR v Bratislave, 2013. St. 267–278.

65. Барановський О. І. Фінансові кризи: передумови, наслідки і шляхи запобігання: монографія. Київ: Київ. нац. торг.екон. ун-т, 2009. 754 с.

66. Коломієць Г. М., Гузненков Ю. Г. Категорія «ризик» в дискусії сучасної економічної теорії. *Вісник Харківського національного університету ім. В.Н. Каразіна*. Серія: Економічна. 2010. № 921. С. 29–34.

67. Зубок М. І., Рубцов В. С., Яременко С. М., Гусаров В. Г. Економічна безпека суб'єктів підприємництва: навчальний посібник / За заг. ред. М.І. Зубка. Київ: Міжнародний фонд соціальної адаптації. 2012. 226 с.

68. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навч. посіб. для вищих навч. закладів / За заг. ред. П. В. Мельника. Ірпінь, 2000. 304 с.

69. Калашнікова Л. В. Співвідношення понять «невизначеність», «ризик», «виклик», «загроза», «небезпека» у контексті соціології безпеки життєдіяльності. *Науково-теоретичний альманах Грані*. 2017. № 20(5). С. 16–23.

70. Білько С. С. Сутнісна характеристика загроз інформаційній безпеці України. RECENT ADVANCES IN SCIENCE: Proceedings of the International Conference, Boston, 15–16 February 2023. Boston, 2023. P. 30–34.

71. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення 10.10.2022).

72. Стратегії кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення 10.10.2022).

73. Білько С. С., Онищенко С. В. Загрози інформаційній безпеці національної економіки. *Науковий вісник Одеського національного економічного університету.* 2022. № 11-12 (300-301). С. 50–56.

74. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дисертація…д-ра юрид. наук: 12.00.07. ДВНЗ «Ужгородський національний університет», Ужгород, 2019. 487 с.

75. Onyshchenko S., Hlushko A., Maslii O. Threats to information security of Ukraine in the conditions of digitalization. The world of science and innovation:

Proceedings of the 12th International scientific and practical conference, London, 1–3 July 2021. London, Cognum Publishing House. 2021. P. 69–73.

76. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. Київ: КНТ, 2006. 280 с.

77. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник. Київ, ООО «Д.В.К.». 2004. 508 с.

78. Шемчук В .В. Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління*. 2020. № 1(7). С. 285–296.

79. Онищенко С. В., Глушко А. Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. 2022. № 1 (84). С. 13–20.

80. ТОП 10 загроз кібербезпеці бізнесу у 2023 році. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/top-10-cybersecurity-threats-to-businesses-in-2023 (дата звернення 10.10.2022).

81. Bilko S., Onyshchenko S., Yanko A., Sivitska S. Business Information Security. *Lecture Notes in Civil Engineering*. 2023. Vol 299. P. 769–778.

82. Білько С. С. Ризики та загрози кібербезпеці бізнесу в умовах цифровізації економіки. *Modernization of science and its influence on global processes*: collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific and Theoretical Conference, Bern, 14 April 2023. Bern, 2023. P. 14–16.

83. Pradeep Nayak, Mohammed Sufiyan, Monisha N. S., Moolly Gautami Bhaskar, Mohan Raju. Review Paper on Cyber Security and Types of Cyber Attacks. *International Journal of Advanced Research in Science, Communication and Technology*. Volume 2, Issue 1. 2022. P.732–735.

84. Must-Know Ransomware Statistics. URL: https://www.fortinet.com/blog/industry-trends/ransomware-are-you-payingattention (дата звернення 10.10.2022).

85. Білько С. С. Інституційне забезпечення інформаційної безпеки України. *Економіка і регіон.* 2021. Вип. 3. С. 36–41.

86. Hlushko A., Marchyshynets O. Institutional provision of the state regulatory policy in Ukraine *Journal of Advanced Research in Law and Economics*. ASERS Publishing House. 2018. Volume 9, Issue 3. P. 941–948.

87. Commons J. R. Institutional Economics. *American Economic Review*. 1931. Vol. 21. P. 648–657. URL: http://socserv2.socsci.mcmaster.ca/econ/ugcm/3ll3/commons/ institutional.txt (дата звернення 10.10.2022).

88. Норт Д. Інституції, інституційна зміна та функціонування економіки [пер. з англ. І. Дзюб]. 2000. Київ: Основи. 198 с.

89. Ostrom E. Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge: Cambridge University Press. 1990. P. 51.

90. Гайдай Т. В. Інституція як інструмент інституційного економічного аналізу. *Економічна теорія*. 2006. № 2. С. 5–64.

91. Онищенко С. В. Інституційне забезпечення бюджетної безпеки України. *Вісник Київського національного університету імені Тараса Шевченка.* Економіка. 2016. Вип. 5. С. 31–38.

92. Veblen T. The Theory of the Leisure Class: An Economic Study of Institutions. New York: B. W. Huebsch. 1918. 401 p. URL: http://oll.libertyfund.org/titles/1657 (дата звернення 10.10.2022).

93. Hodgson G. What Are Institutions? *Voprosy Ekonomiki*. 2007 (8). P. 28–48. URL: https://doi.org/10.32609/0042-8736-2007-8-28-48 (дата звернення 10.10.2022).

94. Буркальцева Д. Д. Суб'єктно-інституційне забезпечення економічної безпеки держави. *Вісник Чернівецького торгівельно-економічного інституту.* Економічні науки. Чернівці: ЧТЕІ КНТЕУ, 2012. Вип. II (46). С. 121–127.

95. Білько С. С. Інституційно-правове забезпечення інформаційної безпеки України. *Розвиток фінансового ринку в Україні: загрози, проблеми та перспективи*: матеріали III Міжнародної наук.-практ. конф., м. Полтава, 27 жовт. 2021 р. Полтава, 2021. С. 37–38.

96. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 08.12.2022).

97. Постанова Верховної Ради України «Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України». URL: https://zakon.rada.gov.ua/rada/show/19-20/print (дата звернення 08.12.2022).

98. Закон України «Про Уповноваженого ВРУ з прав людини». URL: https://zakon.rada.gov.ua/laws/show/776/97-%D0%B2%D1%80#Text (дата звернення 08.12.2022).

99. Закон України «Про Раду національної безпеки і оборони України». URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text (дата звернення 08.12.2022).

100. Україна 2030Е – країна з розвинутою цифровою економікою. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html (дата звернення 20.02.2023).

101. Onyshchenko S., Skryl V., Hlushko A., Maslii O. Inclusive Development Index. *Lecture Notes in Civil Engineering*. 2023. Vol. 299. P. 779–790.

102. Офіційний сайт «Statista». URL: https://www.statista.com/outlook/cmo/footwear/textile-other-footwear/europe (дата звернення 20.02.2023).

103. Індекс цифрової економіки 2022: звіт європейської комісії. URL: https://nqa.gov.ua/news/indeks-cifrovoi-ekonomiki-2022-zvit-evropejskoi-komisii/ (дата звернення 20.02.2023).

104. European Commission. Digital Economy and Society Index 2022. URL: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (дата звернення 20.02.2023).

105. Український інститут майбутнього. Україна 2030Е – країна з розвинутою цифровою економікою: цифрові тренди. Виклики та можливості для України. URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html#6-2-1 (дата звернення 20.02.2023).

106. Офіційний сайт Державної служби статистики України. Валова додана вартість за видами економічної діяльності. URL:

https://www.ukrstat.gov.ua/operativ/menu/menu_u/nac_r.htm (дата звернення 20.02.2023).

107. Офіційний сайт Державної служби статистики України. Валовий внутрішній продукт (у фактичних цінах). URL: http://ukrstat.gov.ua/operativ/operativ2003/vvp/vvp_kv/vvp_kv_u/arh_vvp_kv.html (дата звернення 20.02.2023).

108. Percentage of the ICT sector in GDP. Eurostat: website. URL: https://ec.europa.eu/eurostat/databrowser/view/isoc_bde15ag/default/table?lang=en (дата звернення 20.02.2023).

109. Білько С. С. Інформаційна безпека України в умовах посилення кібератак. *Сталий розвиток: виклики та загрози в умовах воєнного стану*: матеріали Міжнародної наук.-практ. Інтернет-конференції, м. Полтава, 09 черв. 2022 р. Полтава, 2022. С. 113–115.

110. Kenneth Geers. Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO CCD COE Publications. 2015. URL: https://ccdcoe.org/library/publications/cyber-war-in-perspective-russian-aggression-against-ukraine/ (дата звернення 16.04.2023).

111. Офіційний сайт Служби безпеки України. URL: https://www.ssu.gov.ua/ua/ (дата звернення 16.04.2023)

112. Офіційний сайт Департаменту кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/ (дата звернення 16.04.2023).

113. Bilenchuk P., Malyi M. Cybersworld in the new millennium. Who are they: cybercriminals, cybercriminals, cyberterrorists? *Legal Bulletin of Ukraine*. 2019. No 39. P. 14–15.

114. Financial Stability Board. Lessons Learnt from the COVID-19 Pandemic from a Financial Stability Perspective. Interim report. July 13, 2021. URL: https://www.fsb.org/2021/07/lessons-learnt-from-the-covid-19-pandemic-from-a-financial-stability-perspective-interim-report/ (дата звернення 16.04.2023).

115. Microsoft Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. April 27, 2022. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (дата звернення 16.04.2023).

116. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management (IJM)*. 2020. Volume 11, Issue 12. P. 1709–1726.

117. Hansika Saxena and Aastha Mittal. Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022. URL: https://cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022 (дата звернення 16.04.2023).

118. Білько С. С. Інформаційна безпека національної економіки в умовах зростання викликів та загроз. *Економічна безпека: держава, регіон, підприємство*: матеріали VII Міжнародної наук.-практ. Інтернет-конференції, м. Полтава, 17 трав. 2023 р. Полтава, 2023. С. 151–154.

119. Служба безпеки України. Захист інформаційного та кіберпростору. Звіт SIEM. URL: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (дата звернення 12.05.2023).

120. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата звернення 12.05.2023).

121. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Increasing Information Protection in the Information Security Management System of the Enterprise. *Lecture Notes in Civil Engineering*. 2020. Vol. 181.P. 725–738.

122. Білько С. С. Забезпечення інформаційної безпеки бізнесу в умовах загроз воєнного стану. *Економічна безпека: держава, регіон, підприємство*: матеріали Міжнародної наук.-практ. Інтернет-конференції, м. Полтава, 29 верес. 2022 р. / Національний університет імені Юрія Кондратюка. Полтава, 2022. С. 52–55.

123. CIS Controls Implementation Guide for SMEs. URL: CIS-Controls-Guide-for-SMEs.pdf (cisecurity.org) (дата звернення 12.05.2023 р.).

124. ESET. Підсумки року: яким був 2021 рік для кібербезпеки. URL: https://eset.ua/ua/news/view/933/itogi-goda-kakim-byl-2021-dlya-kiberbezopasnosti (дата звернення 12.05.2023).

125. Білько С. С. Інформаційна безпека будівельного бізнесу в Україні. *Молодіжна наука заради миру та розвитку*: матеріали Міжнародної наук.-практ. конф., присвяченої Всесвітньому дню науки, м. Чернівці, 9–11 листоп. 2022 р. Чернівці, 2022. С. 540–543.

126. Official site the International Organization for Standardization. URL: https://www.iso.org/home.html (дата звернення 12.05.2023).

127. Onyshchenko V., Yehorycheva S., Maslii O., Yurkiv N. Impact of Innovation and Digital Technologies on the Financial Security of the State. *Lecture Notes in Civil Engineering*. 2023. P. 749–759.

128. Реверчук, Н. Й. Управління економічною безпекою підприємницьких структур: монографія. Львів: ЛБІ НБУ, 2004. 195 с.

129. Ілляшенко С. М. Економічний ризик: навч. посіб. 2-ге вид., доп., перероб. Київ: Центр навчальної літератури, 2004. 220 с.

130. Кравчук О. Я., Кравчук П. Я. Діагностика рівня та критерії оцінки корпоративної безпеки суб'єктів господарювання. *Економічні науки.* Серія «Економіка та менеджмент». Луцьк: Луцький державний технічний університет, 2004. Вип. 1. С.85–109.

131. Milov O., Voitko A., Husarova I., Domaskin O., Ivanchenko Y., Ivanchenko I., Kots H., et. al. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. *Eastern-European Journal of Enterprise Technologies*. 2019. No. 2 (9 (98)). P. 56–66.

132. Журавель М. Ю., Полозова Т. В., Стороженко О. В. Формування системи показників оцінки рівня інформаційної безпеки підприємства. *Вісник економіки транспорту і промисловості*. 2011. № 33. С. 171–177.

133. Козубцов І. М., Черноног О. О, Козубцова Л. М., Артемчук М. В., Нещерет І. Г. Вибір окремих показників оцінювання здатності функціонування системи захисту інформації і кібербезпеки інформації в інформаційно-

комунікаційних системах спеціального зв'язку. *Кібербезпека: освіта, наука, техніка*. 2022. № 4 (16). С. 19–27.

134. Ros R., Johnson L. Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, 2010. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906065 (дата звернення 30.05.2023).

135. Swanson M., Lennon, E. Security Self-Assessment Guide for Information Technology Systems, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, 2001. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151245 (дата звернення 30.05.2023).

136. ISO/IEC, Information Security Management System Part 2 : Specification for Information Security Management System, 2005. URL: https://www.tuvsud.com/en-ae/-/media/regions/in/pdf-files/auditing-and-system-certification/whitepapers/iso-27001_sa-lr.pdf (дата звернення 30.05.2023).

137. Carnegie Mellon University. SSE-CMM Model Decripton Document. SSE-CMM, 2003. URL: https://webstore.iec.ch/preview/info_isoiec21827%7Bed2.0%7Den.pdf (дата звернення 30.05.2023).

138. Carley M. Social measurement and social indicators: Issues of policy and theory. London:George Allen and Unwin. 1981. 195 с.

139. Carnegie Mellon University. The SSECMM Appraisal Method (SSAM) – Capability Maturity Model. 1999. URL: https://insights.sei.cmu.edu/library/a-description-of-the-systems-engineering-capability-maturity-model-appraisal-method-version-11/ (дата звернення 30.05.2023).

140. Nam-Seok Oh, Young-Soon Han, Chan-Wang Eom, Kyeong-Seok Oh, Bong Gyou Lee. Developing the Assessment Method for Information Security Levels. *Journal of the Korean Electronic Transactions Association*. 2013. Vol. 16. Issue 2. P. 159–169.

141. RSF. Methodology used for compiling the World Press Freedom Index. URL: https://rsf.org/en/index-methodologie-2022?year=2022&data_type=general (дата звернення 10.06.2023 р.).

142. Social Progress Imperative. URL: https://www.socialprogress.org/ (дата звернення 10.06.2023).

143. UN E-Government Survey 2022. URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022 (дата звернення 10.06.2023).

144. Global Innovation Index 2022. URL: https://www.wipo.int/global_innovation_index/en/2022/ (дата звернення 10.06.2023).

145. IMD World Competitiveness Center. World Digital Competitiveness Ranking. URL: https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/ (дата звернення 10.06.2023).

146. Bilko S. Methodical Approaches to Assessment of Information Security. *Scientific research in the modern world*: Proceedings of the 4th International scientific and practical conference, Toronto, 9–11 February 2023. Toronto, 2023. P. 505–510.

147. Новий глобальний індекс кібербезпеки – Національний індекс кіберпотужності. URL: https://www.icu-ng.org/icu-ng/novyny/novyj-globalnyj-indeks-kiberbezpeky-naczionalnyj-indeks-kiberpotuzhnosti/#_ftn1 (дата звернення 10.06.2023).

148. Офіційний сайт NCSI Project Team. URL: https://ncsi.ega.ee/country/ua/ (дата звернення 10.06.2023).

149. Комітет з питань цифрової трансформації. Кращі практики управління кібербезпекою. Оглядовий звіт. URL: https://www1.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_04.pdf (дата звернення 10.06.2023).

150. World Press Freedom Index 2021. URL: https://rsf.org/en/index?year=2021 (дата звернення 10.06.2023).

151. 2023 World Press Freedom Index – journalism threatened by fake content industry. URL: https://reliefweb.int/report/world/2023-world-press-freedom-index-journalism-threatened-fake-content-industry-enru?gad_source=1&gclid=Cj0KCQiA

6vaqBhCbARIsACF9M6lNeAy0mQOP3NxFoo3ON2aRt6-kuDpVhdieojVHw6xqoUFZtt1b-XEaAobPEALw_wcB (дата звернення 10.06.2023).

152. Міністерство соціальної політики України. Україна в рік пандемії піднялась на 17 позицій в глобальному рейтингу за індексом соціального прогресу. URL: https://www.kmu.gov.ua/news/marina-lazebna-ukrayina-v-rik-pandemiyi-pidnyalas-na-17-pozicij-v-globalnomu-rejtingu-za-indeksom-socialnogo-progresu (дата звернення дата звернення 20.06.2023).

153. Global Innovation Index2021. Tracking Innovation through the COVID-19 Crisis. URL: https://www.wipo.int/edocs/pubdocs/en/ wipo_pub_gii_2021.pdf (дата звернення 20.06.2023).

154. Social Progress Index 2021. Executive Summary. URL: https://www.socialprogress.org/static/9e62d6c031f30344f34683259839760d/2021%20Social%20Progress%20Index%20Executive%20Summary-compressed_0.pdf (дата звернення 20.06.2023).

155. Bloom B. S. Taxonomy of educational objectives: The classification of educational goals: Handbook I, cognitive domain. New York: Longman. 1956. 201 p. URL: https://eclass.uoa.gr/modules/document/file.php/PPP242/Benjamin%20S.%20Bloom%20-%20Taxonomy%20of%20Educational%20Objectives%2C%20Handbook%201_%20Cognitive%20Domain-Addison%20Wesley%20Publishing%20Company%20%281956%29.pdf (дата звернення 20.06.2023).

156. Матковський С. О., Гринькевич О. С., Вдовин М. Л., Вільчинська О. М., Марець О. Р., Сорочак О. З. Бізнес-статистика: навч. посібник. Київ: Алерта, 2016. 280 с.

157. Наказ Міністерства економічного розвитку і торгівлі України «Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України». URL: https://zakon.rada.gov.ua/rada/show/v1277731-13#Text (дата звернення 20.06.2023).

158. Павлов К. В. Застосування методів нормування показників та нечіткої логіки при оцінці рівня еколого-безпечного природокористування. Структурні зміни в економіці природокористування: теоретичні основи та прикладні

аспекти: кол. моногр. / за заг. ред. д-ра екон. наук, проф. О. М. Стрішенець. Луцьк: Вежа-Друк, 2016. С. 46–63.

159. Яровенко Г. М. Аналіз макропоказників, що характеризують рівень складових інформаційної безпеки. *Вісник Хмельницького національного університету*. Економічні науки. 2019. № 4, т. 3. С. 47–54.

160. Башинська І. О. Використання методу експертних оцінок в економічних розрахунках. *Актуальні проблеми економіки*. 2015. № 7. С. 408–412.

161. Onyshchenko S., Hlushko A., Yanko A. Role and Importance of Information Security in a Pandemic Environment. *Economics and Region*. 2020. № 2 (77). P. 103–108.

162. Білько С. С. Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку. *Науковий вісник Полісся*. 2021. № 1 (24). С. 58–77.

163. Указ Президента України «Про введення в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави». URL: https://www.president.gov.ua/documents/1632023-46149 (дата звернення 25.06.2023).

164. Інформація Міністерства економіки України щодо інтегрального показника економічної безпеки України за 2010–2020 роки. URL: https://dostup.pravda.com.ua/request/rivien_iekonomichnoyi_biezpieki_3 (дата звернення 25.06.2023).

165. Ліпкан В. А. Синергетичний і гомеостатичний підходи до системи національної безпеки. *Науковий вісник національної академії внутрішніх справ*. 2003. №2. URL: http://www.naiau.kiev.ua/tslc/pages/biblio/visnik/2003_2/_zmist_03/lipka.htm (дата звернення 25.06.2023).

166. Шевцова Г. З. Синергетичний менеджмент підприємств: монографія. Київ: НАН. України, Ін-т економіки пром-сті. 2016. 454 с.

167. Корчевська Л. О. Синергетичне управління економічною безпекою підприємства: дис…. докт. екон. наук : 08.00.04; Херсонський національний технічний університет, Херсон, 2017. 501 с.

168. Даниленко В. А. Синергетичний підхід в дослідженні стійкості економічних систем. Теоретичні та прикладні питання економіки. зб. наук. праць. 2009. Вип. 20. С. 257–265.

169. Крюкова І. Ціннісна синергетика природно-економічної взаємодії в цивілізаційному контексті. *Економіст*. 2008. № 3. С. 45–47.

170. Онищенко С. В., Білько С. С. Концепти синергетичного підходу до формування безпекоорієнтованого інформаційного середовища в Україні *Вісник Хмельницького національного університету.* 2023, № 1 (314). С. 204–211.

171. Коломієць С. В. Управління соціально-економічними системами: синергетичний підхід. *Причорноморські економічні студії*. 2020. № 51. С. 215–220.

172. Коломієць І. Ф., Пабат О. В. Загрози та виклики економічній безпеці держави: синергетичний аспект. *Регіональна економіка*. 2011. № 1. С. 7–13.

173. Цифрова економіка: тренди, ризики та соціальні детермінанти. Київ: Центр Разумкова, 2020. 274 с. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf (дата звернення 25.06.2023).

174. Onyshchenko S., Yanko A., Hlushko A., Sivitska S. Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management*. 2020. №11(12). P. 1709–1726.

175. Паршина О. А., Паршин Ю. І., Савченко Ю. В. Економічна безпека в умовах діджиталізації: сучасний стан та перспективи розвитку інформаційного суспільства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2019. № 2. С. 167–174.

176. Панченко В.А. Основні елементи системи економічної безпеки підприємства. *Ефективна економіка*. 2018. URL: http://www.economy.nayka.com.ua/pdf/3_2018/74.pdf (дата звернення 25.06.2023).

177. Козаченко Г. В. Система економічної безпеки: держава, регіон, підприємство: монографія / Козаченко Г. В. та ін. Луганськ: Промдрук, 2014. Т. 3. 336 с.

178. Ходаківський Є. І., Данилко В. К., Цал-Цалко Ю. С. Методологія наукових досліджень в парадигмі синергетики: монографія / за заг. ред. д-ра екон. наук Є. І. Ходаківського. Житомир: Житомирський державний технологічний університет, 2009. 340 с.

179. Bilko S., Onyshchenko S., Zhyvylo Y., Cherviak A. Determination of the peculiarities peculiarities of using information security systems in financial institutions in order to increase the financial security level. *Eastern-European Journal of Enterprise Technologies*. 2023. No. 5 (13 (125)). P. 65–76.

180. Живило Є., Шевченко Д., Черноног О. Типологія систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. 3(42), 37–44.

181. PCI Security Standards Council. URL: https://www.pcisecuritystandards.org/standards/ (дата звернення 01.07.2023).

182. Sarbanes-Oxley Act (SOX). URL: https://sarbanes-oxley-act.com/ (дата звернення 01.07.2023).

183. Monetary Authority of Singapore-Technology Risk Management (MAS-TRM). URL: https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines (дата звернення 01.07.2023).

184. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/ (дата звернення 01.07.2023).

185. Gramm-Leach-Bliley Financial Services Modernization Act (GLBA). URL: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf (дата звернення 01.07.2023).

186. CVE (Common Vulnerabilities and Exposures). URL: https://cve.mitre.org/ (дата звернення 01.07.2023).

187. CVSS (Common Vulnerability Scoring System). URL: https://www.first.org/cvss/ (дата звернення 01.07.2023).

188. Burp Suite. URL: https://portswigger.net/burp/ (дата звернення 01.07.2023).

189. Прокопенко Т. О. Теорія систем і системний аналіз: навч. посіб. Черкаси: ЧДТУ, 2019. 139 с.

190. Saaty Thomas L. Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors – The Analytic Hierarchy/Network Process. *Review of the Royal Academy of Exact,* Physical and Natural Sciences, Series A: Mathematics (RACSAM). 2008. 102 (2). P. 251–318.

191. Синенко М. А. Метод Сааті при прийнятті управлінських рішень на прикладі підприємства малого бізнесу. *Інтелект XXI*. 2018. № 1. С. 235–238.

192. Ткачова О. К. Метод Сааті при прийнятті управлінських рішень. *Держава та регіони*. Серія: Економіка та підприємництво. 2015. № 4. С. 92–96.

ДОДАТКИ

Додаток А

Таблиця А.1

Наукові підходи до визначення поняття «ризик»

Джерело	Визначення
Мігус І. П., Лаптєв С. М. [49]	Ризик – це об'єктивно-суб'єктивна категорія, яка пов'язана зі стохастичністю у функціонуванні будь-якої економічної системи і відображає міру або ступінь досягнення сподіваного результату (або невдачі, або відхилення від цілей).
Рудніченко Є. М. [50]	Ризик є об'єктивно-суб'єктивною категорією, що пов'язана з певною мірою невизначеності результату внаслідок прийнятого рішення, дії або обставин.
Костюк Ж. С. [51]	Умови для формування ризику створює вплив зовнішнього та внутрішнього середовища, конкуренція у підприємницькому середовищі, наявність певної свободи дій суб'єктів господарювання та суб'єктивні особливості осіб, що приймають потенційно ризикові рішення.
Добринь С. В., Шкляр Д. С. [52]	Ризик – це імовірність настання негативного впливу певних подій.
Ляшенко О. М. [53]	Ризик є як усвідомленою частиною загрози (пасивний бік), так і свідомою дією (активний бік), що може мати негативні наслідки та стати загрозою.
Пазєєва Г. М. [54]	Ризик – це відхилення від певної поставленої мети залежно від ситуації, що настала в певний час.
Бойко І. В. [55]	Ризик – це умова появи небезпеки. Після появи ризику суб'єкт потрапляє у стан небезпеки, але при цьому небезпека є поняттям можливості, вона є гіпотетичною, тобто може бути прихованою або тільки передбачуваною. Ризик – це явище зародження можливої небезпеки, за якого можливість бути убезпеченим падає, а з'являється стан небезпеки.
Васильців Т. Г. [56, с. 27]	Ризик є фактором виникнення загрози. Ризики економічної безпеки підприємництва чинять загрозу існуванню підприємництва як сфери діяльності в умовах ринкової трансформації економіки.
Калініченко Л. Л. [57, с. 105]	Ризик і загроза є формами небезпеки, які за своєю наявністю зменшують рівень безпеки.
Романчик Т. В. [58]	Економічний ризик – це імовірність втрати частини ресурсів, недоотримання доходів або поява додаткових витрат як наслідок певних видів діяльності.
Семенютіна Т. В. [59]	Економічний ризик виникає у тому випадку, коли в процесі прийняття управлінських рішень обираються альтернативні варіанти дій із імовірнісним характером очікуваних результатів (зважаючи на наявність небезпек і загроз), які є найбільш вигідними для забезпечення досягнення поставленої мети, в разі їх успішної реалізації.

Джерело: складено автором на основі зазначених джерел

Додаток Б

Таблиця Б.1

Дефініція категорії «загроза» у нормативних та наукових джерелах

Джерело	Визначення
Закон України «Про національну безпеку України» [21]	Загрози національній безпеці України – явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.
Стратегія інформаційної безпеки [33]	Інформаційна загроза – потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.
Великий тлумачний словник сучасної української мови [48, с. 386]	Неминучість/можливість виникнення будь чого прикрого, небезпечного, тяжкого для будь кого; щось, що може завдати яке-небудь зло, неприємність.
Мігус І. П., Лаптєв С. М. [49]	Загроза – це певна подія, що впливає на діяльність суб'єктів господарювання.
Рудніченко Є. М. [50]	Загроза – це наслідок небезпеки у вигляді об'єктивізованого чинника потенційно негативної дії.
Костюк Ж. С. [51]	Загроза є частиною ризику та конкретною формою небезпеки, яка виникає у разі негативного наслідку прийнятого рішення чи невиправданого ризику.
Добринь С. В., Шкляр Д. С. [52]	Загрози – це сукупність певних факторів, що можуть створювати негативний вплив на діяльність економічних суб'єктів.
Пазєєва Г. М. [54]	Загроза трактується як одна з форм небезпеки, що з'являється і розвивається на основі невизначеності.
Бойко І. В. [55]	Загроза – це реальна подія, за якої небезпека переходить зі стану можливості у реальну площину. Для виникнення загрози є активними обидва компоненти: існують як самі негативні фактори, так і можливості їх впливу на об'єкт економічної безпеки.
Васильців Т. Г. [56, с. 27]	Загроза є похідною від ризику, чинником, який виникає безпосередньо внаслідок дії ризику.
Калініченко Л. Л. [57, с. 105]	Загроза є формою небезпеки, яка своєю наявністю зменшує рівень безпеки.
Романчик Т. В. [58]	Загроза – дія, що підвищує ймовірність небезпеки, наближуючи її до конкретних негативних результатів.
Семенютіна Т. В. [59]	Загрози відображають конкретні наміри здійснення негативного впливу на діяльність суб'єкта господарювання.
Ліпкан В. А. [60]	Загроза – це 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. Загроза свідчить про існування або можливість виникнення негативних наслідків, втім не переростає у діяльність, безпосередньо спрямовану на її здійснення.

Закінчення табл. Б.1

Джерело	Визначення
Попович К. В. [61]	Загрозу – це потенційна, не проявлена, наявна в латентному, прихованому стані небезпека, яка проявляється в разі реалізації ризику.
Ареф'єва О. В. [62, с. 30]	Загроза – це сукупність умов, процесів, факторів, які перешкоджають реалізації національних економічних інтересів або створюють небезпеку для них та суб'єктів господарської діяльності. Загроза економічній безпеці являє у кінцевому підсумку певні збитки, інтегральний показник яких характеризує ступінь зниження економічного потенціалу за конкретний проміжок часу.
Варналій З .С. [63, с. 21, 64]	Загроза – конкретно визначена, безпосередня форма небезпеки чи сукупність негативних умов та чинників. Під загрозами економічній безпеці країни слід розуміти потенційні чи явні діяння, котрі ускладнюють або взагалі унеможливлюють реалізацію стратегічних національних економічних інтересів і породжують небезпеку для політичної та соціально-економічної системи, життєзабезпечення нації, національних цінностей та кожного громадянина.

Джерело: складено автором на основі зазначених джерел

Додаток В

Таблиця В.1

Структура валової доданої вартості за видами економічної діяльності за 2010 – 2022 рр., %

Види економічної діяльності	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
A. Сільське господарство, лісове господарство та рибне господарство	8,4	9,4	9,0	9,9	11,7	14,2	13,8	12,1	12,0	10,4	10,8	12,7	9,3
B. Добувна промисловість і розроблення кар'єрів	6,5	7,3	6,5	6,2	5,7	5,6	6,5	7,0	7,1	6,5	5,3	7,5	6,4
C. Переробна промисловість	14,8	13,6	14,1	12,7	14,0	14,0	14,4	14,2	13,6	12,6	11,8	12,0	8,6
D. Постачання електроенергії, газу, пари та кондиційованого повітря	3,2	3,6	3,6	3,3	3,2	3,2	3,7	3,4	3,7	3,7	3,4	3,9	5,1
E. Водопостачання; каналізація, поводження з відходами	0,8	0,7	0,6	0,5	0,5	0,5	0,4	0,4	0,4	0,4	0,4	0,4	0,3
F. Будівництво	3,7	3,5	3,2	2,9	2,7	2,3	2,3	2,6	2,7	3,1	3,3	3,2	1,4
G. Оптова та роздрібна торгівля; ремонт автотранспортних засобів і мотоциклів	16,4	17,3	16,7	16,7	16,9	16,2	15,7	16,3	15,6	15,4	16,2	15,8	14,0
H. Транспорт, складське господарство, поштова та кур'єрська діяльність	8,8	9,3	8,2	8,2	7,3	8,0	7,8	7,6	7,5	7,7	7,2	6,3	4,5
I. Тимчасове розміщування й організація харчування	1,0	1,0	0,9	0,9	0,7	0,7	0,8	0,7	0,8	1,0	0,9	1,0	0,8

Закінчення табл. В.1

Види економічної діяльності	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
J. Інформація та телекомунікації	3,4	3,4	3,5	3,7	3,8	4,3	4,4	4,4	4,6	5,3	5,8	5,5	5,2
K. Фінансова та страхова діяльність	6,3	5,1	5,0	5,0	5,1	4,0	3,2	3,3	3,3	3,4	3,6	3,4	3,2
L. Операції з нерухомим майном	6,0	6,2	6,9	7,4	7,2	7,3	7,2	6,8	6,8	7,1	7,4	6,7	5,5
M. Професійна, наукова та технічна діяльність	2,8	2,7	3,4	3,6	3,4	3,3	3,4	3,4	3,8	4,1	3,8	3,4	2,1
N. Діяльність у сфері адміністративного та допоміжного обслуговування	1,2	1,3	1,3	1,4	1,3	1,3	1,5	1,4	1,6	1,8	1,7	1,4	0,8
O. Державне управління; обов’язкове соціальне страхування	5,4	4,9	5,1	5,5	5,7	5,6	6,1	6,5	7,0	7,8	8,5	7,2	24,0
P. Освіта	5,6	5,3	6,0	6,1	5,5	4,9	4,4	5,3	5,3	5,1	5,1	5,0	4,7
Q. Охорона здоров’я та надання соціальної допомоги	4,2	3,9	4,2	3,9	3,4	3,0	2,9	3,0	2,5	2,8	3,1	2,9	2,8
R. Мистецтво, спорт, розваги та відпочинок	0,6	0,6	0,8	1,0	0,9	0,7	0,7	0,7	0,7	0,7	0,7	0,7	0,5
S, T. Надання інших видів послуг	0,9	0,9	1,0	1,1	1,0	0,9	0,8	0,9	1,0	1,1	1,0	1,0	0,8
Усього	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0

Джерело: складено автором за даними [106]

Додаток Г

Таблиця Г.1

Матриця спостережень – вихідні дані для розрахунку інтегрального показника рівня інформаційної безпеки національної економіки (місце України в міжнародних рейтингах)

Роки / Міжнародний рейтинг	2013	2014	2015	2016	2017	2018	2019	2020	2021	Кількість країн у рейтингу
Press Freedom Index	126	127	129	107	102	101	102	96	97	180
Social Progress Index	-	62	62	63	88	64	80	63	48	163
E-Government Development Index	-	87	-	62	-	82	-	69	-	193
Global Innovation Index	71	63	64	56	50	43	47	45	49	132
World Digital Competitiveness Rankings	54	50	59	59	60	58	60	58	54	63
Global Cybersecurity Index	-	-	70	59	58	54	-	79	78	175
National Cyber Security Index	-	-	-	24	26	29	28	25	24	160

Джерело: розраховано автором

Таблиця Г.2

Показники рівня інформаційної безпеки національної економіки, приведені до кількісного вигляду

Роки / Міжнародний рейтинг	2013	2014	2015	2016	2017	2018	2019	2020	2021
Press Freedom Index	0,7000	0,7056	0,7167	0,5944	0,5667	0,5611	0,5667	0,5333	0,5389
Social Progress Index	-	0,3804	0,3804	0,3865	0,5399	0,3926	0,4908	0,3865	0,2945
E-Government Development Index	-	0,4508	-	0,3212	-	0,4249	-	0,3575	-
Global Innovation Index	0,5379	0,4773	0,4848	0,4242	0,3788	0,3258	0,3561	0,3409	0,3712
World Digital Competitiveness Rankings	0,8571	0,7937	0,9365	0,9365	0,9524	0,9206	0,9524	0,9206	0,8571
Global Cybersecurity Index	-	-	0,4000	0,3371	0,2990	0,2784	-	0,4072	0,4021
National Cyber Security Index	-	-	-	0,1500	0,1625	0,1813	0,1750	0,1563	0,1500

Джерело: розраховано автором

Таблиця Г.3

Значення R^2 для різних варіантів лінії тренду при прогнозуванні величини показників рівня інформаційної безпеки національної економіки

Показник / Лінія тренду	Social Progress Index	E-Government Development Index	Global Cybersecurity Index	National Cyber Security Index
Лінійна	0,0245	0,1452	0,035	0,0104
Експоненціальна	0,044	0,1187	0,0279	0,0105
Логарифмічна	4E-0,5	0,2153	0,0007	0,0159
Поліноміальна 2 ступеня	0,511	0,2357	0,7037	0,8334
Степенева	0,0017	0,1849	0,0019	0,0163

Джерело: розраховано автором

Таблиця Г.4

Прогнозування відсутніх показників рівня інформаційної безпеки національної економіки з використанням методу згладжування

Роки / Міжнародний рейтинг	2013	2014	2015	2016	2017	2018	2019	2020	2021
Press Freedom Index	0,7000	0,7056	0,7167	0,5944	0,5667	0,5611	0,5667	0,5333	0,5389
Social Progress Index	0,3488	0,3804	0,3804	0,3865	0,5399	0,3926	0,4908	0,3865	0,2945
E-Government Development Index	0,4012	0,4508	0,3860	0,3212	0,3731	0,4249	0,3912	0,3575	0,3680
Global Innovation Index	0,5379	0,4773	0,4848	0,4242	0,3788	0,3258	0,3561	0,3409	0,3712
World Digital Competitiveness Rankings	0,8571	0,7937	0,9365	0,9365	0,9524	0,9206	0,9524	0,9206	0,8571
Global Cybersecurity Index	0,3385	0,3476	0,4000	0,3371	0,2990	0,2784	0,3428	0,4072	0,4021
National Cyber Security Index	0,1635	0,1628	0,1600	0,1500	0,1625	0,1813	0,1750	0,1563	0,1500

Джерело: розраховано автором

Таблиця Г.5

Нормовані показники рівня інформаційної безпеки національної економіки України за 2013 – 2021 роки

Роки / Міжнародний рейтинг	2013	2014	2015	2016	2017	2018	2019	2020	2021
Press Freedom Index	0,3000	0,2944	0,2833	0,4056	0,4333	0,4389	0,4333	0,4667	0,4611
Social Progress Index	0,6512	0,6196	0,6196	0,6135	0,4601	0,6074	0,5092	0,6135	0,7055
E-Government Development Index	0,5988	0,5492	0,6140	0,6788	0,6269	0,5751	0,6088	0,6425	0,6320
Global Innovation Index	0,4621	0,5227	0,5152	0,5758	0,6212	0,6742	0,6439	0,6591	0,6288
World Digital Competitiveness Rankings	0,1429	0,2063	0,0635	0,0635	0,0476	0,0794	0,0476	0,0794	0,1429
Global Cybersecurity Index	0,6615	0,6525	0,6000	0,6629	0,7010	0,7216	0,6572	0,5928	0,5979
National Cyber Security Index	0,8365	0,8372	0,8400	0,8500	0,8375	0,8188	0,8250	0,8438	0,8500

Джерело: розраховано автором

Додаток Д

Таблиця Д.1

Зведена матриця оцінок експертів щодо вагомості показників інформаційної безпеки національної економіки

Складова / Оцінка	Press Freedom Index	Social Progress Index	E-Government Development Index	Global Innovation Index	World Digital Competitiveness Rankings	Global Cybersecurity Index	National Cyber Security Index	Сума рангів (S_j)
Експерт 1	5	4	7	6	8	10	9	49
Експерт 2	6	5	8	4	7	10	9	49
Експерт 3	6	5	7	4	8	9	10	49
Експерт 4	4	6	8	5	7	9	10	49
Експерт 5	6	5	7	4	8	9	10	49
Експерт 6	4	6	7	5	8	10	9	49
Експерт 7	6	4	8	5	7	9	10	49
Експерт 8	5	6	7	4	8	9	10	49
Експерт 9	6	4	7	5	8	10	9	49
Експерт 10	4	6	8	5	7	10	9	49
Експерт 11	6	5	7	4	8	10	9	49
Експерт 12	4	6	8	5	7	10	9	49
Експерт 13	5	4	9	6	7	8	10	49
Експерт 14	5	6	8	4	7	9	10	49
Експерт 15	6	5	7	4	8	9	10	49
Експерт 16	5	4	7	6	8	9	10	49
Експерт 17	6	4	8	5	7	10	9	49
Експерт 18	5	6	7	4	8	9	10	49

Закінчення табл. Д.1

Експерт 19	6	5	8	4	7	10	9	49
Експерт 20	5	4	7	6	8	10	9	49
Сума рангів (S_i)	105	100	150	95	151	189	190	980
Відхилення від середньої	-35	-40	10	-45	11	49	50	0
Квадрат відхилення	1225	1600	100	2025	121	2401	2500	9972
Середня оцінка	5,25	5,00	7,50	4,75	7,55	9,45	9,50	49,00
Ваговий коефіцієнт	0,10	0,10	0,15	0,10	0,15	0,20	0,20	1

Джерело: розраховано автором

Додаток Е

Таблиця Е.1

Динаміка інтегрального показника рівня економічної безпеки України з урахуванням середньозважених субіндексів економічної безпеки за 2013 – 2020 рр.

Субіндекси економічної безпеки	2013	2014	2015	2016	2017	2018	2019	2020	Середнє значення	Відношення максимального значення до середнього	Відношення мінімального значення до середнього
Виробнича безпека, %	49	51	47	58	59	58	57	54	54,13	1,09	0,87
Демографічна безпека, %	46	45	43	46	40	41	39	40	42,50	1,08	0,92
Енергетична безпека, %	39	47	45	58	54	53	49	49	49,25	1,18	0,79
Зовнішньоекономічна безпека, %	29	32	33	35	36	36	40	44	35,63	1,24	0,81
Інвестиційно-інноваційна безпека, %	35	30	33	30	30	31	31	31	31,38	1,12	0,96
Макроекономічна безпека, %	39	33	30	38	37	40	45	43	38,13	1,18	0,79
Продовольча безпека, %	86	94	92	92	91	90	89	85	89,88	1,05	0,95
Соціальна безпека, %	62	57	55	56	59	59	60	59	58,38	1,06	0,94
Фінансова безпека, %	50	40	35	38	40	45	42	40	41,25	1,21	0,85
Інтегральний показник рівня економічної безпеки, %	**47**	**45**	**44**	**48**	**48**	**49**	**49**	**48**	**47,25**	**1,04**	**0,93**

Джерело: розраховано автором за даними [164]

Додаток Ж

Результати кореляційно-регресійного аналізу взаємозв'язку рівня інформаційної безпеки національної економіки та рівня розвитку економіки України, проведеного в додатку Microsoft Excel

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0,712109
R Square	0,507099
Adjusted R Square	0,424949
Standard Error	1,389435
Observations	8

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	11,91682	11,91682	6,172828	0,047514
Residual	6	11,58318	1,930529		
Total	7	23,5			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95,0%*	*Upper 95,0%*
Intercept	6,099946671	16,56987612	0,368134718	0,725411408	-34,44507959	46,64497293	-34,44507959	46,64497293
X Variable 1	0,740175435	0,29791515	2,484517608	0,047513669	0,011203325	1,469147546	0,011203325	1,469147546

RESIDUAL OUTPUT

Observation	*Y*	*Persentil*
1	44	6,25
2	45	18,75
3	47	31,25
4	48	43,75
5	48	56,25
6	48	68,75
7	49	81,25
8	49	93,75

Додаток И

Результати кореляційно-регресійного аналізу взаємозв'язку рівня інформаційної безпеки національної економіки та рівня розвитку економіки України, проведеного в додатку Microsoft Excel

SUMMARY OUTPUT

Regression Statistics	
Multiple R	0,775007058
R Square	0,600635941
Adjusted R Square	0,543583932
Standard Error	22,52463339
Observations	9

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	5341,409079	5341,409079	10,5278667	0,01416132
Residual	7	3551,513767	507,3591095		
Total	8	8892,922846			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95,0%*	*Upper 95,0%*
Intercept	-670,9676552	229,2148302	-2,927243645	0,02211084	-1212,974602	-128,960709	-1212,974602	-128,9607088
X Variable 1	13,28828492	4,095422789	3,244667427	0,01416132	3,604148874	22,97242097	3,604148874	22,97242097

RESIDUAL OUTPUT

Observation	*Y*	*Persentil*
1	31,9887	5,555555556
2	35,834	16,66666667
3	46,2102	27,77777778
4	55,8535	38,88888889
5	70,2243	50
6	84,192	61,11111111
7	94,5898	72,22222222
8	100,4325	83,33333333
9	131,9072	94,44444444

ДОДАТОК К

ДОВІДКИ ПРО ВПРОВАДЖЕННЯ

ВЕРХОВНА РАДА УКРАЇНИ

Комітет з питань гуманітарної та інформаційної політики

01008, м.Київ-8, вул. М. Грушевського, 5, тел.: 255-24-36, 255-27-41

Вих. № К-04/633 від 27.12.2022

Національний університет
«Полтавська політехніка
імені Юрія Кондратюка»

ДОВІДКА

про впровадження результатів дисертаційного дослідження
на здобуття наукового ступеня доктора філософії
Білька Станіслава Сергійовича

Науково-практичні рекомендації, викладені у дисертаційному дослідженні на здобуття наукового ступеня доктора філософії Білька Станіслава Сергійовича, щодо стратегічних напрямів державної регуляторної політики в частині формування безпекоорієнтованого інформаційного середовища в Україні можуть знайти практичне застосування у діяльності Комітету Верховної Ради України з питань гуманітарної та інформаційної політики при оновленні й удосконаленні законодавчої бази у сфері інформаційної політики та інформаційної безпеки.

Пропозиції щодо удосконалення інституційного забезпечення інформаційної безпеки України були враховані під час опрацювання проєкту Закону України «Про внесення змін до деяких законів України щодо особливостей здійснення окремих повноважень Національною радою України з питань телебачення і радіомовлення в умовах воєнного стану».

Голова Комітету **Микита ПОТУРАЄВ**

ICC UKRAINE
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

№ 482
19 12 2022

ДОВІДКА

про впровадження результатів дисертаційного дослідження на здобуття наукового ступеня доктора філософії Білька Станіслава Сергійовича

Результати дисертаційного дослідження Білька Станіслава Сергійовича досліджені на здобуття наукового ступеня доктора філософії щодо формування інформаційної безпеки національної економіки апробовані в діяльності Міжнародної торгової палати (ICC Ukraine) при вдосконаленні механізмів забезпечення інформаційної безпеки як на рівні підприємств, так і національної економіки в цілому, спрямованих на попередження і запобігання ризиків та загроз ефективному функціонуванню бізнесу й національній економіці в умовах цифровізації.

Відзначаємо також наукову та практичну цінність обґрунтованої ієрархії стратегічних орієнтирів забезпечення інформаційної безпеки національної економіки, що дозволяє визначити домінантність задекларованих напрямів реалізації Стратегії інформаційної безпеки та окреслити пріоритетні інструменти реалізації державної політики зміцнення інформаційної безпеки.

Президент,
д.е.н. професор
Академік УАН

Щелкунов В.І.

вул. Рейтарська, 19-б, м. Київ, 01030, Україна
Тел.: (044) 234 42 73, факс: (044) 270 68 29
www.iccua.org e-mail: office@iccua.org

19-b, Reytarskaya Str., Kiev, Ukraine, 01030
T. +380 44 234 42 73, F. +380 44 270 68 29
www.iccua.org e-mail: office@iccua.org

СПІЛКА ПІДПРИЄМЦІВ МАЛИХ, СЕРЕДНІХ І ПРИВАТИЗОВАНИХ ПІДПРИЄМСТВ УКРАЇНИ

Заснована в 1990р.

THE UNION OF THE ENTREPRENEURS OF SMALL, MEDIUM-SIZED AND PRIVATIZED ENTERPRISES OF UKRAINE

№ 2
07.03.2023р.

Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ДОВІДКА

про впровадження результатів дисертаційної роботи Білька Станіслава Сергійовича в практичній діяльності Спілки підприємців малих, середніх і приватизованих підприємств України

В дисертаційній роботі Білька Станіслава Сергійовича на здобуття наукового ступеня доктора філософії розглянуті актуальні питання формування інформаційної безпеки національної економіки, що передбачає, в тому числі, забезпечення безпечного і сприятливого інформаційного бізнес-середовища.

Висновки та пропозиції дисертації мають грунтовні науково-теоретичні та практичні аспекти. Зокрема, необхідно відзначити рекомендації щодо вдосконалення державної регуляторної політики формування безпекоорієнтованого інформаційного середовища в Україні та окреслені концепти забезпечення інформаційної безпеки національної економіки, що грунтуються на посиленні достовірності, конфіденційності, цілісності інформації, яка циркулює на об'єктах економічної інфраструктури в умовах зростання глобальних викликів.

Представлені висновки та рекомендації на основі проведеного дисертаційного дослідження Білька С.С. мають достатню практичну значущість. Вони були враховані при розробці Програми дій Ради та виконавчої дирекції Спілки підприємців малих, середніх і приватизованих підприємств України по реалізації Основних напрямів розвитку Спілки, а також регіональних програм розвитку підприємництва.

Перший віце-президент, генеральний директор **Вячеслав БИКОВЕЦЬ**

01054, м.Київ, Бульварно-Кудрявська, 22, оф.37
тел./факс +38(044) 486-38-82, office@smpu.kiev.ua, http://www.spmsppu.kiev.ua
IBAN UA273204780000000026008243268 в ПАТ АБ "Укргазбанк", ЄДРПОУ 20076330

ПОЛТАВСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ

ДЕПАРТАМЕНТ ЕКОНОМІЧНОГО РОЗВИТКУ, ТОРГІВЛІ ТА ЗАЛУЧЕННЯ ІНВЕСТИЦІЙ

вул. Соборності, 45, м. Полтава, 36014, факс (+38 0532)60-93-38, 56-12-43
E-mail: gue@adm-pl.gov.ua, Код ЄДРПОУ 02741539

10.05.2023 № 15 На № _____ від _____

ДОВІДКА

про впровадження результатів дисертаційного дослідження на здобуття наукового ступеня доктора філософії Білька Станіслава Сергійовича

У Департаменті економічного розвитку, торгівлі та залучення інвестицій Полтавської обласної військової адміністрації розглянуті результати дисертаційної роботи Білька Станіслава Сергійовича. Відзначаємо актуальність та своєчасність проведеного дослідження, його наукову і практичну значущість.

Вважаємо, що розробки, представлені дисертантом, є достатньо обґрунтованими і можуть бути використані у діяльності органів виконавчої влади. Висновки та пропозиції автора можуть слугувати науковим підґрунтям планування та оптимізації державної політики формування безпекоорієнтованого інформаційного середовища. Реалізація запропонованих дисертантом підходів до забезпечення інформаційної безпеки національної економіки, що ґрунтуються на виборі найбільш ефективних програмно-технологічних рішень для захисту інформації та попередження реалізації загроз, передбачає впровадження нових, більш дієвих механізмів управління національною економікою, спрямованих на посилення захищеності економічного та інформаційного середовища.

Виконувач обов'язків
директора Департаменту
економічного розвитку,
торгівлі та залучення інвестицій
обласної військової адміністрації Андрій СОРОЧИНСЬКИЙ

ДЕРЖАВНА КАЗНАЧЕЙСЬКА СЛУЖБА УКРАЇНИ
ГОЛОВНЕ УПРАВЛІННЯ
ДЕРЖАВНОЇ КАЗНАЧЕЙСЬКОЇ СЛУЖБИ УКРАЇНИ
У ПОЛТАВСЬКІЙ ОБЛАСТІ

вул.Шевченка, 1, м. Полтава, 36011, тел/факс (0532) 51-88-16, тел.51-88-14,
E-mail: office@pl.treasury.gov.ua, Код ЄДРПОУ 37959255

23.05.2023 № 201801-14/3035-2023

ДОВІДКА

про впровадження результатів дисертаційної роботи

Результати, висновки й пропозиції, що викладені в дисертаційній роботі на здобуття наукового ступеня доктора філософії Білька Станіслава Сергійовича є науково та практично значущими. Обґрунтовані дисертантом концептуальні засади інформаційної безпеки, які базуються на чіткому алгоритмі процедур забезпечення достовірності, конфіденційності, цілісності й доступності інформаційних ресурсів, а також нейтралізації потенційних та мінімізації реальних ризиків і загроз в інформаційному просторі можуть бути використані органами Державної казначейської служби України для забезпечення безпечного функціонування інформаційно-обчислювальної та внутрішньої платіжної систем Казначейства умовах воєнного стану.

Необхідно відзначити наукову та практичну цінність представлених у дослідженні формалізації взаємного впливу інформаційної та економічної безпеки держави; моделювання ефектів упливу цифровізації на досягнення таргетів захисту національних економічних інтересів, адаптивності і стійкості національної економіки; концептуальної моделі формування безпекоорієнтованого інформаційного середовища, що забезпечує захист національних економічних інтересів та безпеку національної економіки.

Начальник Олег ЧЕПУРНИЙ

МІНІСТЕРСТВО
ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА»
Першотравневий проспект, 24, м. Полтава, Україна, 36011
Тел./факс +38 (0532) 56-98-94;
+38 (0532) 60-87-30 (приймальня)
сайт: www.nupp.edu.ua
e-mail: rector@nupp.edu.ua; kanc@nupp.edu.ua
код згідно з ЄДРПОУ 02071100

MINISTRY OF
EDUCATION AND SCIENCE OF UKRAINE
NATIONAL UNIVERSITY
«YURI KONDRATYUK
POLTAVA POLYTECHNIC»
Pershotravneva Avenue 24, Poltava, 36011, Ukraine
Tel./fax +38 (0532) 56-98-94;
+38 (0532) 60-87-30 (reception)
web: www.nupp.edu.ua
e-mail: rector@nupp.edu.ua; kanc@nupp.edu.ua
USREOU code 02071100

від 03.09.2023 р. № 10-9/2005/1 на № _____ від _____ 20__ р.

Про впровадження результатів
дисертаційної роботи

ДОВІДКА

Теоретичні положення, методичні розробки, узагальнення і висновки, що містяться в дисертаційній роботі Білька Станіслава Сергійовича на здобуття наукового ступеня доктора філософії за спеціальністю 051 «Економіка», використовуються в освітньому процесі Національного університету «Полтавська політехніка імені Юрія Кондратюка», зокрема при викладанні та під час розробки робочих програм і методичних матеріалів з дисциплін: «Соціально-економічний розвиток територій та територіальних громад», «Моделювання економічних ризиків» для здобувачів вищої освіти ступеня магістр спеціальності 051 «Економіка»; «Методологія наукових досліджень у сфері безпекознавства», «Організація та управління системою фінансово-економічної безпеки підприємств», «Організація та управління інформаційно-аналітичним забезпеченням фінансово-економічної безпеки суб'єктів господарювання», «Управління захистом комерційної таємниці в банківських і фінансових установах», «Інформаційна безпека та захист інформації» для здобувачів вищої освіти ступеня магістр, а також при підготовці студентів до участі у науково-практичних конференціях та семінарах.

Проректор з науково-педагогічної
та навчальної роботи Анатолій МАРТИНЕНКО

Директор департаменту організації
навчального процесу, акредитації
та ліцензування Олег МАКСИМЕНКО