

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

Кваліфікаційна наукова
праця на правах рукопису

МАКСИМЕНКО АНДРІЙ ПЕТРОВИЧ

УДК: 338.246:351.863]:004.056

ДИСЕРТАЦІЯ

**ВПЛИВ ЦИФРОВІЗАЦІЇ НА ЗАГРОЗИ
ЕКОНОМІЧНІЙ БЕЗПЕЦІ ДЕРЖАВИ**

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

_____ Андрій МАКСИМЕНКО

(Підпис)

Науковий керівник:

Маслій Олександра Анатоліївна
кандидат економічних наук, доцент

Полтава 2025

АНОТАЦІЯ

Максименко А.П. Вплив цифровізації на загрози економічній безпеці держави. – 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, 2025.

Дисертаційна робота присвячена поглибленню теоретичних положень, удосконаленню методичних підходів та розробленню практичних рекомендацій щодо виявлення та оцінювання впливу цифровізації на загрози економічній безпеці держави.

У дисертаційній роботі розкрито сутність та роль цифровізації у трансформаційних процесах національної економіки шляхом інтеграції трьох концепцій її трактування: техніко-форматної, комерційно-оптимізаційної та технологічно-інформаційної. Здійснено теоретичне узагальнення та структурування категоріального апарату проявів цифровізації. Визначено фундаментальні властивості цифровізації та їхній вплив на формування загроз економічній безпеці держави.

Доповнено класифікацію загроз економічній безпеці держави в умовах цифровізації за рівнем походження та впливом цифрового компонента, що поглиблює розуміння джерел виникнення цифрових загроз та посилює методологічну базу їх ідентифікації. Виділено кластери загроз із максимальним рівнем впливу на економічну безпеку держави в умовах цифровізації.

Розкрито дуальний вплив цифровізації, що, з одного боку, сприяє підвищенню економічної стійкості держави, а з іншої – призводить до формування нових та трансформації існуючих загроз економічній безпеці держави. Виокремлено соціально-економічну, кібернетично-технологічну та інституційно-регуляторну сфери детермінації загроз в умовах цифровізації, що сприяє їх превентивному виявленню.

Здійснено критичний аналіз методичного інструментарію оцінювання рівня економічної безпеки держави та виявлено концептуальні недоліки його застосування в умовах цифровізації, а саме, застарілість, суперечливість нормативного забезпечення, перевантаження індикаторами, фіксованість порогових значень, обмежену гнучкість до нових умов. Доповнено методичні засади оцінювання економічної безпеки держави індикаторами інформаційно-цифрової складової на макро-, мікро- та нанорівнях національної економіки, що дозволяє враховувати вплив цифровізації на загрози економічній безпеці держави.

Проведено діагностику рівня економічної безпеки України та виявлено найбільшу концентрацію загроз у інвестиційно-інноваційній, макроекономічній, фінансовій, зовнішньоекономічній та демографічній сферах. Здійснено оцінювання домінуючого впливу цифровізації і воєнних дій на всі системоутворюючі складові економічної безпеки держави.

На основі відхилень індикаторів інформаційно-цифрової складової економічної безпеки держави від їх критичних значень виявлено реальні та потенційні загрози, спричинені цифровізацією. Визначено, що в умовах динамічного розвитку цифрових технологій, системний вплив на національну економіку мають загрози вразливості економічних суб'єктів до кібератак, залежності від імпорту цифрових технологій та низького рівня цифрової грамотності населення. Виявлено загрози структурних деформацій та надмірної концентрації ресурсів у цифровому секторі, що поглиблює дисбаланси в національній економіці.

Обґрунтовано необхідність удосконалення нормативно-правової бази та інституційного забезпечення економічної безпеки України з урахуванням європейського досвіду. Визначено передумови інтеграції України в європейський цифровий простір та концептуальні засади регуляторного удосконалення для зміцнення економічної безпеки держави в умовах цифровізації.

Спрогнозовано негативну динаміку інтегральних показників економічної безпеки за її складовими на основі ретроспективного аналізу, що є підґрунтям для побудови моделі впливу цифровізації на економічну безпеку держави. Проведено

соціологічне дослідження цифрової грамотності населення як чинника вразливості суб'єктів нанорівня національної економіки до кіберзагроз. Розроблено авторську модель впливу цифровізації на економічну безпеку держави, що відображає динаміку загроз на макро-, мікро- та нанорівнях та критичні точки впливу цифровізації.

Пріоритизовано напрями запобігання загрозам економічній безпеці держави в умовах цифровізації за допомогою використання методів RICE, «Капо» та «Value vs. Effort» на засадах розвитку інституційного забезпечення економічної безпеки та безпекоорієнтованого середовища, що є передумовою зменшення негативного впливу цифровізації на економічну безпеку держави.

Дисертація є завершеним науковим дослідженням, яке містить нові теоретичні положення, науково-методичні підходи та практичні рекомендації щодо виявлення та оцінювання впливу цифровізації на загрози економічній безпеці держави.

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

Практичне значення отриманих результатів роботи полягає в тому, що теоретичні положення, методичні підходи та висновки доведені до рівня прикладних рекомендацій, які в сукупності створюють основу для виявлення та оцінювання впливу цифровізації на загрози економічній безпеці держави. Отримані наукові результати дослідження були використані установами та організаціями у своїй діяльності при підготовці аналітичних матеріалів та здійснення заходів із забезпечення економічної безпеки України в умовах цифровізації.

Ключові слова: цифровізація, національна економіка, економічна безпека, цифрова безпека, інформаційна безпека, загрози економічній безпеці, кіберзагрози, цифрові ризики, цифрові технології, цифрова грамотність.

ABSTRACT

Maksymenko A.P. The Influence of Digitalisation on Threats to the Economic Security of the State – A qualification scientific work on the rights of a manuscript.

Dissertation for obtain the scientific degree of Doctor of Philosophy in the specialty 051 Economics (05 Social and Behavioral Sciences) – National University «Yuri Kondratyuk Poltava Polytechnic». Poltava, 2025.

The dissertation is devoted to deepening theoretical provisions, improving methodological approaches, and developing practical recommendations for identifying and assessing the impact of digitalisation on threats to the economic security of the state.

The dissertation elucidates the essence and role of digitalisation in the transformation processes of the national economy by integrating three concepts of its interpretation: technical-formal, commercial-optimisation, and technological-informational. A theoretical generalisation and structuring of the categorical apparatus of digitalisation manifestations has been carried out. The fundamental properties of digitalisation and their impact on the formation of threats to the economic security of the state are identified.

The classification of threats to the economic security of the state in the context of digitalisation is supplemented by the level of origin and influence of the digital component, which deepens the understanding of the sources of digital threats and strengthens the methodological basis for their identification. In the context of digitalisation, clusters of threats with the maximum level of impact on the economic security of the state have been identified.

The dual impact of digitalisation has been revealed, which, on the one hand, contributes to the economic stability of the state, and on the other hand, leads to the formation of new threats and the transformation of existing threats to the economic security of the state. The identification of the socio-economic, cybernetic-technological and institutional-regulatory spheres of threat determination in the context of digitalisation has been established, thus facilitating their preventive detection.

A critical analysis of the methodological tools for assessing the level of economic security of the state has been carried out, and conceptual shortcomings in their application

in the context of digitalisation have been identified, namely obsolescence, inconsistency of regulatory support, overload of indicators, fixed threshold values, and limited flexibility to new conditions. The methodological basis for assessing the economic security of the state has been supplemented with indicators of the information and digital component at the macro, micro and nano levels of the national economy. This development allows for consideration of the impact of digitalisation on threats to the economic security of the state.

A comprehensive evaluation of Ukraine's economic security has been conducted, identifying the investment and innovation, macroeconomic, financial, foreign economic and demographic domains as the primary sources of threat. An assessment has been conducted on the prevailing impact of digitalisation and military operations on the economic security of the state, with a particular focus on the system-forming components that underpin this security.

A study of the deviations of indicators within the information and digital components of the state's economic security, from their critical values, has enabled the identification of threats to both the real and potential aspects of the system in the context of digitalisation. It was determined that, in the context of the dynamic development of digital technologies, the vulnerability of economic entities to cyberattacks, dependence on imports of digital technologies, and the low level of digital literacy among the population have a systemic impact on the national economy. It has been posited that structural deformations and excessive concentration of resources in the digital sector may be conducive to the deepening of imbalances in the national economy.

The necessity to enhance the regulatory and legal framework, as well as institutional support for Ukraine's economic security, with consideration for European experience, has been substantiated. The necessary conditions for Ukraine to become integrated into the European digital space have been determined, as have the conceptual foundations for regulatory improvement that are required to strengthen the country's economic security in the context of digitalisation.

The negative dynamics of integral indicators of economic security by its components is predicted based on retrospective analysis, which is the basis for building

a model of the impact of digitalisation on the economic security of the state. A sociological study of the digital literacy of the population as a factor in the vulnerability of nano-level entities of the national economy to cyber threats has been conducted. An author has developed a model that explores the impact of digitalisation on the economic security of the state. This model reflects the dynamics of threats at the macro, micro and nano levels, as well as the critical points of impact of digitalisation.

Priority was given to the identification and prevention of threats to the economic security of the state in the context of digitalisation. The RICE, Kano and Value vs. Effort methods were utilised to develop institutional support for economic security and a security-oriented environment. It is imperative to note that this is a prerequisite for reducing the negative impact of digitalisation on the economic security of the state.

The dissertation constitutes a comprehensive scientific study, encompassing novel theoretical provisions, scientific and methodological approaches, and practical recommendations for identifying and assessing the impact of digitalisation on threats to the economic security of the state.

The scientific provisions, conclusions and recommendations presented in the defence were obtained by the author independently. The author's contributions to scientific works published in co-authorship are specified in the list of publications.

The practical significance of the results obtained lies in the fact that the theoretical provisions, methodological approaches and conclusions have been elevated to the level of applied recommendations, which, taken together, form the basis for identifying and assessing the impact of digitalisation on threats to the economic security of the state. The findings of the research were utilised by institutions and organisations in their activities, specifically in the preparation of analytical materials and the implementation of measures to ensure Ukraine's economic security within the context of digitalisation.

Keywords: digitalisation, national economy, economic security, digital security, information security, threats to economic security, cyber threats, digital risks, digital technologies, digital literacy.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Публікації у виданнях, що включені до міжнародних наукометричних баз

1. Onyshchenko V., Onyshchenko S., Maslii O., Maksymenko A. Systematization of Threats to Financial Security of Individual, Society, Business and the State in Terms of the Pandemic. *Lecture Notes in Civil Engineering*. 2023. Vol. 299. Springer, Cham. P. 749-760. DOI: https://doi.org/10.1007/978-3-031-17385-1_63. (Scopus) (0,55 друк. арк.).

Особистий внесок здобувача: визначено ризики для національної фінансової системи, пов'язані з глобалізацією та цифровізацією, які не враховуються чинними методичними рекомендаціями щодо розрахунку рівня економічної безпеки України (0,09 друк. арк.).

2. Maslii O., Maksymenko A. Digital transformation and economic deindustrialisation: impact on state financial security. *Financial and credit activity: problems of theory and practice*. 2025. Vol. 1(60). P. 401–414. DOI: <https://doi.org/10.55643/fcaptp.1.60.2025.4599> (Scopus) (1,21 друк. арк.).

Особистий внесок здобувача: проведено дослідження взаємозв'язку та дуального впливу прискореної цифрової трансформації та економічної деіндустріалізації на фінансову складову економічної безпеки держави; досліджено кореляцію між зростанням сектора інформаційних технологій і падінням промислового виробництва з використанням моделі споживання електроенергії (0,6 друк. арк.).

Публікації в наукових фахових виданнях України

3. Onyshchenko S., Maslii O., Maksymenko A. The Threats of Ukraine Financial Security: Identification and Systemization. *Economic and Region*. 2019. № 2(73). P. 73–80. DOI: [https://doi.org/10.26906/eir.2019.2\(73\).1629](https://doi.org/10.26906/eir.2019.2(73).1629) (0,6 друк. арк.).

Особистий внесок здобувача: узагальнено вплив системних загроз у фінансовій сфері на економічну безпеку держави (0,17 друк. арк.).

4. Ptashchenko L., Berezhetska T., Maksymenko A. Small Business Simplification under Digitalization and Globalization Challenges: Teal Organizations Development. *Economic and Region*. 2019. № 4(75). P. 107–112. DOI: [https://doi.org/10.26906/eir.2019.4\(75\).1858](https://doi.org/10.26906/eir.2019.4(75).1858) (0,54 друк. арк.).

Особистий внесок здобувача: виявлено тенденції до прискореної діджиталізації бізнес-процесів та впровадження інноваційних цифрових технологій ведення бізнесу (0,18 друк. арк.).

5. Маслій О., Максименко А. Ризики та загрози економічній безпеці України у цифровій сфері в умовах війни. *Ринкова економіка: сучасна теорія і практика управління*. 2022. Том 21, № 3(52). С. 176–196. DOI: [https://doi.org/10.18524/2413-9998.2022.3\(52\).275802](https://doi.org/10.18524/2413-9998.2022.3(52).275802) (0,76 друк. арк.).

Особистий внесок здобувача: розкрито дуальний вплив цифровізації економіки на економічну безпеку держави; визначено ризики і загрози економічній безпеці держави у цифровій сфері в умовах війни; проаналізовано динаміку кібератак РФ проти України як ключової загрози економічній безпеці держави у цифровій сфері (0,2 друк. арк.).

6. Максименко А. Реальні та потенційні загрози цифрової економіки в умовах війни. *Економічний простір*. 2023. № 188. С. 41-49. DOI: <https://doi.org/10.32782/2224-6282/188-7> (0,66 друк. арк.).

7. Жукова Л., Максименко А., Дерюга А. Сучасні тенденції цифрової трансформації національного господарства як чинник забезпечення економічної безпеки. *Інвестиції: практика та досвід*. 2024. № 8. С. 71–76. DOI: <https://doi.org/10.32702/2306-6814.2024.8.71> (0,56 друк. арк.).

Особистий внесок здобувача: розглянуто сучасні тенденції цифрової трансформації національного господарства як чинника забезпечення економічної безпеки; обґрунтовано методологію аналізу сучасних інноваційних трендів у сфері інформаційно-комунікаційних технологій управління (0,13 друк. арк.).

8. Маслій О., Максименко А. Діджиталізація як об'єкт економічної безпекології. *Науковий погляд: економіка та управління*. 2024. № 2(86). С. 19-26. DOI: <https://doi.org/10.32782/2521-666x/2024-86-3> (0,75 друк. арк.).

Особистий внесок здобувача: розглянуто категоріальний апарат економічної безпекології; надано сутнісно-змістовну характеристику діджиталізації як об'єкта економічної безпекології на різних рівнях соціальної ієрархії; змодельовано саморозвиваючий процес цифровізації економіки для цілей регулювання в економічній безпекології; ідентифіковано основні характеристики процесу діджиталізації, як об'єкта безпекозабезпечувальної діяльності та дослідження економічної безпекології (0,41 друк. арк.).

9. Максименко А.П. Пріоритетні напрями запобігання загрозам економічної безпеки України в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2025. Випуск 2(17). С. 128–135. DOI: <https://doi.org/10.32782/dees.17-21> (0,63 друк. арк.).

Тези доповідей на наукових конференціях

10. Маслій О., Максименко А. Оцінка ризиків фінансовій безпеці бізнесу в умовах пандемії з використанням міжнародного досвіду. *Підприємництво і торгівля: тенденції розвитку: матеріали IV Міжнародної науково-практичної конференції, 20–21 травня 2021 р. Одеса : Національний університет «Одеська політехніка», 2021. С. 297–300 (0,2 друк. арк.).*
Особистий внесок здобувача: систематизовано міжнародний досвід оцінювання ризиків фінансовій безпеці бізнесу (0,08 друк. арк.).

11. Максименко А. П. Цифровізація економіки під час пандемії COVID-19: загрози та переваги гіг-праці. *Розвиток фінансового ринку в Україні: загрози, проблеми та перспективи* : матеріали III Міжнародної науково-практичної конференції, 27 жовтня 2021 р. Полтава : НУПП, 2021. С. 65–67 (0,17 друк. арк.).

12. Маслій О., Максименко А. Неокейнсіанська модель виходу з кризи в умовах пандемії COVID-19. *Трансформація національної моделі фінансово-кредитних відносин: виклики глобалізації та регіональні аспекти* :

матеріали VI Всеукраїнської науково-практичної конференції, 24 листопада 2021 р. Ужгород : УжНУ, 2021. С. 27–28 (0,11 друк. арк.).

Особистий внесок здобувача: адаптовано заходи забезпечення економічної безпеки держави у відповідності до основних засад неокейнсіанської моделі виходу з кризи (0,05 друк. арк.).

13. Максименко А. Вплив діджиталізації на подолання мовних та комунікативних бар'єрів. *Інформація та документ у сучасному науковому дискурсі*: матеріали VII Всеукраїнської дистанційної науково-практичної конференції, 20 травня 2022 р. Івано-Франківськ : ІФНТУНГ, 2022. С. 159–164 (0,18 друк. арк.).

14. Максименко А. Цифровізація України: переваги та загрози для розвитку молодіжного бізнесу. *Підприємництво і торгівля: тенденції розвитку*: матеріали V Міжнародної науково-практичної конференції, 19–20 травня 2022 р. Одеса : Державний університет «Одеська політехніка», 2022. С. 178–180 (0,2 друк. арк.).

15. Маслій О., Максименко А. Мінімізація загроз економічній безпеці України в умовах воєнного стану з використанням резервів цифровізації. *Сталий розвиток: виклики та загрози в умовах воєнного стану*: матеріали Міжнародної науково-практичної інтернет-конференції, 9 червня 2022 р. Полтава : НУПП, 2022. С. 153–155 (0,2 друк. арк.).

Особистий внесок здобувача: проаналізовано резервний потенціал цифрового сектору економіки для підвищення рівня економічної безпеки України (0,1 друк. арк.).

16. Маслій О., Максименко А. Загрози критичній цифровій інфраструктурі в умовах війни. *Економічна безпека: держава, регіон, підприємство*: матеріали Міжнародної науково-практичної Інтернет-конференції, 29 вересня 2022 р. Полтава: НУПП, 2022. С. 144–148 (0,13 друк. арк.).

Особистий внесок здобувача: проаналізовано особливості застосування кібератак по цифровій інфраструктурі та використання цифрових технологій в умовах війни (0,09 друк. арк.).

17. Максименко А. Загрози цифровій економіці спричинені криптовалютами. *Розвиток фінансового ринку в Україні: загрози, проблеми та перспективи* : матеріали IV Міжнародної науково-практичної конференції, 25 листопада 2022 р. Полтава : НУПП, 2022. С. 45–48 (0,2 друк. арк.).

18. Максименко А., Маслій О. ChatGPT як інструмент діджиталізації економіки: переваги та загрози. *Розвиток фінансів, аудиту, бухгалтерського обліку та оподаткування: реалії часу* : матеріали II Міжнародної науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених пам'яті видатного українського вченого-економіста Сергія Ілліча Юрія, 1 лютого 2023 р. Кам'янець-Подільський : НРЗВО, 2023. С. 427–430 (0,18 друк. арк.).

Особистий внесок здобувача: здійснено аналіз переваг та недоліків впровадження інструментів діджиталізації (0,1 друк. арк.).

19. Максименко А. Цифрова адаптивність небанківської фінансової складової економічної безпеки України. *Економіка, фінанси, банківська справа та освіта: актуальні питання розвитку, досягнення та інновації* : матеріали VIII Міжнародної науково-практичної Інтернет-конференції, 6–7 квітня 2023 р. Одеса-Острава : ОНЕУ-ЄПР, 2023. С. 216–229 (0,2 друк. арк.).

20. Максименко А. Роль технологічного оптимізму у цифровізації економіки України. *Modern Scientific Views on the Development of the World Economy and International Cooperation*. October 6-7, 2023. Leipzig, Germany : Baltija Publishing. P. 95–99. DOI: <https://doi.org/10.30525/978-9934-26-356-9-27> (0,14 друк. арк.).

21. Pavlova O., Maksimenko A. Directions of modern development of the IT sphere in Ukraine. *Impact of Artificial Intelligence and Other Technologies on Sustainable Development* : Proceedings of the 1st International Scientific and Practical Internet Conference, 28–29 December 2023. Dnipro : FOP Marenichenko V.V., 2023. P. 26–29 (0,26 друк. арк.).

Особистий внесок здобувача: проаналізовано вплив цифрових технологій на розвиток сектору інформаційно-комунікаційних технологій національної економіки України (0,14 друк. арк.).

22. Maksymenko A. Transnational instruments to ensure the security of the EU digital economy. *Реформування економіки в контексті міжнародного співробітництва: механізми та стратегії* : матеріали доповідей Міжнародної науково-практичної конференції, 6–7 березня 2024 р. Львів-Торунь : Liha-Pres, 2024. С. 37–41 (0,18 друк. арк.).

23. Максименко А. Специфіка безпекових ризиків України в загальносвітових обставинах. *Наукові стратегії в контексті глобальних викликів* : матеріали I Міжнародної науково-практичної конференції, 16 квітня 2024 р. Київ : ГО «МАН», 2024. С. 74–76 (0,1 друк. арк.).

24. Максименко А. Діджиталізація медіа та дезінформація як загрози економічній безпеці держави. *Економічна безпека: держава, регіон, підприємство* : матеріали VIII Міжнародної науково-практичної конференції, 16 травня 2024 р. Полтава : НУПП, 2024. С. 146–150 (0,12 друк. арк.).

25. Максименко А. Вплив цифровізації на формування та трансформацію загроз економічній безпеці держави. *Економічна безпека: держава, регіон, підприємство* : матеріали IX Міжнародної науково-практичної конференції, 15 травня 2025 р. Полтава : НУПП, 2025. С. 204–207 (0,12 друк. арк.).

ЗМІСТ

ВСТУП.....	15
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ВПЛИВУ ЦИФРОВІЗАЦІЇ НА ЕКОНОМІЧНУ БЕЗПЕКУ ДЕРЖАВИ	24
1.1. Сутність, зміст та роль цифровізації в національній економіці.....	24
1.2. Загрози економічній безпеці держави та детермінанти їх виникнення в умовах цифровізації.....	37
1.3. Особливості впливу цифровізації на економічну безпеку держави	53
Висновки до розділу 1	72
РОЗДІЛ 2. ДІАГНОСТИКА ВПЛИВУ ЦИФРОВІЗАЦІЇ НА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ.....	74
2.1. Оцінювання рівня економічної безпеки України з урахуванням впливу цифровізації.....	74
2.2. Ідентифікація потенційних та реальних загроз економічній безпеці держави в умовах цифровізації	90
2.3. Аналіз впливу сучасних тенденцій цифровізації України на загрози її економічній безпеці	104
Висновки до розділу 2	129
РОЗДІЛ 3. СТРАТЕГІЧНІ ПРІОРИТЕТИ МІНІМІЗАЦІЇ ЗАГРОЗ ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ЦИФРОВІЗАЦІЇ	131
3.1. Розвиток інституційного забезпечення економічної безпеки України в умовах цифровізації.....	131
3.2. Моделювання впливу цифровізації на загрози економічній безпеці України	154
3.3. Пріоритетні напрями запобігання загрозам економічній безпеці держави	175
Висновки до розділу 3	194
ВИСНОВКИ	196
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	199
ДОДАТКИ	230

ВСТУП

Науковий прогрес і цифровізація кардинально змінили сучасні економічні процеси. Інтенсивне впровадження інформаційно-комунікаційних технологій, мережі Інтернет, мобільного зв'язку, соціальних мереж, онлайн-сервісів, зокрема, автоматизованих алгоритмів та віртуальних грошей, створюють можливості для підвищення конкурентоспроможності, ефективності праці, якості життя та прозорості державних послуг. Водночас, процеси цифровізації економіки супроводжуються появою принципово нових викликів і загроз економічній безпеці держави.

Останнім часом цифрові ризики набули системного характеру, поширюючись не тільки на комерційний сектор, а й на всі рівні національної економіки. Така тенденція становить загрозу не лише економічній безпеці підприємств, а й державному суверенітету та макроекономічній стабільності. Найбільш небезпечними є загрози, які стали майже неконтрольованими, а саме кібератаки та маніпулювання інформацією, які можуть порушити функціонування критичної інфраструктури національної економіки.

З огляду на ці обставини, питання інформаційної та цифрової складової економічної безпеки держави набуває особливої актуальності. Так, протидія цифровим загрозам вимагає поєднання заходів та знань в питаннях економіки, кібербезпеки, технологічних досліджень та розробки ефективної державної економічної політики. Тому, завдяки міждисциплінарному підходу можливе створення ефективних стратегій із забезпечення економічної безпеки держави з урахуванням впливу цифровізації.

Проблема забезпечення економічної безпеки держави розглядається в низці ґрунтовних працях таких науковців, як І. Бабець, З. Варналій, Т. Васильців, Т. Ганущак, О. Власюк, А. Гальчинський, В. Геєць, В. Горбулін, Я. Жаліло, С. Єгоричева, С. Онищенко та інших. У фундаментальних дослідженнях з економічної безпекології висвітлюються теоретико-методичні засади забезпечення економічної безпеки з позицій філософського та

соціологічного осмислення. Питанню цифровізації, як новітнього процесу впровадження цифрових технологій в усі сфери людського життя та його наслідків, присвячені роботи низки науковців, а саме: С. Бермана, Р. Белла, О. Грибіненко, С. Король, В. Кулик, Л. Лігоненко, С. Лукіна, М. Міхровської, Г. Назарової, В. Наместнік, І. Струтинської, Е. Столтермена, С. Федюніна, А. Фросс та інших. Так, поєднання питань забезпечення економічної безпеки та динамічних змін, зумовлених цифровізацією, призводить до актуалізації необхідності формування ефективних механізмів забезпечення інформаційної безпеки з урахуванням цифрових ризиків і загроз, що знаходить відображення в роботах окремих українських та іноземних науковців, зокрема, Дж. Блумберга, В. Бондарчук, С. Бреннера, А. Глушко, К. Краус, Д. Крейс, Т. Левіта, О. Маслій, Т. Маринич, О. Пахненко, О. Піжук, В. Пілінського, А. Пустоварова, Ю. Суботовича, А. Тернера, С. Фаругья, Ю. Худолій, К. Шиманської та інших.

Утім, попри вагомий науковий доробок з проблематики цифровізації та економічної безпеки держави, сучасні тенденції цифрового розвитку й загострення глобальних викликів обумовили появу нових форм загроз і трансформацію вже наявних. У таких умовах виникає потреба в системному опрацюванні питання виявлення та оцінювання впливу цифровізації на загрози економічній безпеці держави, що зумовило вибір теми дисертаційної роботи, обґрунтування мети та визначення завдань дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Робота відповідає пріоритетним напрямам наукових досліджень кафедри фінансів, банківського бізнесу та оподаткування Національного університету «Полтавська політехніка імені Юрія Кондратюка». А саме, в рамках виконання науково-дослідної роботи «Формування організаційно-економічних засад запобігання загрозам соціально-економічній безпеці України в умовах пандемії» (номер держреєстрації 0122U001749, 2022-2023 рр.), здійснено ґрунтовний аналіз впливу цифровізації на загрози економічній безпеці в умовах воєнних дій та розкрита діалектична сутність цифровізації. В рамках

виконання «Формування безпекоорієнтованого інформаційного середовища для підвищення економічної безпеки України у воєнний та повоєнний періоди» (номер держреєстрації 0124U000615, 2024-2025 рр.), було розкрито дуальний вплив цифровізації на національну економіку, що є водночас як джерелом інноваційного розвитку, так і фактором посилення загроз економічній безпеці.

Мета і завдання дослідження. Метою дисертаційної роботи є поглиблення теоретичних положень, удосконалення методичних підходів та розроблення практичних рекомендацій щодо виявлення та оцінювання впливу цифровізації на загрози економічній безпеці держави.

Для досягнення поставленої мети були визначені такі завдання:

- розвинути теоретичні підходи до визначення сутності цифровізації;
- удосконалити наукові підходи до класифікації загроз економічній безпеці держави з урахуванням впливу цифровізації;
- дослідити та визначити сфери детермінації загроз цифровізації економічній безпеці держави;
- поглибити науково-методичні засади оцінювання впливу цифровізації на економічну безпеку держави та ідентифікації реальних і потенційних загроз;
- здійснити моніторинг впливу сучасних тенденцій цифровізації на загрози економічній безпеці України;
- уточнити структуру інституційного забезпечення економічної безпеки України з урахуванням інтеграції у європейський цифровий простір;
- обґрунтувати науково-практичний підхід до моделювання впливу цифровізації на економічну безпеку держави;
- надати пропозиції щодо визначення пріоритетних напрямів запобігання загрозам економічній безпеці держави в умовах цифровізації.

Об'єктом дослідження є процес виявлення та оцінювання впливу загроз на економічну безпеку держави в умовах цифровізації.

Предметом дослідження є науково-методичні та практичні засади виявлення та оцінювання впливу цифровізації на загрози економічній безпеці держави.

Методи дослідження. Методологічну основу дослідження становлять базові принципи економічної теорії, актуальні концепції безпекології, теорії інституційного державного регулювання економічних процесів, а також наукові праці, присвячені управлінню національною економікою, механізмам оцінки та ідентифікації цифрових загроз.

Для досягнення поставленої мети та вирішення поставлених завдань у дисертаційній роботі використані загальнонаукові та спеціальні методи дослідження: діалектичний, аналіз і синтез, логічне узагальнення та групування, системний та синергетичний підходи, наукова абстракція, системний аналіз – при дослідженні теоретичних засад виникнення, реалізації та поширення загроз економічній безпеці держави в умовах цифровізації; економіко-статистичний, графічний та ретроспективний аналіз – при визначенні тенденцій розвитку впливу цифровізації на економічну безпеку України; порівняльний аналіз – при встановленні кореляції показників та аналізі міжнародного досвіду інституційного забезпечення економічної безпеки держави; кореляційний і регресійний аналіз – при встановленні взаємозв'язків між показниками національної економіки; нормування, згладжування та інтегрального оцінювання – при формуванні системи індикаторів та оцінюванні інформаційно-цифрової складової економічної безпеки України; системний підхід та структурно-логічний метод – при обґрунтуванні пріоритетних напрямів запобігання загрозам економічній безпеці України в умовах цифровізації. Розрахунки здійснено з використанням програмних продуктів MS Excel та Google Forms.

Інформаційну базу дослідження сформовано на основі законодавчих та нормативно-правових актів Верховної Ради України та Кабінету Міністрів України, указів Президента України, національних стратегій, Стратегії економічної безпеки ЄС, регламентах Європейської Комісії та Ради Європи,

аналітичних даних та нормативних інструментах Європейського Союзу, Міжнародних безпекових актах, даних Державної служби статистики України. Для розрахунків використано офіційні дані досліджень міжнародних організацій, зокрема UNCTAD, Міжнародного валютного фонду та аналітичної платформи Statista, звітів центральних банків країн Європи та США, наукові праці вітчизняних та іноземних науковців з питань економічної безпеки та цифровізації економіки, результати авторських розрахунків та досліджень.

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

удосконалено:

наукові підходи до визначення та оцінювання дуального впливу цифровізації на загрози економічній безпеці держави, який інтегрує три сфери детермінації (соціально-економічну, кібернетично-технологічну, інституційно-регуляторну), й слугує підґрунтям для формування стратегічних орієнтирів і заходів мінімізації загроз в умовах обмеженості ресурсного потенціалу держави та необхідності прискореної інтеграції в європейський цифровий простір;

класифікацію загроз економічній безпеці держави в умовах цифровізації шляхом їх системної структуризації за рівнем походження (національний, наднаціональний) та впливом цифрового компонента (активний, пасивний, відсутній), що, на відміну від існуючих підходів, розширює можливість розуміння природи загроз, посилює методологічну базу їх виявлення та ідентифікації впливу цифрового компонента;

науково-методичні засади ідентифікації загроз інформаційно-цифровій складовій економічної безпеки держави, що ґрунтуються на результатах критичного аналізу національного методичного інструментарію та подолання його концептуальних недоліків (застарілість, суперечливість нормативного забезпечення, перевантаження індикаторами, фіксованість порогових значень, обмежена адаптивність до глобальних змін), шляхом впровадження

індикаторів оцінювання впливу цифровізації через діяльність суб'єктів макро-, мікро- та нанорівня національної економіки, що дозволяє формувати заходи протидії загрозам економічній безпеці держави та ідентифікувати дуальний вплив цифровізації, який породжує асиметрію розвитку національної економіки;

набули подальшого розвитку:

теоретичні підходи до визначення цифровізації, що інтегрують три концепції її трактування (техніко-форматну, комерційно-оптимізаційну, технологічно-інформаційну) та систематизують структурно-логічні зв'язки між поняттями цифрової сфери з виокремленням їх фундаментальних властивостей адаптивності, мультиплікативності та циклічного розвитку. Це, на відміну від існуючих підходів, уможливорює комплексне розуміння багатовекторності проявів і наслідків цифровізації, що дозволяє здійснювати превентивну ідентифікацію потенційних загроз економічній безпеці держави;

науково-практичний підхід до моделювання впливу цифровізації на економічну безпеку держави, що, за авторською методикою, інтегрує кількісні та якісні методи аналізу, включаючи соціологічне дослідження цифрової грамотності, та відображає адаптивну динаміку впливу цифровізації на загрози економічній безпеці через діяльність суб'єктів на макро-, мікро- та нанорівні національної економіки. Це дозволило визначити критичні точки деструктивних процесів, зокрема, зростання кількості кібератак, формування структурних дисбалансів між секторами економіки, загострення конкуренції за кваліфіковані кадри в умовах ресурсного виснаження економіки та воєнних дій, що сприятиме мінімізації негативного впливу цифровізації на загрози економічній безпеці України;

науково-методичні засади визначення пріоритетних напрямів запобігання загрозам економічній безпеці держави, що, на відміну від існуючих, базуються на комплексному застосуванні методів RICE, Kano, Value vs. Effort, для системної координації інституційного, нормативно-правового та техніко-технологічного забезпечення економічної безпеки держави. Це слугує

підґрунтям оптимізації стратегічних рішень на засадах максимального охоплення суб'єктів економічної діяльності та формування безпекоорієнтованого інформаційного середовища в умовах цифровізації, що дозволяє зменшити негативний вплив загроз на економічну безпеку держави.

Практичне значення одержаних результатів полягає в тому, що основні наукові положення, методичні підходи й висновки дисертаційного дослідження доведені до рівня прикладних рекомендацій та є підґрунтям для розробки та впровадження заходів із мінімізації негативного впливу цифровізації на загрози економічній безпеці України.

Науково-практичні результати пройшли апробацію та впроваджені в діяльність Національного інституту стратегічних досліджень (довідка №293/313 від 28.04.2025 р.) при підготовці аналітичних матеріалів з обґрунтування стратегічних напрямів зміцнення економічної безпеки в умовах цифровізації; Департаментом економічного розвитку, торгівлі та залучення інвестицій Полтавської обласної військової адміністрації (довідка 01-1.08/1109 від 09.05.2025 р.) при забезпеченні економічної безпеки на регіональному рівні в умовах цифровізації; Головним управлінням Пенсійного фонду в Полтавській області (довідка №1600-0702-8/35409 від 08.05.2025 р.) при виявленні та оцінюванні впливу цифровізації на захищеність персональних даних, електронного документообігу та ідентифікації загроз економічній безпеці суб'єктів нанорівня національної економіки.

Результати дисертації впроваджено в освітній процес Національного університету «Полтавська політехніка імені Юрія Кондратюка» при викладанні лекцій з навчальних дисциплін «Теорія безпеки соціально-економічних систем», «Фінансово-економічна безпека» та при підготовці завдань для практичних занять, самостійної та індивідуальної роботи студентів з дисциплін «Організація та управління системою фінансово-економічної безпеки підприємств», «Глобальні виклики розвитку національної економіки та ЄС» (довідка №10-10/2121 від 29.05.2025).

Особистий внесок здобувача. Дисертаційна робота є завершеним та самостійно виконаним науковим дослідженням, у якому поглиблено теоретичні положення, удосконалено методичні підходи та розроблено практичні рекомендації щодо виявлення та оцінювання впливу цифровізації на загрози економічній безпеці держави. Наукові результати, отримані автором, відображені в опублікованих працях. Особистий внесок автора у результати досліджень, опублікованих у співавторстві, деталізовано у наведеному списку публікацій.

Апробація результатів дисертації. Основні положення і результати дисертації пройшли апробацію й отримали схвальну оцінку на всеукраїнських та міжнародних науково-практичних конференціях, у тому числі: VII Всеукраїнській дистанційній науково-практичній конференції «Інформація та документ у сучасному науковому дискурсі» (м. Івано-Франківськ, 2022 р.), II Міжнародній науково-практичній інтернет-конференції студентів, аспірантів та молодих вчених пам'яті видатного українського вченого-економіста Сергія Ілліча Юрія «Розвиток фінансів, аудиту, бухгалтерського обліку та оподаткування: реалії часу» (м. Кам'янець-Подільський, 2023 р.), VIII Міжнародній науково-практичній Інтернет-конференції «Економіка, фінанси, банківська справа та освіта: актуальні питання розвитку, досягнення та інновації» (Україна-Чехія, м. Одеса-Острава, 2023 р.), Міжнародній науково-практичній конференції «Сучасні наукові погляди на розвиток світової економіки та міжнародного співробітництва» (Німеччина, м. Лейпциг, 2023 р.), 1st International Scientific and Practical Internet Conference «Impact of Artificial Intelligence and Other Technologies on Sustainable Development» (м. Дніпро, 2023 р.), Міжнародній науково-практичній конференції «Реформування економіки в контексті міжнародного співробітництва: механізми та стратегії» (м. Запоріжжя, 2024 р.), I Міжнародній науково-практичній конференції «Наукові стратегії в контексті глобальних викликів» (Польща, м. Варшава, 2024 р.), IX Міжнародній

науково-практичній конференції «Економічна безпека: держава, регіон, підприємство» (м. Полтава, 2025 р.).

Публікації. Основні результати дослідження за темою дисертації опубліковано в 25 наукових працях, з яких 2 статті у виданнях, проіндексованих у базі даних Scopus, 7 статей у наукових фахових виданнях України, 16 тез доповідей у матеріалах всеукраїнських та міжнародних науково-практичних конференцій, загальний обсяг публікацій – 8,1 д.а., з яких особисто автору належить 5,07 д.а.

Структура й обсяг дисертації. Дисертаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел й додатків. Загальний обсяг роботи становить 267 сторінок, що містить 42 рисунки, 22 таблиці та 10 додатків. Список використаних джерел складається з 280 найменувань.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ВПЛИВУ ЦИФРОВІЗАЦІЇ НА ЕКОНОМІЧНУ БЕЗПЕКУ ДЕРЖАВИ

1.1. Сутність, зміст та роль цифровізації в національній економіці

Динамічний розвиток технологій, проникнення цифрових рішень в усі сфери суспільного життя, зміна підходів до споживання інформації та зростання обсягів цифрової комерції зробили цифровізацію незворотнім, домінуючим процесом в усьому світі. Під її впливом відбуваються структурні зрушення в економіці, зростає прозорість публічних послуг, виникають нові ринки та активи. Зміна характеру економічних відносин потребує переосмислення підходів до забезпечення держави в умовах цифрової трансформації.

До виникнення цифровізації призвели паралельні процеси розвитку систем військового та наукового зв'язку в поєднанні із глобалізацією світової торгівлі, що бере початок у 50-80 роках XX ст. із створенням дослідної мережі ARPANET. Першочергово вона дозволила здійснювати обмін інформацією в мережі між університетами, однак ще не мала значного економічного впливу. Загалом погоджуємося з С. Берманом та Р. Белл, що еволюцію цифровізації економіки варто поділяти на етапи відповідно до рівня проникнення технологій та поширення процесів: виникнення цифрових продуктів та інфраструктури в 1990-2000 роках, цифрову дистрибуцію та мережу в 2000-2010 роках та цифровізацію бізнес-моделей у 2010-2020 роках [1]. Утім, на нашу думку, наразі існує умовний четвертий етап, що бере початок у 2020 роках і передбачає використання великих масивів статистичних даних для аналізу та навчання штучного інтелекту.

Цифровізація є драйвером нових техніко-економічних перетворень, що призводять до глобального зростання. Зважаючи на це, обмеження її впливу

може стати причиною втрати конкурентоспроможності національної економіки та виникнення неідентифікованих загроз економічній безпеці держави. Тому гостро постає питання підтримки галузі інформаційно-комунікаційних технологій (далі – ІКТ) і пов’язаних з нею сфер та мінімізації негативного впливу цифровізації.

Враховуючи інтенсивність, новизну та актуальність явища цифровізації в нових економічних умовах, варто провести аналіз наукових підходів до визначення цього терміну (таблиця А.1, додаток А). Так, О. Абакуменко [4] та Л. Лігоненко [12] при трактуванні сутності цифровізації акцентують увагу на зміні формату передачі інформації, що, на наш погляд, виокремлює лише один аспект цього комплексного явища. При цьому, на думку О. Грибіненко [16] та Т. Оноре [20], таким аспектом є автоматизація та збільшення ефективності праці за результатами впровадження цифрових технологій на підприємстві. В свою чергу, І. Струтинська [11], О. Гудзь, С. Федюнін [19], А. Гуренко [21] та М. Міхровська [24] акцентують увагу не лише на технологічних трансформаціях, а й на зміні управлінських рішень, зокрема, комунікації з клієнтами. На наш погляд, подібний підхід є достатнім на мікрорівні, проте не включає ряд інфраструктурних, мережевих та соціальних взаємозв’язків.

Підтримуємо думку Українського інституту майбутнього [10] та С. Король [22], які визначають цифровізацію як процес впровадження цифрових технологій для взаємодії та обробки інформації, а також перехід від матеріальних явищ до цифрових.

За результатами аналізу та узагальнення наукових підходів до визначення сутності цифровізації доцільно визначити концепції її трактування техніко-форматна – визначає цифровізацію, в першу чергу, як процес перетворення інформації з аналогового формату в цифровий з метою її подальшого використання із застосуванням комп’ютерної техніки; комерційно-оптимізаційна – передбачає використання цифрових технологій з метою оптимізації бізнес-процесів для збільшення прибутку або ефективності праці, акцентуючи увагу на прозорості публічного управління або покращення якості

надання послуг, оскільки вони також зосереджені на збільшенні ефективності виробництва та впровадження автоматизації; технологічно-інформаційна – полягає у впровадженні цифрових технологій в усі сфери соціально-економічної взаємодії і призводить до потреби створення систем збору, зберігання і аналізу даних.

Отже, зважаючи на багатовекторність проявів і наслідків цифровізації, вважаємо за доцільне інтеграцію трьох концепцій її трактування, що на відміну від існуючих підходів, уможливило комплексне розуміння процесів впровадження цифрових технологій в усі сфери соціально-економічної взаємодії. Так, окрім перенесення інформації з аналогового формату в цифровий, автоматизації бізнес-процесів за допомогою новітніх технологій, цифровізація поширюється на сфери державного управління, фінансів, оборони, соціальних технологій, охорони здоров'я та інші.

Враховуючи динамічний характер та значне різноманіття проявів цифровізації, виникає необхідність визначення, ідентифікації та класифікації супутніх термінів, до яких відносимо цифрову трансформацію, цифрову економіку, цифровізацію, діджиталізацію, діджитизацію, а також: цифрові технології, цифрові рішення, цифрові послуги, цифрові гроші, цифрову демократію, цифрову інфраструктуру, цифровий переворот та цифрову революцію.

Погоджуємося з думкою М. Міхровської [24] щодо рівноцінності понять цифровізація та діджиталізація, оскільки останнє є простою транскрипцією (з англ. digitalisation – оцифрування), а його виокремлення створює додаткове непорозуміння. А також підтримуємо визначення «цифрової трансформації» як більш глобального явища, що стосується суспільних, культурних та політичних процесів, а «діджитизації» – виключно як окремого технічного процесу оцифрування інформації.

Крім того, існує категоріальна невизначеність між поняттями «цифрова революція», «цифрова трансформація» та «цифровізація». У тому чи іншому вигляді, науковці [3; 27; 29] трактують цифрову революцію як наступний

індустріальний перехід до цифрового суспільства, який характеризується масовим впровадженням цифрових технологій, зміною способів виробництва, комунікації та споживання інформації. Аналіз наведених трактувань [1-3; 25-28] свідчить, що майже у кожному з них ключовими проявами і наслідками цифровізації є цифрові інновації, які призводять до ряду радикальних економічних, соціальних, наукових змін.

Погоджуємось з Е. Столтерменом та А. Фросс [38], що цифрова трансформація є, в першу чергу, суспільним перетворенням, яке виникає внаслідок багатопланового проникнення цифрових технологій у всі аспекти повсякденного життя і призводить до значних функціональних та поведінкових змін.

Узагальнення підходів науковців до визначення цифрової революції, цифрової трансформації та, власне, цифровізації дозволяє розподілити їх на три рівні ієрархії. Так, цифровізація є причиною формування цифрової трансформації як кумулятивного прояву від активного впровадження технологій та наслідку відповідної реакції бізнесу, органів влади, інституцій і домогосподарств. А вже результатом цифрової трансформації є цифрова революція, тобто зміна суспільно-економічного устрою разом із переходом на нову фазу індустріалізації. Також, на нашу думку, зіставними за значущістю наслідками цифровізації та складовими цифрової революції є поступове формування цифрової економіки та розбудова цифрової інфраструктури.

М. Личковська обґрунтовує визначення цифрової економіки як динамічної та інноваційної економіки, основою якої є інновації та інформаційно-комунікаційні технології, які активно впроваджуються у всі форми економічної діяльності та суспільного життя, що може підвищити ефективність та конкурентоспроможність окремих підприємств, економічного та соціального життя, рівень життя населення [7]. Утім, на нашу думку, саме явище цифрової економіки лише набуває своїх виразних форм на противагу більш усталеному явищу цифрової революції.

У збірці наукових праць «The Economics of Digitization», за редакцією Ш. Грінстейна, наводиться наступне визначення цифрової інфраструктури як

комплексу матеріальних засобів та інформаційних продуктів, що забезпечують обчислювальні, телекомунікаційні та мережеві процеси функціонування цифрових технологій. Вони поділяються на опорні (жорсткі) та сервісні (м'які) [25]. Так, доповнюючи думкою Л. Мельник, опорні складаються з технічного обладнання та реальних засобів, що забезпечують дію цифрових технологій, а сервісні включають інформаційні продукти, необхідні для функціонування цифрових технологій, такі як програми, стандарти, дані, алгоритми, сервіси тощо [86]. Проведений аналіз змісту та класифікації цифрової інфраструктури дозволяє виокремити цілий перелік форм та механізмів супутніх до використання цифрових технологій як наслідок різноманіття проявів цифровізації.

Іншою складовою цифровізації є цифрова грамотність, що визначає готовність середовища до цифрових технологій. Так, аналізуючи матеріали державної платформи «Дія.Освіта» [229], можна сформулювати, що цифрова грамотність є сукупністю знань, навичок і компетенцій, необхідних для ефективного використання цифрових технологій. Вона передбачає вміння використовувати програмне забезпечення, критично оцінювати інформацію та розуміти основи кібербезпеки.

Звертаючись до питання прикладних проявів цифровізації, науковці одностайні у тому, що ними є технології, рішення та послуги. Так, цифрові технології є сукупністю практичних методів і інструментів для використання цифрових даних та передачі інформації. Своєю чергою, цифрові рішення – це комплексні програмно-технічні засоби, що самі використовують цифрові технології для вирішення операційних завдань. Тоді як цифрова послуга являє собою форму надання комерційних та публічних послуг з використанням цифрових технологій та мереж для передачі інформації.

Одним з найпоширеніших прикладів застосування цифрових технологій є цифрові гроші. Досі триває дискусія щодо сутнісного визначення та класифікації цієї категорії. Такі науковці як М. Єрмолаєва [29] та В. Помулева [32] відносять до них всі безготівкові гроші, цифрові валюти центрального

банку, віртуальні електронні гроші та цінні активи засновані на блокчейні (криптовалюти). На наш погляд, подібна класифікація є дещо узагальненою, втім, якщо не враховувати криптовалюти, відповідає цілям нашого дослідження, а в подальшому, перелік і пояснення змісту цих категорій потребує окремого глибшого дослідження.

Важливим проявом цифровізації є цифрові послуги, які дозволяють громадянам формувати запити до органів влади або отримувати інформацію за допомогою мережі Інтернет. А закладена в онлайн-сервіси інклюзивність зробила цей прояв драйвером цифровізації всього суспільства, вивівши її з виключно комерційних процесів в загальнодержавні.

Тому, спираючись на науковий доробок науковців, доцільно розкрити систему взаємозв'язків між проявами та наслідками цифровізації (рис. 1.1), що дозволить поглибити розуміння їх змісту.

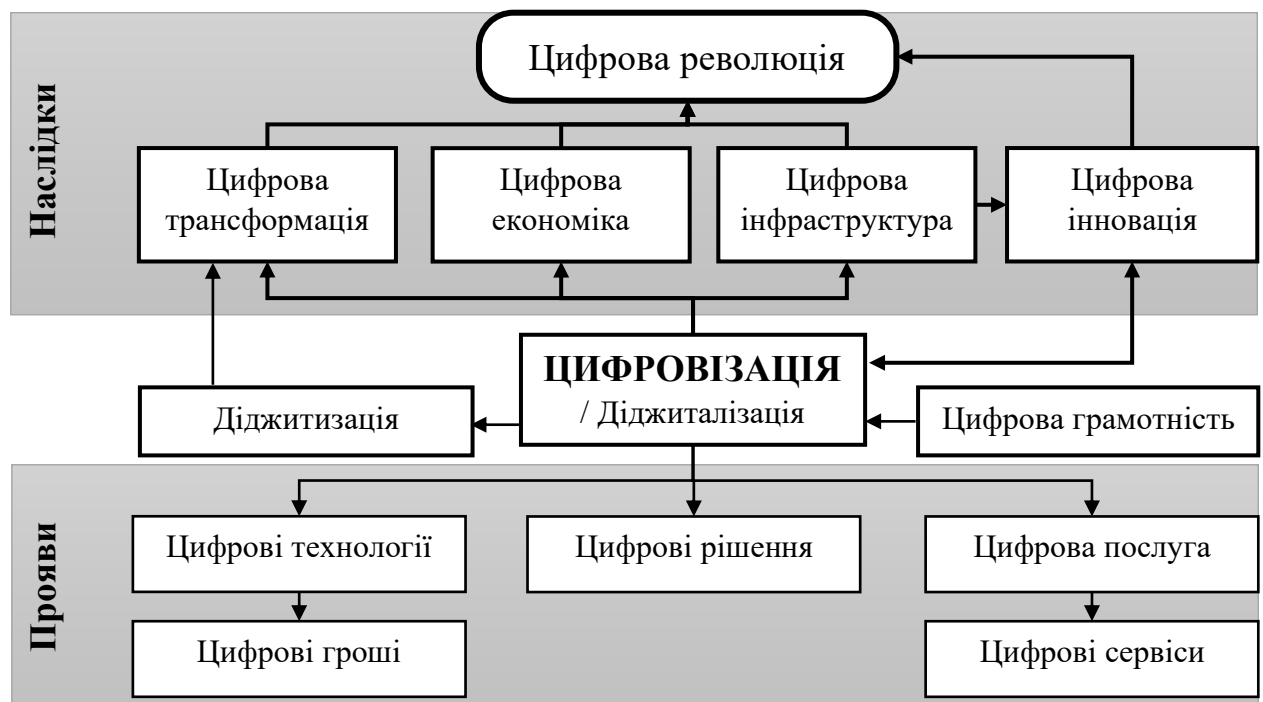


Рис. 1.1. Взаємозв'язок наслідків та проявів цифровізації

Джерело: розроблено автором

Для розуміння сутності цифровізації важливо більш докладно розкрити її прояви, що є предметом дослідження ряду науковців [1-3, 9-10]. Умовно ці

прояви можна поділити на технології (5G-зв'язок, розробки штучного інтелекту, інтернет речей), рішення (автоматизація безпеки, виробництва, дистанційне управління) та послуги (хмарні платформи, віртуальна реальність). На нашу думку найбільш звичними та значимими для сучасної економіки є наступні прояви цифровізації (табл. 1.1).

Таблиця 1.1

Визначення основних проявів цифровізації

Прояв цифровізації	Визначення
Автоматизація виробництва	Використання машинної техніки та програмного забезпечення, коли регулювання й керування виробничими процесами здійснюються без участі людини, а лише під її контролем
Електронна комерція та цифрові платформи	Купівля і продаж товарів і послуг через онлайн сервіси в Інтернеті.
Цифрові платежі	Використання електронних платіжних систем, онлайн-гаманців та криптовалют для здійснення фінансових операцій
Віртуалізація ІКТ-інфраструктури	Використання хмарних технологій, тобто серверів з віддаленим доступом, для зберігання і обробки даних.
Big Data та штучний інтелект	Застосування алгоритмів, нейромереж та великого обсягу даних для машинного навчання, аналізу даних і прийняття рішень на їх основі.
Діджитизація	Перенесення інформації з аналогової форми в цифровий формат для полегшення доступу і роботи з нею.
Сервісне програмне обслуговування	Надання підприємствами програмного обслуговування, що виходить за межі стандартного постачання запчастин.
Інтернет речей	Підключення до мережі Інтернет побутових пристроїв і датчиків, що обмінюються даними.
Цифрова демократія	Форма надання державних послуг в цифровому форматі за допомогою мережі Інтернет і також розробка технологій для реалізації волевиявлення онлайн.
Розумні міста	Концепт використання систем моніторингу для управління міською інфраструктурою.
Фінансові технології	Цифрові рішення в фінансовому секторі для здійснення та / або захисту фінансових операцій онлайн.
Віддалена робота та аутсорс	Система оформлення зайнятості, навчання, а також передача бізнесом частини власних завдань та / або процесів зовнішнім підрядникам в режимі онлайн.

Джерело: систематизовано автором на основі [1-7; 25-30]

Перелічене різноманіття проявів цифровізації дозволяє додатково актуалізувати значимість, адаптивність, поширення і суспільну затребуваність

цього явища, а також уточнити та розкрити зміст цифровізації економіки як окремого самостійного явища (рис. 1.2).

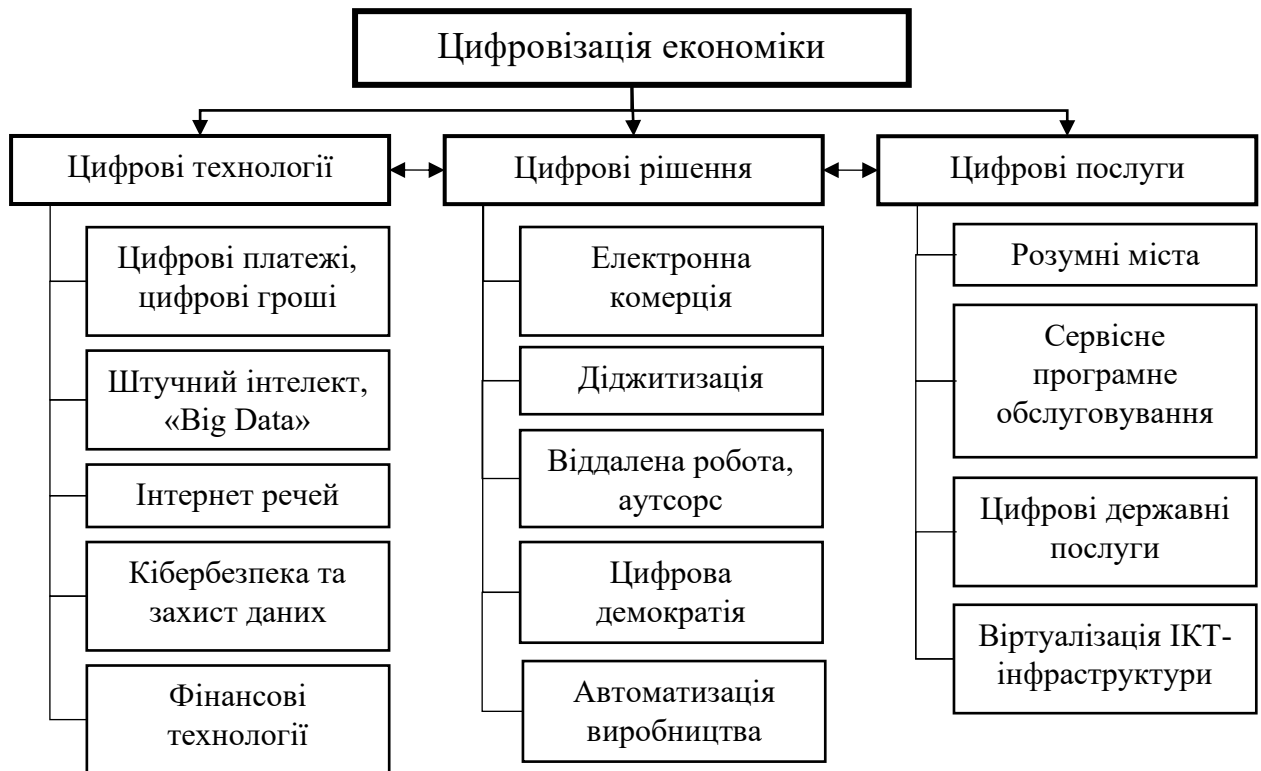


Рис. 1.2. Зміст проявів цифровізації економіки

Джерело: розроблено автором

Утім, перелік і пояснення змісту проявів цифровізації можуть суттєво відрізнятися в залежності від напрямів дослідження різних науковців, що свідчить про динамічний та стрімкий розвиток науки в питаннях цифровізації.

Зазначене різноманіття цифрових технологій, рішень та послуг внаслідок їх використання в різних секторах економіки є проявом особливих властивостей адаптивності та мультиплікативності цифровізації. Свідченням цього є також те, що внаслідок взаємодії суб'єктів на різних рівнях та секторах, поєднання рішень, послуг і технологій у відповідності та унікальних потреб, забезпечення відповідного правового поля багаторазово збільшується загальний обсяг варіативності проявів цифровізації та їх вплив.

Таким чином, поряд із каналом прямого впливу цифровізації на національну економіку, варто розглядати і канал опосередкованого впливу

(рис. 1.3), адже вона суттєво трансформує підходи до забезпечення національної безпеки, сприяє підвищенню ефективності державного управління, обороноздатності, зростанню якості життя. Разом із цим, під впливом цифровізації формуються нові загрози в інформаційному просторі, що зумовлює виникнення такої окремої складової національної безпеки, як кібербезпека.



Рис. 1.3. Канали впливу цифровізації на національну економіку

Джерело: розроблено автором

Вже зазначені вище адаптивність та мультиплікативність цифровізації також тісно пов'язані з її іншою характерною властивістю, а саме, циклічною динамікою її розвитку (рис. 1.4), де кожен етап покращення інтегрує попередні здобутки і створює умови появи та розвитку нових цифрових технологій, рішень і послуг. Це приводить до того, що попередні досягнення стають вже

традиційним рівнем технологій, таким чином збільшуючи рівень проникнення цифровізації в більш консервативні та традиційні галузі економіки.

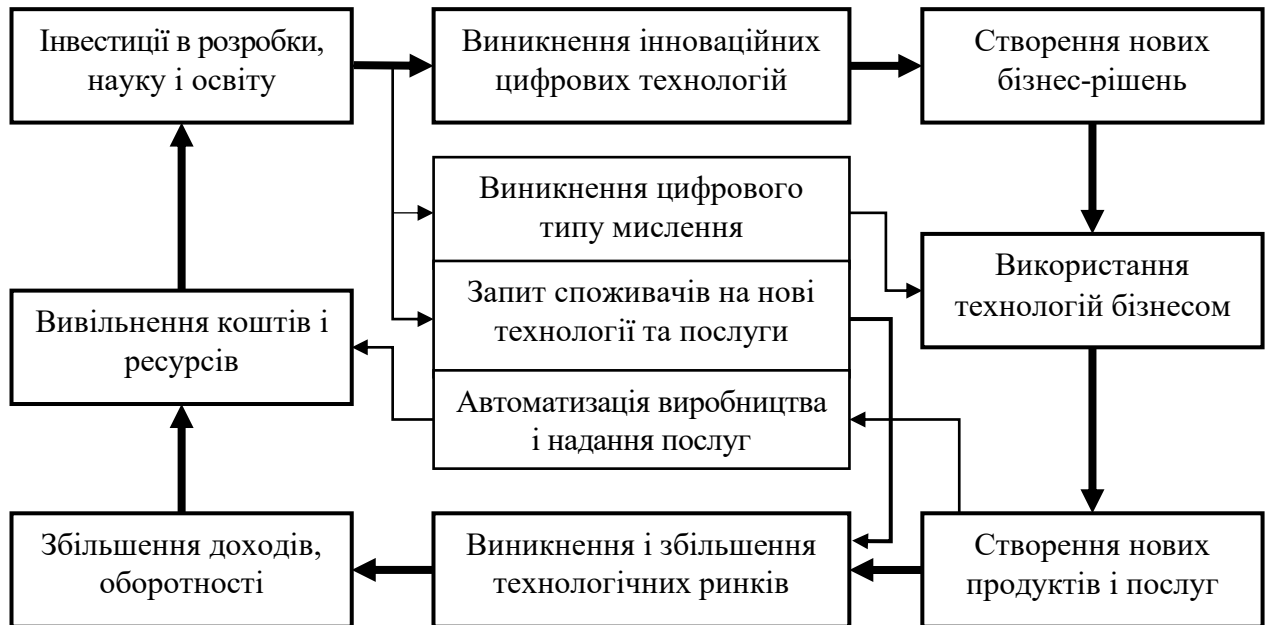


Рис. 1.4. Циклічна динаміка розвитку цифровізації економіки

Джерело: розроблено автором

Поясненням для властивості циклічної динаміки розвитку цифровізації є невідпинне зростання потужності комп'ютерів, більш відоме як «закон Мура», що дозволяє ефективніше виконувати та обчислювати складні програмні алгоритми з кожним новим поколінням цифрових технологій, точніше потужності напівпровідників. А це сприяє розвитку комплексного та продуктивного програмного забезпечення, яке створює передумови для впровадження нових технічних рішень. Аналогічні процеси відбуваються і в комерційному вимірі, вивільняючи, завдяки автоматизації та зростанню дохідності, більше ресурсів для подальшого цифрового розвитку.

Розвиваючи думку, щодо інших властивостей цифровізації економіки погоджуємося з позицією О. Гудзь, С. Федюніна [19] та О. Грибіненко [20], які визначають трансформацію, як іманентну властивість цифровізації, що містить передумови безперервної зміни об'єктів її впливу. Така точка зору є синонімічною до розуміння поняття «розвитку» в роботах Ю. Погорелова [35]

як спроможності до змін. Утім, в питанні цифровізації, варто зазначити не лише техніко-технологічні перетворення, а й звернути увагу на соціальні трансформації на всіх рівнях, в чому погоджуємося з цілим рядом науковців [11; 13; 15; 17; 22], які визначають вплив цифрових технологій, який призводить до зміни форми суспільно-владних взаємовідносин, у вигляді їх перенесення у віртуальний простір та наступній адаптації управління і комунікації.

Цілком погоджуємося з виокремленням властивості автоматизації, що збільшує ефективність та зменшує потреби в ручній праці, яку виділяють такі науковці як І. Струтинська [11], Т. Оноре [16], М. Міхровська [24] та С. Король [22]. На нашу думку, саме збільшення ефективності праці і якості обслуговування, виражені в комерційній вигоді, є першопричиною активного розвитку та перетворення цифровізації на домінуючий світовий процес.

У свою чергу, В. Куйбіда [15], О. Карпенко, В. Наместнік, М. Павлов [17] та С. Лукін [18] відзначають масштабність цифровізації. Зокрема, аналогічної позиції притримуються і С. Берман, Р. Белл [1], С. Бреннер та Д. Крейс [2], які визначають цифрову трансформацію такою, що має взаємопов'язаний вплив на суспільство, економіку, науку тощо. Таким чином, цифрові технології, рішення та послуги, формуючи власну інфраструктуру та накопичуючи великі обсяги інформації про споживачів, дозволяють науковцям та аналітикам скористатися новим рівнем масштабу аналізу статистичних даних, створюють міжнародний доступ до онлайн-платформ торгівлі і поширення контенту, нові рекламні, комерційні та бізнес-моделі розраховані на глобальну аудиторію тощо.

Крім вищенаведених фундаментальних властивостей цифровізації, пропонуємо виділяти такі властивості цифровізації: анонімність, притаманну користувачам та окремим сайтам у мережі Інтернет, і особливо в соціальних мережах, криптовалютам; мобільність, що значно зросла з доступом до цифрової інфраструктури через збільшення покриття мобільного зв'язку; персоналізація, дозволяючи алгоритмічно налаштовувати пропозиції під

конкретного споживача за його попередньою поведінкою; віртуальність, оскільки більшість технологій, рішень та послуг не існують у фізичному вираженні, а надаються виключно онлайн. Поєднання цих властивостей призводить до формування нової економічної реальності, в якій цифрові технології є основою для конкурентоспроможності та розвитку.

Все це лише підкреслює невідпинний процес цифровізації, що саморозвивається. Тому, згідно з «Економічною стратегією України 2030» Українського інституту майбутнього [10], цифровізація має відповідати завданням забезпечення кожному громадянину рівного доступу до цифрових технологій, спрямовуватися на створення переваг та слугувати інструментом економічного зростання через підвищення ефективності, продуктивності та конкурентоспроможності національної економіки, розвитку інформаційного суспільства та засобів масової інформації, орієнтуватися на співробітництво з метою інтеграції України до Європейського Союзу (далі – ЄС) і супроводжуватися підвищенням рівня довіри й безпеки.

Водночас, у Стратегії цифрового розвитку інноваційної діяльності України [59] також виокремлено серед основних пріоритетів покращення доступу населення до даних, сприяння соціальному розвитку та інклюзивності публічних послуг, утім акцентується увага і на управлінні цифровою власністю, використанні цифрових технологій для зміцнення обороноздатності, автоматизації державного управління. Зокрема, у документі визначено, що Україна має стати країною з розвиненою цифровою економікою шляхом забезпечення доступу до цифрових державних та соціальних послуг, зростання рівня життя та мінімізації корупційних ризиків, що, на нашу думку, гарантує їй визначальну роль у подальшому розвитку країни та підтверджується формуванням і впливом Міністерства цифрового розвитку України.

Аналіз стратегічного бачення цифровізації узгоджується з думкою науковців В. Куйбіди, О. Карпенко [15], В. Наместнік, М. Павлова [17] та С. Лукіна [18] про виокремлення властивості транспарентності в сприянні

боротьбі з корупцією та протидії злочинності. Проте, на нашу думку, ця характеристика поряд із властивістю анонімності у мережі свідчить про внутрішню суперечливість цифровізації.

Підсумовуючи, варто зазначити, що цифровізація є глобальною, всепроникною, незворотною, невід’ємною детермінантою сучасного економічного розвитку. Так, поєднання сукупності характерних властивостей адаптивності, анонімності, віртуальності, мультиплікативності, циклічного розвитку, масштабності, мобільності, персоналізації, транспарентності та трансформації, зокрема соціальної, стали причиною для становлення цифровізації, як домінуючого чинника в формуванні індустріальних та суспільних радикальних змін.

Так, позитивними наслідками цифровізації стали більша доступність освіти, медицини та фінансових послуг для громадян із віддалених регіонів. Доступ до онлайн-сервісів сприяв розвитку фінансової інклюзії та якості державних послуг. Удосконалення останніх, за допомогою цифрових технологій, додатково дозволило не лише підвищити їх доступність, а й знизити корупційні ризики.

Утім, цифровізація, попри свої сильні сторони, не має самодостатнього внутрішнього механізму забезпечення економічної безпеки на національному рівні. Серед усіх її характерних властивостей лише транспарентність спрямована на забезпечення стабільності, стійкості та передбачуваності економіки. Водночас, супутні до цифровізації, динамічний розвиток та структурні зміни в економіці, навпаки призводять до формування та посилення деструктивних явищ.

І хоча, проаналізовані стратегічні документи, свідчать про потенціал застосування проявів цифровізації для забезпечення економічної безпеки, вони потребують значних інвестицій та супутніх безпекових заходів. А тому виникає питання дослідження загроз економічній безпеці держави саме через призму детермінант, що дозволить визначити джерела виникнення та становлення негативного впливу цифровізації.

1.2. Загрози економічній безпеці держави та детермінанти їх виникнення в умовах цифровізації

Сучасні соціально-економічних системи функціонують в динамічних та нестабільних умовах. Такий стан середовища зумовлює їх вразливість до різноманітних факторів. Окремі явища можуть сприяти розвитку та зміцненню економіки, а інші – навпаки створювати загрози. І тому вирішальну роль у мінімізації негативного впливу цифровізації відіграє система економічної безпеки на відповідному рівні.

Так, економічна безпека на рівні держави визначається таким станом національної економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз і здатний задовольняти потреби особи, сім'ї, суспільства та держави [30].

Загалом існує безліч поглядів науковців на трактування категорії «економічна безпека», що не обмежується лише категорією стану. Так, С. Козловський [37] наводить таку класифікацію підходів до визначення економічної безпеки: як процес задоволення потреб населення та держави; як захист національних інтересів держави; як економічну стійкість та незалежність країни; як сукупність умов і факторів, які забезпечують незалежність національної економіки, її здатність до постійного оновлення і удосконалення.

А вже більш предметно вивчаючи питання підходів до визначення «економічної безпеки», Є. Франчук, І. Корчинський [40], Ю. Неустроєв [41] та О. Молдован [101] в своїх працях наголошують на категорії такого стану, при якому система може мінімізувати негативний вплив зовнішнього та внутрішнього середовища, одночасно зберігаючи можливість розвиватися.

З достатньо широкого переліку, що пропонується сучасною економічною безпекологією (табл А.2, додаток А), слід відзначити думку Я. Жаліла [235] та Т. Бондарук [239], які визначають економічну безпеку, як складну багатфакторну категорію, яка передбачає стійкість до зовнішніх

дестабілізуючих чинників та конкурентоспроможність і можливість до подальшого розвитку економіки з метою задоволення потреб суспільства.

Подібної думки у вітчизняному дискурсі дотримуються також В. Рожков [243], О. Чубукова та Т. Воронкова [244]. Вони визначають різні властивості економічної безпеки, а саме стійкість, стабільність, здатність протидіяти загрозам, повноцінну реалізацію всіх функцій та забезпеченість ресурсами на всіх рівнях національного господарства з метою задоволення потреб та захисту інтересів між суб'єктами економіки.

На нашу думку, основними складовими визначення категорії економічної безпеки держави є захищеність від зовнішніх та внутрішніх загроз при збереженні здатності до розвитку та функціонування з метою задоволення національних інтересів. Утім, варто виокремити ті підходи, що відповідають завданням нашого дослідження, а саме питанням економічної безпеки держави в умовах цифровізації. Так, Л. Акміова [42] визначає передусім її динамічну складову, що адаптується до умов часу та визначається інтегральним станом складових національної економіки.

При цьому, на думку З. Варналія, Д. Буркальцева, О. Саєнко [43] економічна безпека визначається сукупністю форм і методів узгодження різних інтересів суб'єктів економіки таким чином, що дозволяє вирішувати конфлікти з найменшими витратами та з використанням найменш руйнівного для економіки способу. Цей підхід, на нашу думку, набуває особливої актуальності в умовах цифровізації, заважаючи на її характерні властивості.

Вивчення значного наукового доробку в сфері дослідження економічної безпеки дозволяє зробити певні теоретичні припущення. Так, визначення економічної безпеки держави в умовах цифровізації – є сукупністю форм і методів управління трансформаційними процесами з найменшими витратами та з використанням найменш руйнівного для економіки способу. Тобто при забезпеченні стійкості, стабільності, здатності протидіяти внутрішнім і зовнішнім загрозам, повноцінної реалізації всіх складових економіки на всіх рівнях національного господарства.

Отже, діяльність окремих елементів будь-якої системи відображають її загальний стан. А хаос та вплив деструктивних явищ навпаки заважають системі функціонувати, що в подальшому призводить до виникнення та подальшого поширення нових негативних явищ.

Тому, на нашу думку, важливим питанням економічної безпеки держави є визначення терміну «загроза». На жаль, це поняття достатньо тривалий час є об'єктом вивчення вітчизняної безпекології і досі, досить часто, в наукових доробках зустрічається використання альтернативних понять, як то «ризик», «небезпека» та «загроза» на позначення деструктивних явищ. Незважаючи на це, донині в наукових колах триває активна дискусія щодо визначення суті зазначених понять (табл. А.3, додаток А).

Тому, здійснюючи аналіз наведених визначень з погляду цифровізації, трактування загроз економічній безпеці, пропоновані Т. Ганущак [33], І. Мігус [249] та Н. Цікановською [251], є дещо узагальненими, такими, що не розкривають глибоку сутність категорії. На противагу, В. Мунтіян [238], В. Предбродський [247], І. Плетнікова [252], М. Камлик [253], надмірно акцентують увагу на шкоді від деструктивних явищ, нанесеній інтересам суб'єкта безпеки, без врахування складніших наслідків, які не можна порахувати у вигляді збитків.

При цьому, на думку З. Варналія, Д. Буркальцева, О. Саєнко [43], а також О. Мійняло, Ю. Уманціва [245], І. Дідович [248], О. Маслій [204] під загрозами економічній безпеці національної економіки варто розуміти такі явища, що не лише завдають шкоди, а й ускладнюють або унеможливлюють реалізацію національних економічних інтересів та створюють небезпеку для цінностей всіх суб'єктів, що також подібно до визначення в Законі України «Про національну безпеку» від 2018 р. [31].

Здійснюючи узагальнення підходів науковців до трактування поняття «загроз економічній безпеці держави» вважаємо за доцільне її визначення як явищ, тенденцій і чинників, котрі унеможливлюють чи ускладнюють або потенційно можуть унеможливити чи ускладнити реалізацію національних

економічних інтересів та збереження функціональних властивостей національної економіки.

У питанні дослідження цифровізації, важливо зауважити, що загрози є органічним, невід’ємним та невідворотнім наслідком структурних змін від впровадження та застосування нових технологій, рішень і послуг. Утім, їхня потенційна наявність не визначає впливу цифровізації. Так, ефективна система економічної безпеки держави має слугувати фільтром, відсіюючи несприятливі явища, а ніяк не бар’єром, що стоїть на заваді соціально-економічним трансформаціям та технологічним досягненням.

Тому створення механізму забезпечення економічної безпеки держави має починатися з конкретної формалізації чинників, що призводять до небезпеки. Такими подіями чи явищами різні науковці визначають близькі категорії «загрози», «ризик» та «виклики» в різній послідовності взаємозв’язків. У наукових працях, присвячених цьому питанню, В. Мунтіян [238], Н. Цікановська [251], О. Дмитрова [89], О. Маслій [204] наводять різні підходи до категоризації шляхом етимологічного, структурного та логічного розборів.

Утім, у межах безпекологічного дослідження погоджуємося з позицією О. Маслій [204] та подальшим науковим доробком А. Черв’як [254] та С. Білька [255], що встановлюють послідовність взаємозв’язків як «виклик-ризик-загроза-небезпека». Тобто категорії «виклик» та «ризик» знаходяться у відносно безпечних межах, лише передуючи більш негативним категоріям «загроза» та «небезпека», які вже є результатом неправильних рішень суб’єктів на відповідному рівні.

Таким чином, вважаємо, що загрози є першочерговим об’єктом безпекозабезпечувальної діяльності, а також елементом цифровізації зокрема, внаслідок її характерних властивостей масштабування та адаптивності. Тому і загрози, і заходи протидії їм є елементами системи забезпечення економічної безпеки держави в умовах цифровізації (рис. 1.5).

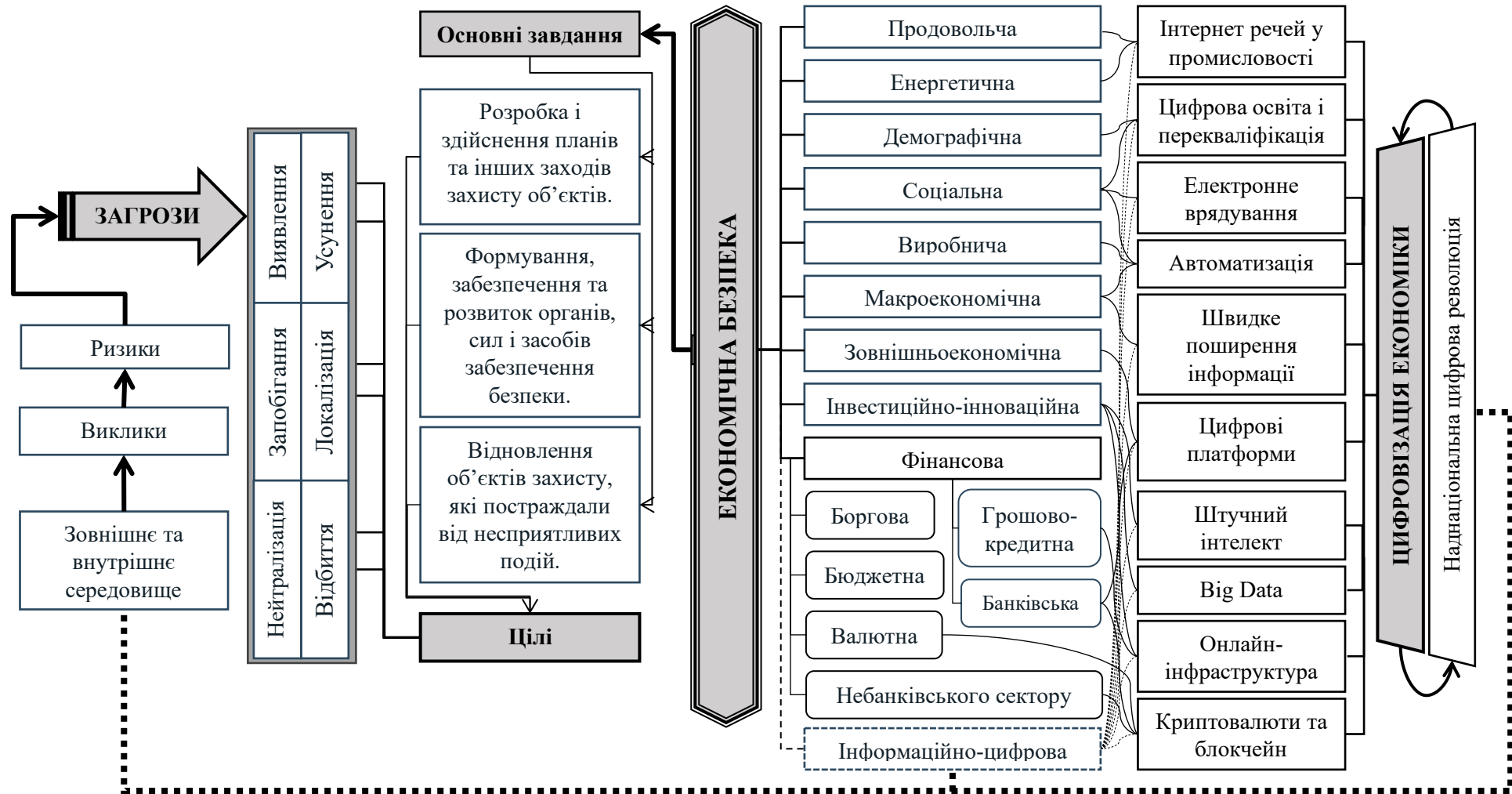


Рис. 1.5. Модель забезпечення економічної безпеки держави в умовах цифровізації

Джерело: систематизовано автором на основі джерел [30; 33-39; 43; 88]

Представлена вище комплексна модель забезпечення економічної безпеки держави в умовах цифровізації насамперед актуалізує питання визначення та класифікації загроз з урахуванням трансформаційних процесів. Передусім науковці одностайні в поділі загроз на внутрішні та зовнішні, потенційні та реальні. Втім, у подальшому, різні науковці визначають різні категорії та кластери у відповідності до предмету дослідження.

Перш за все, О. Пугач [45] додатково акцентує на класифікації за ступенем небезпеки (особливо небезпечні, звичайного характеру небезпеки та потенційні), в залежності від прояву джерела загрози (з традиційною та з нетрадиційною формою реалізації), за раптовістю настання (прогнозовані, миттєві та раптові), за періодичністю (системні, періодичні та разові), від часу прояву деструктивного впливу (актуальні та перспективні), за терміном дії (постійні та тимчасові) за механізмом впливу (прямі та непрямі) та за масштабом впливу (загальнонаціональні, локальні та індивідуальні).

Варто також відмітити і думку І. Кузнецової та О. Кюне [53], що також виділяють тривалість впливу, систематичність прояву, прогнозованість та масштаб, утім доповнюють наступним переліком: за ступенем імовірності (реальні та приховані) за величиною втрат (несуттєві, істотні, значні, катастрофічні), за ступенем керованості (керовані та некеровані), сферою виникнення загроз (правові, ринкові, політичні, екологічні, соціальні, науково-технічні, технологічні, демографічні), та за можливістю нейтралізації (частково піддаються, зовсім не піддаються).

Продовжуючи розгляд науковців, О. Кириченко [54] виділяє складові, масштаб впливу, можливість реалізації, тривалість дії та механізм впливу, втім, а ще доповнює класифікацію: за характером впливу (системні, локальні та реакційні), за ступенем небезпеки (особливо небезпечні та безпечні), та за ступенем реалізації (нереалізовані, частково реалізовані, реалізовані).

Спираючись на науковий доробок вітчизняних авторів, варто здійснити багатокритеріальну класифікацію, що якнайкраще відповідатиме предмету дослідження. Тобто вона має розкривати природу впливу цифровізації на загрози

економічній безпеці держави, джерела їх походження, та сприяти їх кращій ідентифікації. Загалом, традиційний поділ на внутрішні та зовнішні, а також на реальні та потенційні залишається актуальним в незалежності від досліджуваного питання.

Внутрішні загрози економічній безпеці держави безпосередньо пов'язані з особливостями функціонування економіки в умовах цифровізації. До їх числа слід відносити недоліки законодавчої бази, розширення та цифровізація тіньового сектору, високий рівень монополізації, криміналізація, поширення корупційних схем та організованої злочинності. Зовнішні загрози визначаються глобальними економічними чинниками та міжнародними зв'язками. До них належать недостатній розвиток інфраструктури, зокрема цифрової, трудова міграція, низька інвестиційна привабливість, поширення транскордонної кіберзлочинності, залежність від імпорту цифрових технологій.

Так, реальні загрози це ті, що існують у поточний момент та перешкоджають реалізації національних економічних інтересів, наприклад, як кібератаки, витоки даних, збій автоматизованих систем, дезінформація. Тоді як при потенційних загрозах існує лише ймовірність завдання певної шкоди економічній безпеці, зокрема, ними є падіння потенціалу сектору традиційного виробництва, структурні та соціальні деформації.

На нашу думку, актуальним в умовах цифровізації залишається класифікація за терміном дії загрози та моментом існування, зважаючи на описану динамічність середовища. Поділ за ступенем очевидності та віддаленістю, зважаючи, що цифровізація та супутні технології є новими і складно передбачити довгострокові наслідки. Не менш важливими є визначення загроз за об'єктивністю їх існування, зважаючи на консервативне ставлення до технологій, а також за можливістю впливу на загрози та джерела їх виникнення: на керовані, щодо захисту та поширення цифрової інфраструктури, та некеровані, які не піддаються впливу на них з боку органів державної влади. До прикладу останніх належить нелегальний обіг криптовалюти чи поширення злочинних практик в мережі Інтернет.

Окремо варто звернути увагу на поділ загроз за можливістю прогнозування, оскільки цифрові технології та рішення мають динамічну форму прояву та знаходяться в постійному розвитку, а передбачення тенденцій є ускладненим як через нестачу стабільних ретроспективних даних, так і внаслідок радикальних змін технологій. Тому важливою є класифікація загроз за ступенем небезпеки та вірогідністю, оскільки менш помітні тимчасові тенденції можуть слугувати лише перехідним етапом для технологій і не потребують уваги суб'єктів забезпечення економічної безпеки держави в умовах обмеженості ресурсів.

Перелічені підходи до класифікації загроз відзначають здебільшого горизонтальний їх поділ, проте через комплексний вплив значної кількості загроз їх слід розглядати і у вертикальному розрізі за можливістю впливу на них. Так, на макрорівні здійснюється протидія найбільш небезпечним для реалізації національних економічних інтересів загрозам, яким неможливо запобігти на мезо-, мікро- та нанорівнях. Утім, загрози можуть мати джерело походження та впливу на наднаціональному, глобальному рівні. Тому доцільно здійснювати їх системну структурування за рівнем походження на національні та наднаціональні, що розширює можливість розуміння природи загроз та посилює методологічну базу їх виявлення.

На нашу думку, також варто виділити поділ загроз за впливом цифрового компонента. Так, загрози з активним компонентом, пов'язані з умисними діями злочинців, які використовують цифрову інфраструктуру для отримання власної незаконної вигоди, мають кінцевого бенефіціара ризику, а з пасивним є наслідком складних комплексних процесів цифровізації, які утворюють загальні тенденції трансформації та залежать лише від об'єктивних процесів в національній економіці.

А отже, беручи до уваги вищенаведений аналіз наукових праць та обґрунтовані критерії поділу за рівнем походження й впливом цифрового компонента, можна побудувати наступну широку класифікацію загроз економічній безпеці держави в умовах цифровізації (рис. 1.6).

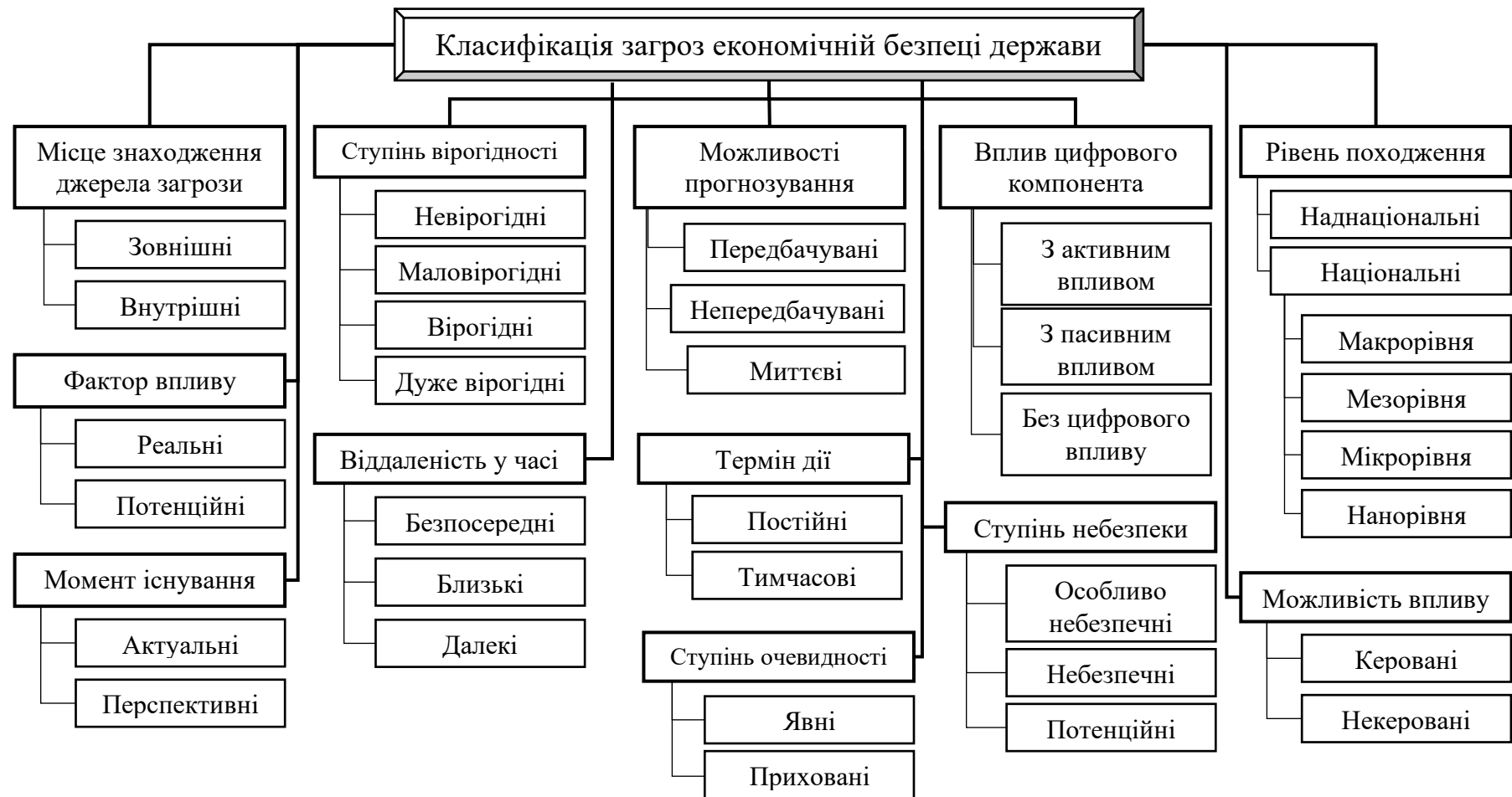


Рис. 1.6. Класифікація загроз економічній безпеці держави в умовах цифровізації

Джерело: систематизовано автором на основі [45; 53-54]

Так, розглядаючи класифікацію загроз економічній безпеці, вважаємо за доцільне здійснити кластеризацією загроз економічній безпеці держави, спричинених цифровізацією. Таким чином можна буде сформулювати перелік пов'язаних загроз та визначити їх взаємозв'язок.

Для цього здійснимо міждисциплінарний аналіз інструментом Connected Papers [87], який дозволяє скласти бібліографічні кластерні мапи методом графів за схожістю пов'язаних наукових досліджень. Для поставленого завдання перевагою цього інструменту є міждисциплінарна широта охоплених публікацій. Передбачається, що дві статті, які прямо не цитують одна одну, але мають збіг за цитуваннями, мають більший імовірність розглядати споріднену тему, навіть попри різні ключові слова та назву роботи. Ця перевага закладена у використанні концепції спільного цитування та бібліографічного зв'язку.

Отже, першим кроком, керуючись Global Risk Report 2024 та 2025 роки [110; 136], визначаємо перелік з шести техногенних загроз. Ними є несприятливі наслідки технологій штучного інтелекту (далі – ШІ) та передових технологій загалом, цензура і нагляд, цифровий шпівонаж та кібервійни, дезінформація та введення в оману, онлайн-насильтство. Визначений перелік і формує основну для бібліографічного пошуку.

На другому кроці визначаємо найбільш вагомi статті з найвищою кількістю цитувань за ключовими словами, які збігаються з визначеними раніше технологічними загрозами (додаток Б).

Третім кроком концептуалізуємо утворені довкола обраних статей кластери досліджень та формуємо міждисциплінарні зв'язки. Для цього можна провести вторинну кластеризацію загроз за ключовими словами, темами та анотаціями наукових статей методом графів (рис. 1.7). Значимість кластеру і його елементів відобразимо пропорційно до вже визначеного попередниками глобального ландшафту ризиків Global Risk Report [136], а класифіковані загрози, які збігаються з переліком, також пропорційно збільшимо на мапі для більшої наочності.

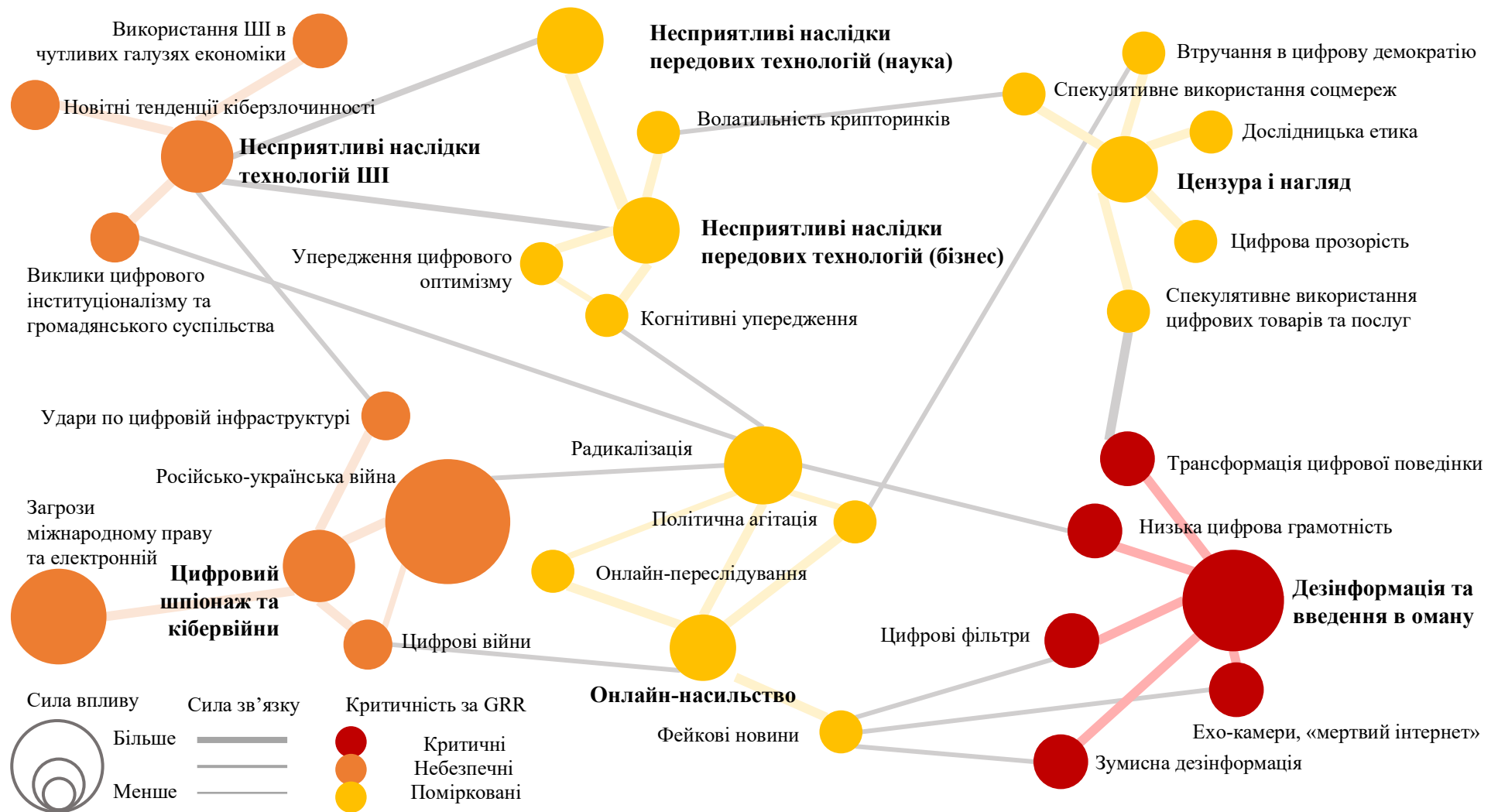


Рис. 1.7. Мапа кластеризації загроз економічній безпеці держави в умовах цифровізації інструментом Connected Papers за спільним цитуванням та бібліографічним зв'язком

Джерело: складено автором на основі [227-228]

Центром ваг кластеризації (табл. 1.2) є дезінформація та введення в оману, що створює значний соціальний, політичний та економічний тиск. Тобто велика кількість неякісної інформації зумовлює загальний несприятливий вплив подальшої цифровізації. А найбільш загрозливими для економіки є міжнародні суперечки та геополітичні конфлікти.

Таблиця 1.2

Розподіл понять по кластерам за ключовими словами в базі даних

Semantic Scholar Paper Corpus до інструменту Connected Papers

Кластер	Центральне поняття (розмір)	Складові поняття (розмір)
Червоний	Дезінформація та введення в оману (1,7)	Трансформація цифрової поведінки, низька цифрова грамотність, цифрові фільтри, ехо-камери, «мертвий інтернет», зумисна дезінформація (0,9).
Помаранчевий	Цифровий шпіонаж та кібервійни (1,2)	Російсько-українська війна (2,1), загрози міжнародному праву та електронній комерції (1,6), цифрові війни, удари по цифровій інфраструктурі (0,8).
	Несприятливі наслідки технологій ІІІ (1,2)	Виклики цифрового інституціоналізму та громадянського суспільства, новітні тенденції кіберзлочинності, використання штучного інтелекту в чутливих галузях економіки (0,8).
Жовтий	Несприятливі наслідки передових технологій (1,1)	Волатильність крипторинків, упередження цифрового оптимізму, когнітивні упередження (0,7).
	Онлайн-наси́льство (1,1)	Радикалізація (1,3), політична агітація, онлайн-переслідування, фейкові новини (0,7).
	Цензура і нагляд (1,1)	Втручання в цифрову демократію, спекулятивне використання соцмереж, дослідницька етика, цифрова прозорість, предметна цифрова трансформація (0,7).

Джерело: складено автором на основі джерел [110; 136; 227-228]

Визначена класифікація загроз економічній безпеці держави підкреслює характерні властивості цифровізації, а також глибину та ширину її поширення в національній економіці. Проте це дає лише опосередковане розуміння джерела їх походження. Тому впливає потреба не лише описати загрози економічній безпеці держави, а й визначити детермінанти їх походження, а саме сукупність внутрішніх та зовнішніх передумов, умов, явищ, процесів, тенденцій та інших факторів, які формують саме середовище виникнення загроз.

Так, в умовах цифровізації, джерело більшості загроз знаходиться на зовнішньому рівні, тобто поза межами впливу суб'єктів забезпечення економічної безпеки держави. У той же час, окремі загрози економічній безпеці держави спричинені внутрішніми детермінантами.

Погоджуємось з визначенням К. Мактутіса [49], що серед детермінант потенційних загроз, які кіберзлочинці становлять для внутрішньої безпеки країни, найнебезпечнішими є місцеві громадяни. На жаль, вони можуть бути використані як співники в міжнародній кіберзлочинності. Транскордонна та кіберзлочинність стають значними зовнішніми загрозами і легко поширюються на країни, що характеризуються поганою безпековою політикою, відсутністю потенціалу та інструментів для боротьби із цифровою злочинністю.

Також важливою є думка О. Мардера [48] який визначає, що наявні внутрішні деструктивні явища та недосконалості створюють сприятливе середовище для детермінант зовнішнього негативного впливу на систему економічної безпеки держави. Тобто злочинці в мережі Інтернет можуть використовувати вразливу економічну систему для своєї вигоди. Окрім того, бідність, злочинність мають тенденцію розповсюджуватися, зокрема шляхом міграції населення, а разом із тим нести «троянського коня» у вигляді деструктивних практик із недобросовісного використання цифрових технологій. Це призводить до того, що не всі суб'єкти системи міжнародної економічної безпеки можуть або прагнуть брати у протидії загрозам.

На нашу думку, доцільно всіх суб'єктів світової економічної діяльності поділяти на бенефіціарів забезпечення безпеки, які отримують вигоди від конкурентної торгівлі, прозорого ринку, зростання якості життя громадян. Та на бенефіціарів ризикової поведінки, які беруть на себе репутаційні та криміногенні ризики для використання вразливостей економіки. Зокрема вразливостей створених впливом цифровізації, для досягнення неконкурентної переваги та отримання недоброчесної вигоди. Подібні дії ускладнюють реалізацію безпекових заходів суб'єктами забезпечення безпеки, що робить загрози цифровізації більш стійкими.

Диференційоване ставлення до цифровізації на міжнародному рівні та її властивості адаптивності, анонімності масштабності, мультиплікативності і проникності ускладнюють зовнішнє середовище загалом. А загрози внутрішнього середовища одних країн можуть поширювати на інші держави, або й взагалі слугувати посередниками між двома іншими середовищами. Тому, зважаючи, на визначені вище загрози за впливом цифрового компонента та загрози національного і наднаціонального рівня, визначення їх детермінант потребує трирівневої системи.

Це з підходами М. Портера [46] та Д. Джонсона, К. Шоулза, Р. Уїтгінгтона [47] щодо розділення зовнішнього середовища на ближнє та дальнє, а внутрішнє лишати без змін. Такий поділ має на меті виокремлення універсальних детермінант, які впливають на більшість економік світу з одного боку, а також транснаціональних, характерних для окремих груп країн та регіонів з іншого. Наприклад війни, в аспекті конвенційних загроз, мають вплив лише на залучені країни, але розрив ланцюгів постачання через них вже на світову економіку загалом.

Отже, детермінанти загроз економічній безпеці в умовах цифровізації формують трирівневу систему з передумов, умов, явищ, процесів, тенденцій та інших факторів, із суб'єктами забезпечення безпеки та ризикової поведінки на всіх рівнях. Вплив детермінант на середовище є системним та взаємозалежним.

Можна зазначити наступний порядок впливу: спершу глобальні процеси цифрової революції перетворюються в зовнішні чинники, які далі сприяють сильній адаптивній економіці або тиснуть на слабку і негнучку, утворюючи внутрішні виклики та загрози. У загальному вигляді вплив, взаємодія і протидія зовнішнім ближнім та дальнім внутрішнім детермінантами формує ієрархічну послідовність у забезпечення економічної безпеки держави (рис. 1.8).

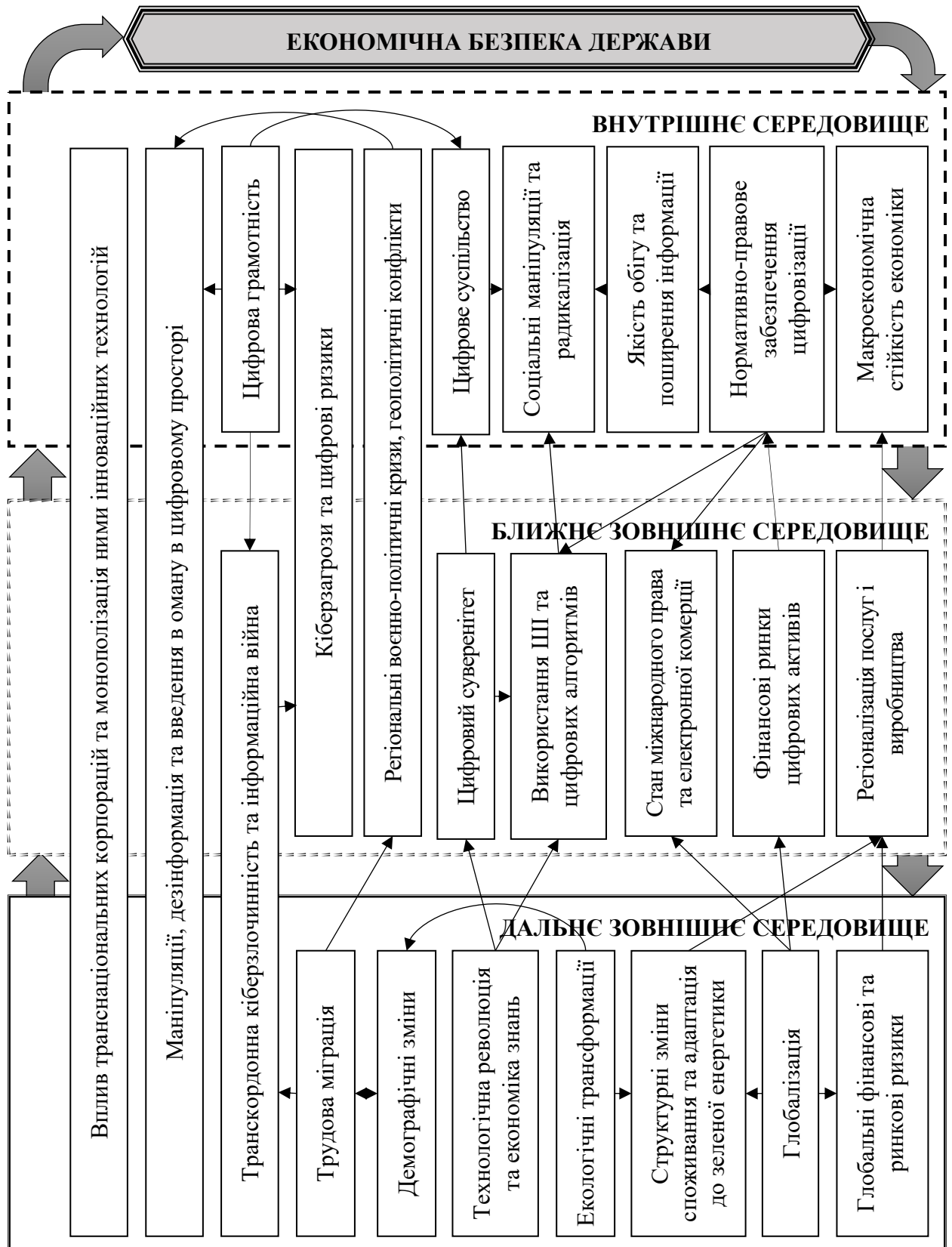


Рис. 1.8. Детермінанти загроз економічній безпеці держави в умовах цифровізації

Джерело: складено автором на основі джерел [42-49]

Підсумовуючи аналіз загроз економічній безпеці держави та детермінант їх виникнення в умовах цифровізації, можна визначити загрози як системні явища, які виникають внаслідок недосконалого середовища, впливу непередбачуваних, нестабільних, неефективних чи прямо деструктивних внутрішніх та зовнішніх детермінант. Важливим, на нашу думку, для визначення впливу цифровізації на загрози економічній безпеці держави є їх поділ за середовищем виникнення, що пропорційно відображають світові процеси з одного боку, стабільність та стійкість – з іншого.

Саме тому забезпечення економічної безпеки держави потребує кооперації та співпраці для мінімізації негативного впливу загроз, зокрема шляхом підсилення національних економік, протидії транскордонній злочинності, регулювання впливу транснаціональних компаній та формування міжнародної системи безпеки.

Також, варто відзначити вплив бенефіціарів ризикової поведінки, які навпаки прагнуть зменшити рівень забезпечення глобальної безпеки. Своїми діями, вони сприяють виникненню та поширенню загроз, зокрема, шляхом використання новітніх інновацій зі злочинним умислом, створюють для цього віртуальну тіньову інфраструктуру та обмежують вплив інституцій.

У момент, коли одні суб'єкти світової економіки забезпечують безпеку, а інші компрометують її, поляризація стає очевидним проявом дуального впливу цифровізації. В першу чергу вона зумовлена можливістю використання нейтральних за своєю природою детермінант цифрової трансформації з різною метою. Так, об'єктивні властивості та детермінанти цифровізації здатні не лише сприяти соціально-економічному розвитку та зростанню якості життя, а й набувати негативного вираження, деформувати економічні процеси та поглиблювати соціальну нерівність.

1.3. Особливості впливу цифровізації на економічну безпеку держави

Визначені у попередніх підрозділах властивості та детермінанти цифровізації свідчать про дуальність впливу цього процесу, а також про супутню поляризацію, іманентний діалектизм та конфліктність між її суб'єктами. Навряд чи можна погодитися з тим, що цифровізація є виключно фактором економічного зростання, як це зазначено в роботах за редакції О. Гальцової [50] та М. Акулюшиної [56], оскільки навіть самі автори визначають потребу в забезпеченні кібербезпеки та розвитку інформаційної інфраструктури в умовах всеосяжної цифрової трансформації соціально-економічних відносин.

Враховуючи це, цілий ряд науковців, зокрема І. Тарасенко [65], І. Шевчук, Б. Депутат [69], О. Вінник [70] та О. Череп, І. Дашко, Л. Брехтер [71] наголошують на необхідності застосування дуального підходу при дослідженні особливостей впливу цифровізації на економічну безпеку держави. Насамперед, вони погоджуються з тим, що цифровізація сприяє розвитку технологій, прозорості публічних послуг, цифровій інклюзії, боротьбі з корупцією, пожвавленню комерції, формуванню нових ринків, зростанню продуктивності праці та якості життя. Проте, водночас, автоматизація як невід'ємна складова цифровізації може спричинити зростання соціальної нерівності, рівня безробіття та бідності, а також призвести до структурної деформації у розміщенні продуктивних сил.

Попередній розгляд позитивного впливу цифровізації, що деталізований у працях науковців, можна згрупувати за такими основними напрямками: підвищення ефективності та продуктивності виробництва; розвиток нових ринків та бізнес-моделей; покращення адміністративних послуг, якості життя та прозорості публічного управління; зміцнення економічної стійкості держави; прискоренні інноваційного та технологічного розвитку. Разом із цим, з позиції захисного підходу до забезпечення економічної безпеки держави, необхідно

розглянути та дослідити потенційний негативний вплив цифровізації на стійкість та розвиток національної економіки на практичних кейсах.

Так, автоматизація, діджитизація, зниження операційних витрат і сприятливий леверидж інвестицій складають рушійну силу зростання ефективності та продуктивності комерційного та державного секторів національної економіки. Наприклад, дослідження Європейського центрального банку демонструє, що компанії, які суттєво збільшують інвестиції у цифрові технології, через п'ять років після їх впровадження покращують як продуктивність праці, так і загальну продуктивність. Зазначається, що загальний приріст продуктивності становить від 20 % до 300 % [47].

Визначена в підрозділі 1.1 властивість циклічної динаміки розвитку цифровізації сприяє пришвидшеному зростанню нових цифрових ринків, а саме електронної комерції, фрилансу, криптовалют та блокчейну, хмарних технологій, онлайн-сервісів, віртуальної реальності, цифрового контенту тощо. В результаті стрімкого розвитку цифрових послуг розмір ІКТ-галузі за даними UNCTAD [132] оцінюється від 4,5 % до 15,5% світового ВВП, що становить від 3389,6 до 12711,0 трлн. дол. США та свідчить про значний потенціал для подальшого розвитку цього сектору національної економіки.

Утім, на противагу зазначених переваг, К. Маркевич [52] відзначає, що зі зростанням цифрового сектору актуалізуються загрози конфіденційності даних та можливого злому цифрових систем із несанкціонованим доступом до персональних даних. Зазначимо, що кількість даних, зібраних датчиками інтернету речей, невпинно зростає, тому однією із основних загроз є відсутність повної згоди на збір та обробку персональних даних. При цьому, викликають занепокоєння не лише питання етичності збирання та комерційного використання особистих даних, а й потенційні витoki цієї інформації, кодів і ключів доступу, що також створюють суттєві ризики для компаній. Окрім безпосередніх фінансових, втрат такі інциденти можуть призвести до репутаційних збитків, котрі знижують конкурентоспроможність

бізнесу. Разом із тим, постійно зростають і витрати на юридичні послуги для подолання наслідків витоку інформації, залучення персоналу для розслідування, виплати штрафів та компенсацій, повідомлення можливих жертв, відновлення ділової репутації тощо. При цьому витік критичної інформації цілком може призвести до порушення операційної діяльності цілого підприємства. У економічних показниках середні витрати, спричинені одним витоком даних по всьому світу, дорівнюють 4,24 млн дол. США, що складає 38% загальних витрат бізнесу [74], а з червня 2016 року по грудень 2021 року в результаті понад 241 000 інцидентів зі зломом електронної пошти шахраями було викрадено 43,31 млрд дол. США коштів фізичних та приватних осіб [75].

До того ж масштабні витoki даних можуть дестабілізувати фінансовий сектор та сприяють зростанню кіберзлочинності. Зрештою, саме вразливість цифрової інфраструктури комерційних компаній робить національну економіку вразливою до технологічного шпигунства.

Продовжуючи розгляд позитивних аспектів, такі науковці, як О. Вінник [70], О. Череп, І. Дашко та Л. Брехтер [71] відзначають, що застосування цифрових технологій у публічних послугах, включаючи освіту й медицину, сприяє підвищенню їх доступності та якості. При тому цифровізація, на думку авторів, здатна сприяти соціальному, культурному та економічному розвитку, а також зміцненню демократичності суспільства та інституцій.

Це підтверджується взаємозв'язком показників індексу ефективності уряду (рис. 1.9) та впровадження цифрових державних послуг (рис. 1.10). Так, держави, що займають лідерські позиції за ефективністю публічних послуг, а саме Данія, Естонія, Мальта, Швейцарія мають значні досягнення і в питаннях цифровізації державних послуг. Можна відмітити, що країни з меншою територією та чисельністю населення, демонструють вищу схильність до використання аналогових послуг. Тоді як більші за територією держави, особливо ті, що характеризуються нижчою ефективністю управління, намагаються модернізувати публічні інституції через впровадження цифрових технологій.

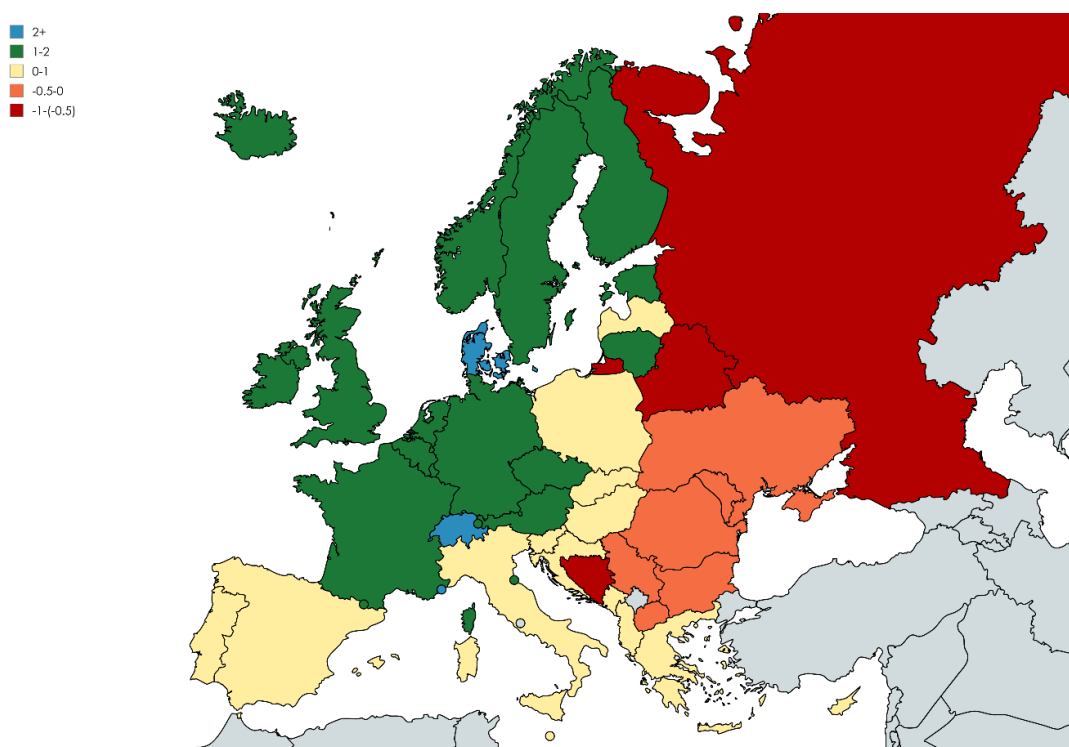


Рис. 1.9. Розподіл країн за показником індексу ефективності уряду за 2023 р.

Джерело: складено автором на основі [224]

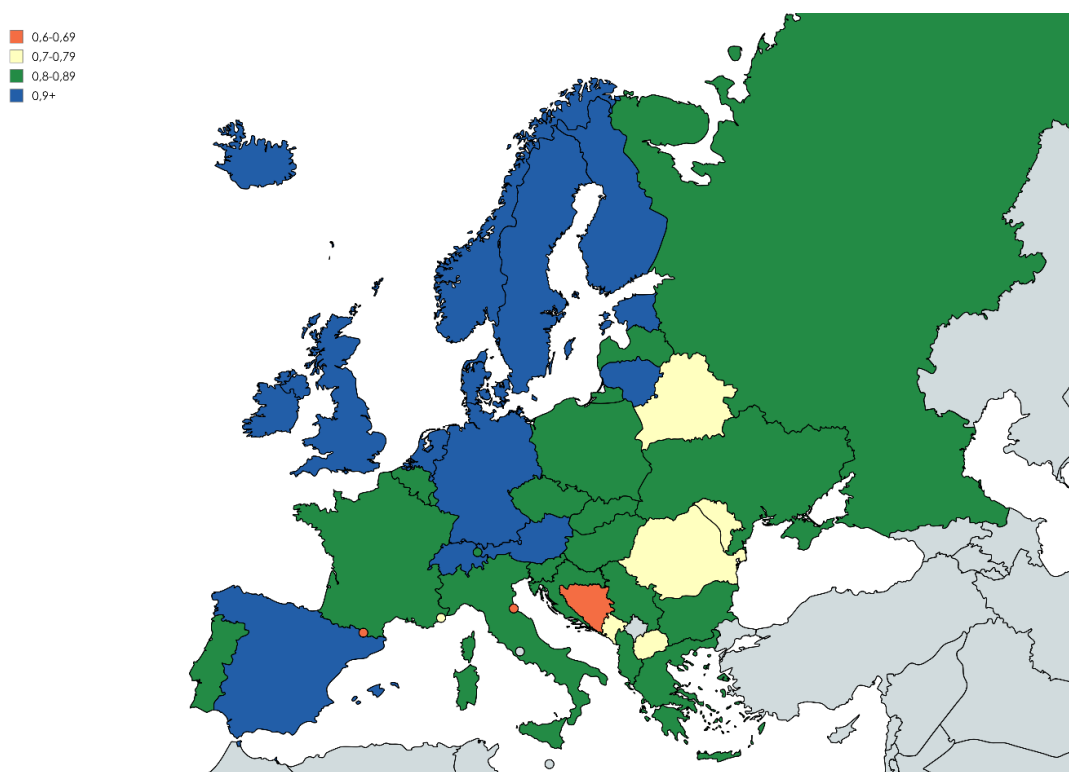


Рис. 1.10. Розподіл країн за показником впровадження цифрових державних послуг за 2023 р.

Джерело: складено автором на основі [223]

Натомість, з іншого боку, цифровізація може використовуватися в авторитарних та деспотичних цілях контролю за населенням. Наприклад уряд Китаю, використовуючи дані інтернет-провайдерів, стільникових операторів, власників сайтів, роботодавців, університетів, правоохоронних органів, податкових відомств, банків тощо, за допомогою можливостей «Big Data» та вже наявної тоталітарної моделі контролю за громадянами впровадив розрахунок суспільного рейтингу. За цим експериментом громадянин набуває можливості користуватися пільгами у випадку високого індивідуального рейтингу, а у випадку низького його очікує притиснення його громадянських, соціальних та економічних прав [58]. Слід зауважити, що контроль над статистичними даними та алгоритмами, окрім їх неетичності, генерує загрози економічній безпеці держави, оскільки може бути використаний для маніпулювання даними в мережі Інтернет, штучного завищення вартості національних цінних паперів, неринкових механізмів міжнародної конкуренції та шпіонажу.

Утім, поряд із зазначеними ризиками, цифровізацію правомірно вважати драйвером інноваційного розвитку. У даному контексті цілком погоджуємося з думкою А. Ворзау й К. Бокеман [92], що цифровізація стимулює появу інноваційних рішень у всіх секторах національної економіки та сприяє їх швидкій розробці і впровадженню. Окрім цього, компанії, які інвестують у цифрові технології, отримують ранні переваги; опиняються краще підготовленими до майбутніх викликів та зазвичай ефективніше використовують нові можливості в умовах цифровізації.

Разом із цим, інтеграція цифрових платформ у бізнес-процеси полегшує обмін інформацією, сприяє тіснішій співпраці між компаніями, науковими установами та державними структурами, що забезпечує ширший доступ до ринку для малих і середніх підприємств. Тому це знаходить вираження у зростанні рівня інноваційного розвитку зі збільшенням цифрової конкурентоспроможності держави (табл. 1.3).

Таблиця 1.3

Порівняння показників інноваційного розвитку та цифрової
конкурентоспроможності країн Європи

Країна	Цифрова конкурентоспроможність		Глобальний індекс інновацій	
	Місце	Оцінка	Місце	Оцінка
Швейцарія	2	(93,15)	1	(67,5)
Данія	3	(91,99)	10	(57,1)
Швеція	4	(90,42)	2	(64,5)
Нідерланди	8	(87,3)	8	(58,1)
Норвегія	10	(84,58)	21	(49,1)
Фінляндія	12	(83,57)	7	(59,4)
Ірландія	17	(80,75)	19	(50,0)
Велика Британія	18	(78,21)	5	(61,0)
Ісландія	19	(78,18)	22	(48,5)
Франція	20	(76,58)	12	(55,4)
Бельгія	21	(75,61)	24	(47,7)
Литва	22	(75,66)	45	(40,1)
Австрія	25	(72,87)	17	(50,3)
Іспанія	28	(70,86)	28	(44,9)
Люксембург	29	(69,46)	20	(49,1)

Джерело: складено автором на основі [151; 227]

За результатами порівняння можна дійти висновку, що країни-лідери із використання цифрових технологій для досягнення конкурентних переваг одночасно є лідерами інноваційного розвитку. Це підтверджує позитивний вплив цифровізації на інноваційний розвиток національної економіки.

На нашу думку, варто зауважити, що незважаючи на існуючий оптимізм щодо переваг цифровізації, дана позиція значною мірою ігнорує нерівномірний вплив цього процесу у світовому масштабі. Наприклад, незважаючи на значний приріст інтернет-користувачів у країнах Африки та Азії за останні понад 20 років, покриття цих континентів знаходиться лише на рівні 50% [132], що суттєво обмежує можливості впровадження цифрових технологій та використання переваг цифровізації у цих країнах.

Разом із цим, наявність внутрішнього кадрового потенціалу не гарантує реалізації переваг цифровізації, оскільки сектор інформаційно-комунікаційних технологій (далі – ІКТ) здебільшого орієнтований на експорт

цифрових рішень за рахунок використання дешевшої робочої сили. Так, О. Пищуліна [93] відзначає, що попри значні показники України в експорті ІКТ-послуг, це не забезпечило високої цифрової конкурентоспроможності країни через структурні проблеми, зокрема, дефіцит висококваліфікованих кадрів та їхню еміграцію. Таким чином ІКТ-індустрія України посідає третє місце серед секторів економіки з найбільшою часткою в експорті країни, а понад 70% експорту ІКТ-послуг припадає на розробку програмного забезпечення на замовлення, їх частка у загальному експорті становить 20%, а темпи зростання сягають 26% на рік. Водночас, ці успіхи не забезпечили високих позицій України у міжнародних рейтингах. Так за індексом цифрової конкурентоспроможності Міжнародного валютного фонду Україна посідає лише 54-те місце серед 63 країн [151]. Однією з ключових проблем є дефіцит висококваліфікованих фахівців через їх виїзд за кордон, зокрема, у Європу, де щорічна потреба у інженерних кадрах оцінюється у 100 тис. осіб. Так, із 17 тис. спеціалістів, що випускають українські вищі навчальні заклади, майже 10 тис. орієнтовані на еміграцію [93].

Зважаючи на такі статистичні дані, головними бенефіціарами цифровізації стають саме країни з високим рівнем доходу, що можуть, з одного боку, користуватися вже розвиненим ринком цифрових послуг, а з іншого – залучати дешевих спеціалістів у сфері ІКТ з інших країн. Тоді як більшість країн із рівнем доходів нижче середнього відчують загрозу дефіциту спеціалістів, адже вони не можуть залучити їх без значних фінансових інвестицій, що в подальшому лише збільшує розрив у цифровому розвитку. Тому цифровізація не є передумовою подолання соціальних бар'єрів чи фактором розвитку всіх держав. Так, в окремих країнах цифровізація призвела до зростання якості життя, проте в значній кількості країн не відбулося вагомих позитивних зрушень для переважної більшості їх населення.

Розглядаючи дуальний вплив цифровізації та її можливість генерувати загрози економічній безпеці держави, беззаперечно варто виділити виникнення в процесі цифрової трансформації соціально-економічних

відносин кіберризиків та кіберзагроз. Так, ризики інцидентів кіберзлочинності увійшли до трійки глобальних бізнес-ризиків у 2021 році за рейтингом Allianz Risk [112]. Сама ж кіберзлочинність коштувала світовій економіці понад 1 трлн США, тобто більше ніж 1% світового ВВП у 2021 р. [112]. Утім, навіть така сума є заниженою, оскільки підрахувати витрати на подолання наслідків та недоотриманий прибуток від виведення з ладу цифрової інфраструктури є вкрай складним завданням.

Прикладом можливого застосування цифрових технологій для враження критичної інфраструктури є інцидент «Stuxnet», коли група хакерів проникла у систему керування іранською атомною електростанцією (далі – АЕС). Потенційну шкоду, викликану такою атакою, складно оцінити, бо виключно зупинка АЕС призвела б до значних виробничих та гуманітарних втрат. Групу, що стояла за атакою, не було знайдено, як і не відомий рівень проникнення конфліктуючих держав по всьому світу у критичну інфраструктуру один одного.

Так, реальна можливість безкарного дистанційного руйнування об'єктів критичної інфраструктури становить небезпеку аналогічну ядерним ударам. Зі зростанням інтернету речей, хакери зможуть виконувати подібного роду атаки на постійній основі. Прикладом подібної кібератаки по інфраструктурі за допомогою цифрових технологій є удар по стратегічному нафтопроводу «Баку-Тбілісі-Джейхан». І, що важливо, послідує обмеження експорту та шкода економікам Туреччини та Грузії мали під собою військові цілі.

У питанні кібератак по інфраструктурі, варто виділити загрози використання низькоякісного або піратського програмного забезпечення з ненадійними протоколами безпеки. Так, домінування російської мови на територіях колишнього СРСР сприяло поширенню застарілих або нелегальних програмних продуктів. А їх використання, через економічні та мовні чинники, створило в подальшому чисельні вразливості для кібератак. При цьому висока вартість ліцензійного софту та мовні бар'єри лише підсилюють потенційні можливості для ударів по вже вразливим економікам.

Саме таким методом у 2017-2018 рр. було атаковано АТ «Прикарпаттяобленерго», АТ «Чернівціобленерго» та ПАТ «Київобленерго» з дистанційним відключенням підсистем, викраденням та видаленням даних, блокуванням дистанційного доступу.

Таким чином, найбільша загроза, яку можуть створити хакери – це відімкнення країни від її власної електромережі. Також можливе місцеве ураження дистанційно керованої критичної інфраструктури, що, в свою чергу, може призвести до втрати керованості на декілька днів або навіть тижнів, зупинити економічні процеси, фінансові операції, створити транспортний колапс тощо. Проте, поки що такі операції надскладні, потребують багато часу і все ще можуть бути нівельовані системою ручного керування. Але з подальшим цифровим розвитком прогнозовано зростатимуть загрози руйнівних ударів по критичній інфраструктурі з використанням цифрових інструментів.

Іншим важливим аспектом впливу цифровізації на економічну безпеку держави є формування нових економічних циклів. Так, наприклад «криза Доткомів», що була пов'язана з надмірними інвестиціями в Інтернет-економіку, стала першою, проте не єдиною бульбашкою цифрових технологій.

Окрім того, потрібно виділити вплив цифровізації на ринок праці, демографію та робочі процеси. Так, автоматизація, віртуалізація, цифрові платформи, інтернет речей та промислові роботи вже змінили структуру економіки. А, разом з тим, і вимоги до кваліфікації працівників й організації робочих процесів. До того ж, вважаємо, що в цьому питанні доцільно розділяти вплив цифровізації на наслідки від впровадження цифрових сервісів, та наслідки від промислових роботів та автоматизації.

Досліджуючи питання трансформаційних процесів в економіці, С. Ешфорд, Б. Каза, Е. Рейд, В.Панченко, Н. Резнікова, О. Іващенко та Д. Русак [60-61] визначають, що цифрові трудові платформи формують новий тип цифрової зайнятості, при якому організації або окремі особи використовують

цифрові рішення для доступу до ринку праці, а трудові відносини базуються на тимчасових контрактах та гнучких принципах ціноутворення.

У зв'язку з безальтернативністю розвитку нових форм ринку праці в умовах цифровізації погоджуємося з думкою науковців, щодо виникнення потенційних загроз економічній безпеці держави у соціальній сфері, адже короткострокові або неформальні трудові відносини створюють суттєві ризики для працівників через відсутність трудових гарантій, нестабільність доходів та юридичну незахищеність.

Іншим впливом цифровізації на структуру ринку праці є автоматизація та роботизація виробничих процесів. Д. Блум, М. МакКена, К. Претнер [64] зазначають, що від 9% до 47% робочих місць в країнах з високим рівнем доходу будуть замінені роботами чи нейромережами у найближчі два десятиліття. Таким чином, технології штучного інтелекту вже використовуються для виконання частини робіт, у тому числі креативних, що зменшує попит на ринку праці і може призвести до зростання безробіття.

Д. Асмогли [67] та П. Рестепо [68] визначають, що в сучасних умовах один промисловий робот заміщує від 5,6 до 6,2 працівників, а збільшення їх кількості у 2010-2030 роках буде еквівалентне приросту робочої сили на 57-64 млн осіб, що підвищує мінімальну потребу створення робочих місць для збереження цільового рівня безробіття, як одного з показників економічної безпеки держави.

Проте, попри потенційне скорочення зайнятості у виробничому секторі автоматизація супроводжується ще й зростанням попиту на інженерні кадри для налаштування, обслуговування та виробництва роботизованих систем. Особливо це актуально для країн із рівнем доходів вище середнього та демографічними викликами, такими як старіння населення та нестача працівників у секторі послуг. У свою чергу, в країнах із вищою часткою молодого населення ця проблема менш виражена, оскільки має більший притік робочої сили та менші потреби в її заміні роботами.

Отже, хоча роботизація потенційно може створити загрозу безробіття в майбутньому, проте зараз вона здебільшого посилює вже існуючу нерівність між країнами з різним рівнем економічного розвитку та спричиняє посилення транскордонної трудової міграції. Утім, існують дієві заходи протидії, доступні соціальним інституціям. Наприклад, галузеві угоди профспілок можуть знижувати вартість низько- та середньокваліфікованої робочої сили в обмін на гарантії збереження робочих місць. Проте, це призводить до зменшення позитивного ефекту від цифровізації, оскільки зменшуються і якість життя, і ефективність праці.

Вищенаведений перелік прикладів дає змогу визначити, що вплив цифровізації є діалектичним за сутністю, оскільки однакові процеси знаходять позитивне та негативне вираження (рис. 1.11), залежно від дій суб'єктів та стану зовнішнього середовища.



Рис. 1.11. Дуальний вплив цифровізації на економічний розвиток

Джерело: розроблено автором

Більшість науковців погоджуються, що недосконалістю існуючого законодавства посилює негативний вплив цифровізації. Так, до цього закони були розраховані виключно на аналогові процеси та форми діяльності і тепер не відповідають актуальним потребам. Тому, такі комплексні категорії, як цифровий медіа акаунт, права власності на цифрове майно, додаткові вимоги, умови та можливості програмного забезпечення, приховані елементи гравального бізнесу, криптовалюти і криптовалютні гаманці, відокремленість поняття цифрової власності і довічної оренди продукту не мають належного регулювання.

У чинному законодавстві, товари, які продаються на онлайн платформах, здебільшого не відрізняються від тих, що продаються на аналогових ринках. Таким чином, за визначенням Європейської ради [76] цифрові товари представляють ту категорію товарів, які зберігаються, архівуються, доставляються та/або використовуються в електронному форматі та доставляються електронному споживачу електронною поштою або завантажуються з мережі Інтернет. Проте такий підхід не дозволяє регулювати покупки всередині цифрових продуктів, наприклад, іграх, що поглибило дискусії стосовно цифрової форми товарів.

У США та Канаді компанія Entertainment Software Rating Board (ESRB) з 2020 року запровадила новий маркер для цифрових товарів із азартними елементами [77]. Такі країни як Бельгія та Нідерланди обмежили оборот подібних товарів, а Китай і Японія вводять обмеження і змушують розкривати додаткові дані про такі товари. Нові вимоги у подальшому викликали відповідні обмеження від видавців, які оскаржили поточні умови роботи в цих країнах, бо вони перешкоджають виходу на ринок їх цифрових продуктів [78].

Такі обмеження окремих країн та виробників призводять до загрози знецінення цифрових покупок. Внаслідок цього відбуваються втрати або зниження вартості товару через технологічне старіння, зміни у бізнес-моделях, відсутність фізичної власності, закриття сервісів чи змін у ліцензійних угодах. Натомість нові версії програм витісняють попередні, роблячи їх менш

актуальними або несумісними з сучасними пристроями. Так, цифрові продукти не мають фізичної форми, що ускладнює їх перепродаж або передачу, обмежуючи права споживачів. Що гірше, оновлення умов використання можуть в односторонньому порядку обмежити права користувачів на раніше придбані цифрові товари.

А з іншого боку, постачальники цифрових послуг, які діють як посередники під час здійснення діяльності з надання сервісів для зберігання інформації, мають право на звільнення від відповідальності за збитки або кримінальні покарання, пов'язані з вмістом, наданим третіми особами за допомогою їхніх мереж. Згідно ст. 15 Директиви про електронну торгівлю ЄС [79] державам-членам, регіональним органам влади заборонено накладати на постачальників будь-які загальні зобов'язання щодо цифрового контенту, до якого вони надають доступ.

Утім, одну з найбільших загроз економічній безпеці держави в умовах цифровізації становить трансформація форм грошей та цінних паперів, тому варто окремо зупинитися на них. Так, П. Рубанов [62] та С. Грицай [63] виділяють наступні категорії: електронні, цифрові та віртуальні гроші, а також криптовалюти. Втім, на нашу думку, доцільно розділяти саме цифрові гроші, зокрема цифрові валюти комерційних та центральних банків (анг. central bank digital currency, далі – CBDC) та криптовалюти, а інші варіанти є несуттєвими для цілей дослідження через їх локальне застосування та малу значимість.

Основними перевагами використання CBDC є те, що ці валюти знижують витрати на перекази та забезпечують глибшу інтеграцію держави у використання блокчейну. Натомість, криптовалюти, цифрові токени, дохід сектору надання віртуальних послуг та цифрових товарів мають високу спекулятивність та волатильність. Але, насамперед, значною загрозою є їх використання бенефіціарами ризикової поведінки для фінансування тероризму, відмивання коштів, отриманих злочинним шляхом, та ухилення від сплати податків.

Варто відмітити, що окремі криптовалюти є більш криміналізованими ніж інші. Так, у дослідженні С. Фаруджі, Дж. Еллула, Г. Аззорпарді [80] доведено, що 40% облікових записів мережі Ehtereum були пов'язані із незаконною діяльністю й використовувалися для фішингу, відмивання грошей, шахрайства, створення фінансових пірамід тощо. Окрім того, автори відзначають, що ця загроза є транснаціональною, і попри актуальні математичні системи вирахування махінацій та активну протидію спільноти із маркування ненадійних акаунтів, ця криптовалюта все ще залишається зручним інструментом для протизаконної діяльності та створює загрозу зростання тіньового сектору національної і світової економіки.

До подібних висновків приходять і Л. Хорнуф, Т. Кюк, та А. Швенбахер, що близько 20% «початкових пропозицій монет» (з англ, initial coin offering далі – ICO) токенів мали ознаки шахрайства [81]. Примітно, що ці цифрові активи виступають аналогом цифрових цінних паперів. І хоча в основі деяких ICO може лежати ринковий інтерес, існує значна частина спекулятивних ICO, а також тих, що не набувають жодного вираження.

Разом із цим, Ф. Наварро Кардосо [82] відзначає, що з усіх криптовалют, Bitcoin має вкрай низький ризик відмивання грошей. На ринку обсягом в 500 млрд дол. США лише 10 млрд використовуються для шахрайства та іншої незаконної діяльності, що становить лише 2% від загальної кількості [82].

Поруч із вигодами від використання цифрових активів та криптовалют, їх головний атрибут – анонімність – зумовлює використання для анонімної оплати злочинних послуг, що охоплюють торгівлю наркотиками, підробленими документами, викраденими банківськими даними, шкідливим програмним забезпеченням тощо [84]. Друга форма використання цифрових активів та криптовалют передбачає неконтрольоване їх розміщення з метою маніпуляцій та створення фінансових схем без належного нагляду [84]. Третя форма використання полягає у відмиванні грошей – злочинні доходи конвертуються у криптовалюту, після чого проходять через механізми

анонімізації, що ускладнює їхнє відстеження та подальше виведення у легальну економіку [82].

Таким чином, цифровізація призводить до виникнення якісно нових та трансформації традиційних загроз економічній безпеці держави. Потрібно відмітити, що вивчені наукові праці дозволяють розглядати негативний вплив цифровізації на економічну безпеку держави як трикомпонентний. Так, з одного боку, варто виділяти новоутворені прямі загрози, що виникають безпосередньо через недобросовісне використання цифрових технологій, рішень та послуг і не існують без цифрової інфраструктури. Разом з ними виникають новоутворені опосередковані загрози внаслідок структурних змін у національній економіці в умовах цифровізації. При цьому під впливом цифровізації трансформують традиційні загрози, які набувають нових властивостей та змінюють характер впливу на економічну безпеку держави (рис. 1.12). Цьому також сприяє трансформація товарів, посередників та покупців, що призводить до глибоких інфраструктурних, регуляторних і соціальних змін.

Отже, неупинний технічний прогрес створює нові та підсилює вже наявні виклики, ризики та загрози. Власне самі загрози, спричинені цифровізацією – системне та комплексне явище, що є проявом змін та впливу неідеального середовища, непередбачуваних, нестабільних, неефективних чи деструктивних зовнішніх та внутрішніх детермінант.

Однак, попри дуальність цифровізації, саме система забезпечення економічної безпеки держави є визначальним фактором протидії загрозам та мінімізації її негативного впливу. Дія комплексних заходів з ідентифікації деструктивних явищ, стабілізації систем та створення позитивних стимулів в економіці для подальших реформ є вирішальним фактором при формуванні позитивного або негативного впливу цифровізації. У подальшому ці заходи мають розповсюджуватися і на зовнішній рівень, залучаючи інвестиції, міжнародний досвід та підтримку для спільних дій із забезпечення економічної безпеки ряду держав.



Рис. 1.12. Вплив цифровізації на формування та трансформацію загроз економічній безпеці держави

Джерело: систематизовано автором на основі [50-84]

Так, основними напрямками мінімізації негативного впливу цифровізації є удосконалення нормативно-правового забезпечення, розвиток та впровадження передових інформаційно-технологічних інструментів, посилення інституцій, кадрового потенціалу економіки та інтеграція в міжнародний безпековий простір. Тому подальший розвиток цифрового середовища вимагає адаптації та оновлення законодавчої бази для ефективного регулювання нових викликів й загроз. А основою, для забезпечення правової визначеності й захисту інтересів усіх учасників економіки в умовах цифровізації є, зокрема, розробка законів щодо захисту персональних даних та контроль за діяльністю цифрових платформ.

Також важливими є інвестиції в інноваційні технології та створення власних цифрових платформ для підвищення стійкості до кіберзагроз та зменшення залежності від іноземних постачальників цифрових продуктів. Інший важливий напрямок полягає в зміцненні інституційної спроможності через формування ефективних формальних і неформальних інституцій держави. Разом з тим, невід’ємною складовою забезпечення кібербезпеки є розвиток кадрового потенціалу, удосконалення державного управління кваліфікованими кадрами та раціональним використанням цифрових технологій, як передумови мінімізації негативного впливу цифровізації на економічну безпеку держави.

Максимізація позитивного впливу цифровізації згідно з Цифровим компасом ЄС [72] передбачає удосконалення цифрових навичок і забезпечення доступності інфраструктури та державних послуг. Згідно з Стратегією цифрового розвитку інноваційної діяльності України на період до 2030 року [59] регулювання дуального впливу цифровізації передбачає розвиток людського капіталу, національної системи інновацій та комплексне економічне стимулювання інноваційної діяльності, зокрема галузеву підтримку бізнесу.

Тому поєднання пріоритетів цифровізації та заходів мінімізації її негативного впливу на загрози економічній безпеці держави дозволяє повністю відобразити сфери детермінації загроз із врахуванням її дуального впливу (рис. 1.13).

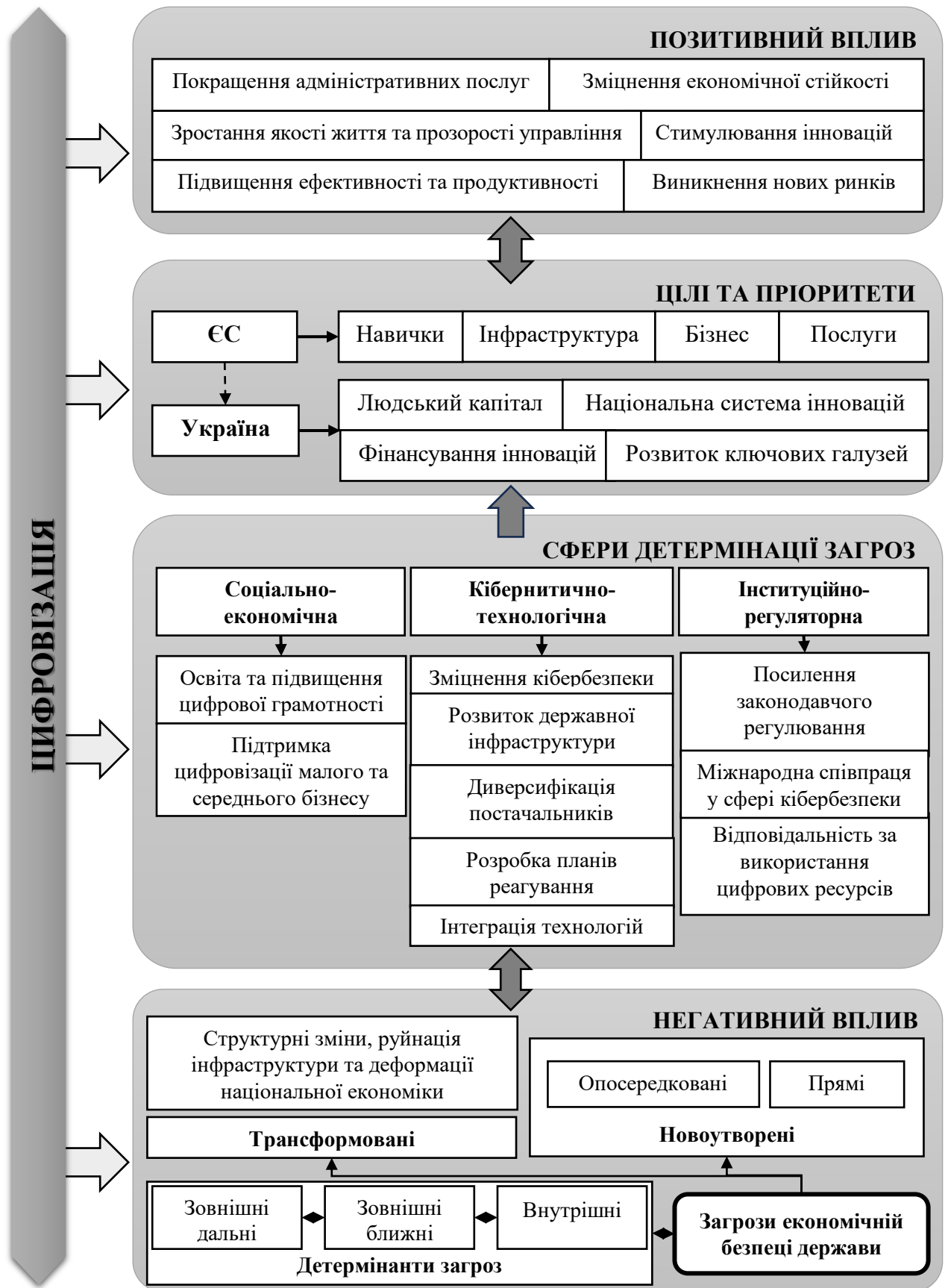


Рис. 1.13. Концептуальні засади розвитку цифровізації в умовах посилення її дуального впливу на загрози економічній безпеці держави

Джерело: розроблено автором

Отже, вплив цифровізації на економічну безпеку є дуальним, комплексним, незворотнім і незалежним. Він, з одного боку, сприяє розвитку економіки, прозорості публічних послуг та зростанню якості життя, але також спричиняє деформації та надає бенефіціарам ризикової поведінки додаткові інструменти для отримання недобросовісної вигоди.

Тому регулювання негативного впливу цифровізації має забезпечуватися та координуватися відповідно до цілей та орієнтирів цифрового розвитку економіки. Утім, виключно внутрішні заходи не можуть вважатися достатніми, оскільки найбільш ефективним захистом від загроз зовнішнього середовища є, насамперед, міжнародна співпраця. Потрібно відмітити, що забезпечення економічної безпеки держави має базуватися на принципах дотримання стабільності, передбачуваності, незалежності та економічного розвитку.

Отже, в умовах воєнного стану та цифровізації Україна має потребу у впровадженні якісно нового підходу до аналізу впливу потенційних і реальних загроз економічній безпеці держави. Такий підхід повинен враховувати особливості трансформаційних процесів, динаміку геополітичного середовища та сучасні технологічні тенденції.

Разом із тим, дуальний вплив цифровізації зумовлює необхідність його регулювання та унормування шляхом діагностики рівня економічної безпеки держави, виявлення та оцінювання потенційних загроз цифровізації. Важливими складовими таких заходів мають бути не лише кількісний аналіз показників впровадження цифрових технологій, а й моніторинг стійкості цифрової інфраструктури та цифрової грамотності населення, оскільки за значеннями цих індикаторів можна оцінювати зростання національної економіки та якості життя від впровадження цифрових технологій, рішень і послуг.

Висновки до розділу 1

1. Узагальнено та систематизовано теоретичні підходи до трактування сутності цифровізації з урахуванням її ролі у трансформації національної економіки. Запропоновано інтегрований підхід до визначення цифровізації шляхом поєднання техніко-форматної, комерційно-оптимізаційної та технологічно-інформаційної концепцій. Обґрунтовано змістовне наповнення категорійного апарату проявів цифровізації, що встановлює структурно-логічні зв'язки між основними поняттями цифрової сфери, а саме цифровою трансформацією, цифровою революцією, цифровою економікою, цифровою інфраструктурою, цифровою грамотністю, цифровими технологіями, рішеннями та послугами, що забезпечує цілісне бачення багатовекторності впливу цифровізації на економічну безпеку держави.

2. Виокремлено основні властивості цифровізації, серед яких адаптивність, мультиплікативність, циклічність розвитку, анонімність, віртуальність, масштабність, мобільність, персоналізація, транспарентність, що визначають особливості трансформації соціально-економічних відносин внаслідок динамічного розвитку цифрової сфери та уможливають ідентифікацію загроз економічній безпеці держави в умовах активного впровадження цифрових технологій.

3. На підставі узагальнення результатів попередніх досліджень, доповнено класифікацію загроз економічній безпеці держави в умовах цифровізації шляхом їх поділу за рівнем походження на наднаціональні й національні, а також за впливом цифрового компонента – на загрози з активним, пасивним та відсутнім впливом цифрового компонента.

4. За результатами бібліографічного аналізу виділено основні кластери загроз економічній безпеці держави в умовах цифровізації, а саме: дезінформація та маніпуляції, цифрові війни та кібершпionaж, несприятливі наслідки впровадження штучного інтелекту та інших цифрових технологій, онлайн-наси́льство, цифрові цензура та нагляд. Виявлено, що загрози

російсько-української війни та радикалізація в мережі Інтернет мають критичний негативний вплив, який виходить далеко за межі виділених кластерів загроз. Обґрунтовано трирівневу систему внутрішніх, ближніх та дальніх зовнішніх детермінант впливу цифровізації на загрози економічній безпеці держави, визначено взаємозв'язок між ними, що дозволило розширити розуміння природи загроз для їх превентивної ідентифікації.

5. Охарактеризовано дуальний вплив цифровізації на економічну безпеку держави, який, з одного боку, полягає у підвищенні стійкості й стимулюванні розвитку національної економіки, а з іншого – виступає каталізатором нових форм загроз та трансформації існуючих. Визначено три сфери детермінації загроз в умовах цифровізації, а саме соціально-економічна, кібернетично-технологічна та інституційно-регуляторна, що слугує підґрунтям для формування стратегічних орієнтирів, пріоритетних напрямів та заходів мінімізації загроз в умовах обмеженості ресурсного потенціалу національної економіки.

Основні результати дослідження відображені у наукових працях автора [183; 201; 207; 208; 209; 212; 213; 214; 216; 215].

РОЗДІЛ 2

ДІАГНОСТИКА ВПЛИВУ ЦИФРОВІЗАЦІЇ НА ЗАГРОЗИ ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ

2.1. Оцінювання рівня економічної безпеки України з урахуванням впливу цифровізації

Оцінювання рівня економічної безпеки України є передумовою для формування й реалізації ефективних механізмів її забезпечення та мінімізації негативного впливу цифровізації. В умовах воєнного стану ідентифікація та оцінювання загроз економічної безпеки держави ускладнена обмеженим доступом до значної кількості її показників. Крім цього, за макроекономічними показниками можна виявити вкрай обмежений перелік сучасних загроз. Для цілого пласту прихованих та комбінованих загроз економічній безпеці держави потрібно використовувати складні математичні моделі. Їх, передусім, можна поділити на кількісні, що передбачають індикаторний аналіз, економетричне та сценарне моделювання, SWOT-аналіз, та якісні, серед яких слід відмітити метод експертних оцінок, аналіз регуляторного впливу, форсайт методи прогнозування. Значну практичну цінність в умовах дуального впливу цифровізації мають комбіновані методи оцінювання економічної безпеки держави, як то інтегральний аналіз, порівняння або бенчмаркінг.

У вітчизняній науковій думці сформувалося кілька методичних підходів до оцінювання економічної безпеки держави. По-перше, це функціональний, який передбачає використання комплексної системи показників, які згортаються з метою отримання інтегрального показника; індикаторний, що ґрунтується на порівнянні фактичних значень ключових показників з встановленими еталонними значеннями; формальний та неформалізовані матричні, які передбачають використання матриць для побудови аналітичних

моделей між різними факторами; експертне оцінювання – у випадках, коли застосування кількісних показників є обмеженим.

Натомість у світовій практиці більш поширена система показників та індексів для міжнародних співставлень, представлених у звітах міжнародних організацій та форумів (табл. 2.1). За допомогою цих показників можна опосередковано визначити рівень економічної безпеки держави, шляхом їх адаптації до національних систем оцінювання, відслідковування динаміки чи порівняння з іншими країнами.

Таблиця 2.1

**Основні міжнародні джерела даних моніторингу показників рівня
економічної безпеки держави**

Організація	Звіт	Опис
Міжнародний валютний фонд	World Economic Outlook	Розрахунок макроекономічних прогнозів та оцінка глобального економічного розвитку.
	Global Financial Stability Report	Звіт про стан міжнародних фінансових ринків, ризиків для банківської системи та вразливості глобальної фінансової інфраструктури.
Міжнародний економічний форум	Global Risks Report	Звіт про стан ключових ризиків світової економіки. Включає питання фінансової стабільності, технологічної трансформації та цифрових загроз.
	The Global Competitiveness Index	Аналіз спроможності країн забезпечити високий рівень процвітання власних громадян, який залежить від ефективності використання державою наявних в неї ресурсів.
Світовий банк	Global Economic Prospects	Оцінка макроекономічних трендів, можливих криз та їхнього впливу на вразливі країни.
	World Development Report	Звіт про стан довгострокових факторів економічного розвитку, зокрема їх цифрових, економічних та соціальних аспектів.
UNCTAD	Digital Economy Report	Звіт про розвиток цифрових технологій та їхній вплив на міжнародну торгівлю, регулювання даних і глобальну цифрову нерівність.
Організація економічного співробітництва та розвитку	Digital Economy Outlook	Оцінка рівня регулювання та впливу цифровізації на продуктивність праці і зайнятість.
	Going Digital: Shaping Policies, Improving Lives	Практичні рекомендації щодо цифрової політики, управління даними та захисту прав у цифровому середовищі.
Банк міжнародних розрахунків	Annual Economic Report	Звіт про глобальні фінансові ризики, монетарну політику та стан банківської системи.
	Digital Currencies and the Future of Monetary Policy	Дослідження ролі цифрових валют центральних банків (CBDC) у фінансовій системі та їх потенційного впливу на глобальну монетарну політику.

Джерело: систематизовано автором на основі [94; 132; 136; 151; 154; 196; 224; 227]

Розвиваючи тему міжнародного досвіду, в ЄС особлива увага приділяється комплексним дворівневим рішенням. Так, першочергово оцінюється економічна безпека на рівні всього об'єднання, а на другому рівні здійснюється моніторинг економічної безпеки національних економік, їх інвестиційної привабливості, дотриманням верховенства права, демократичних цінностей.

Але ці показники специфічні для окремих національних економік, так Ю. Субботович та О. Антропова [96] відзначають специфічні індикатори тривоги у Франції, а у Німеччині акцентують на показниках бюджету. У практиці США, М. Єрмошенко [97] виділяє індикатори короткострокового розвитку економіки, так звані «попередні показники», що сигналізують про небезпеку. А в Австралії акцент зміщується на оцінювання впливу нових регуляторних ініціатив на економічну безпеку. Таким чином, це різноманіття, на нашу думку, відображає існуючу проблему адаптації досвіду та порівняння значень різних національних економік.

Утім, у нових умовах цифровізації та загострення геополітичної напруженості, особливого занепокоєння викликає питання запобігання дезінформації та стійкості цифрової інфраструктури від гібридних кіберзагроз. Тому, актуалізується потреба в інтеграції показників кіберстійкості, рівня цифрового розвитку та інформаційної захищеності в окрему інформаційно-цифрову складову економічної безпеки держави. Виділення і аналіз окремої складової потребуватиме комбінування існуючих підходів та розробку нових. На нашу думку, до них мають належати аналіз макроекономічних показників, стійкості фінансових систем, порівняння ефективності, вразливості та готовності національної економіки до впровадження передових технологій.

В питанні існуючих підходів до оцінювання економічної безпеки держави та ідентифікації її загроз, потрібно відмітити, що основним нормативно-правовим документом України є Методичні рекомендації щодо розрахунку рівня економічної безпеки України [30], втім в них не передбачено інформаційно-цифрової складової.

Загалом інтегральний метод оцінки пропонує послідовну схему, що включає формування переліку індикаторів, встановлення характеристичних значень, нормування даних, визначення вагових коефіцієнтів і розрахунків інтегральних індексів. Значною перевагою такого методу є можливість врахування численних аспектів економічної безпеки держави в одному показнику. Також використання даних Державної служби статистики та інших відомств, у свою чергу, забезпечує офіційність та достовірність розрахунків, а експертне опитування доповнює складні для кількісного вимірювання аспекти.

За результатами детального аналізу переліку показників економічної безпеки України, визначених офіційною методикою, можна виділити ряд її критичних недоліків, що унеможливають отримання достовірних результатів в умовах сьогодення (табл. 2.2). Насамперед, без належної оцінки залишається ряд новітніх загроз, таких як кібернетичні війни, поширення дезінформації та руйнація цифрової інфраструктури. Більше за те, національна методика остаточно втратила свою актуальність в умовах повномасштабного вторгнення Росії, тривалих наслідків пандемії COVID-19 та цифровізації економіки.

Таблиця 2.2

**Критичні аналіз національного методичного інструментарію оцінювання
рівня економічної безпеки України**

Недолік	Опис концептуального недоліку
1	2
Застарілість	Нормативний документ протягом минулих 12 років не мав доповнень чи змін, навіть попри закладений механізм оновлення кожні 5 років. За цей час розрахунок та облік окремих показників припинився, вагові коефіцієнти не відповідають реаліям і потребують перегляду.
Невідповідність стратегічним орієнтирам України	Структура української економіки за 12 років зазнала суттєвих змін внаслідок євроінтеграції, збільшення ролі цифровізації в економіці та актуалізації питань впливу глобальних ланцюгів постачання, критичних технологій та розвитку військово-промислового комплексу в усьому світі, що робить визначені раніше показники невідповідними до нових умов та викликів сучасності, а їх розрахунок не дає відомостей, які б доповнювали оцінку виконання державних стратегій.

Продовження табл. 2.2

1	2
Суперечливість нормативного забезпечення	Методичні рекомендації мають проблеми із правовою визначеністю, оскільки вони не є обов'язковими до виконання. Натомість перелік показників, визначених в Стратегію економічної безпеки України до 2025 року, Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року на період до 2030 року та Стратегії національної безпеки України від 2020 року відрізняється від індикаторів, запропонованих у методиці, що призводить до розрахунку і створення неспівставних даних.
Обмежена адаптивність до глобальних змін	Першочергово методика була розроблена з урахуванням специфіки української економіки на той час, зараз вона втрачає контекст міжнародних співставлень та досвіду ЄС. У 2013 році еталонами виробничої спроможності було обрано показники Китаю та росії, але зараз вони є нерепрезентативними поза показниками військового потенціалу.
Відсутність офіційного розрахунку з 2022 року	Відсутність оцінки інтегрального індексу економічної безпеки в період 2022–2024 років пов'язано з тим, що органи державної статистики не мали можливості забезпечити збір, аналіз та поширення необхідної статистичної інформації в умовах воєнного стану. Тому, з урахуванням норм Закону України від 03.03.2022 № 2115-IX «Про захист інтересів суб'єктів подання звітності та інших документів у період дії воєнного стану або стану війни», розрахунок показників обмежено.
Невідповідність міжнародним співставленням	Індикатори не узгоджуються з міжнародними підходами до оцінки економічної безпеки, не враховують міжнародні рейтинги та індекси, зокрема конкурентоспроможності, економічної свободи, політичної стабільності, прозорості. Це робить національну методику нерелевантною та невідповідною міжнародним співставленням.
Надмірна кількість індикаторів	Використання аж 127 окремих показників, які не відображають сучасних тенденцій внаслідок відсутності їх оновлення, створює труднощі у зборі даних, а також їх узгодженості та регулярному оновленні. Особливо це помітно, коли деякі індикатори публікуються з часовою затримкою або оновлюються нерегулярно.
Фіксованість порогових значень	Методика передбачає використання заздалегідь визначених порогових значень, але це не відображає накопичених змін у внутрішній структурі економіки та зовнішньому середовищі.

Джерело: складено автором

Підсумовуючи, можна зазначити, що національний методичний підхід до оцінювання економічної безпеки держави вже зараз потребує значного оновлення та адаптації до новітніх викликів. Утім, на нашу думку, переваги існуючого підходу спонукають до продовження її використання із рядом удосконалень та доповнень, що дозволить зберегти і збільшити охоплений часовий проміжок розрахунку індикаторів для більшої наочності та проведення майбутніх досліджень.

Головним доповненням має бути виокремлення інформаційно-цифрової складової економічної безпеки. Тобто визначення ряду індикаторів на основі опрацювання законів України та звітів міжнародних організацій, має відповідати на питання впливу цифровізації на торгівлю та технологічну автономію, розвиток людського капіталу та державних цифрових послуг, баланс у впровадженні цифрових технологій та готовність до них, а також кібербезпеку та цифрові загрози загалом.

Отже, для потреби відображення загроз залежності економіки держави від імпорту цифрових технологій та недостатнього розвитку цифрової інфраструктури варто додати до методичних рекомендацій дев'ять індикаторів загроз цифровізації. Так, по-перше, це коефіцієнт покриття експортом імпорту цифрових товарів, який вказуватиме на стан сальдо торгівлі цифровими товарами і послугами, що розкриває характеристику залежності економіки держави від зовнішніх цифрових технологій та рівня технологічного суверенітету. Показники глобального індексу впровадження криптовалюти та приросту дохідності електронної комерції відображатимуть зміну у споживанні цифрових технологій. А вже оцінка рівня цифрової доступності та освіченості населення, разом із коефіцієнтом цифрової грамотності населення та часткою підприємств, які проводили навчання ІКТ, як і частка підприємств, які використовують штучний інтелект, вказуватимуть на реакцію середовища та зростання (падіння) попиту на цифрові технології і потребу в їх імпорті.

Наостанок, про розвиток цифрової інфраструктури свідчитимуть частка населення з доступом до мережі Інтернет та частка населення з доступом до фіксованого широкосмугового зв'язку, що визначає покриття мережі загалом та рівень проникнення провідних технологій високошвидкісного інтернет-зв'язку.

Для ідентифікації іншого порядку загроз, а саме дисбалансу між традиційними та провідними галузями сучасної національної економіки, в питанні впровадження цифрових технологій, що призводить до втрати технологічної конкурентоспроможності та деградації сектору традиційного виробництва доцільно розраховувати три відповідні індикатори. А саме, коефіцієнт структурних

деформацій, що відображає частку зниження частки традиційного виробництва через зростаючий вплив цифровізації, у поєднанні з оцінкою розриву впровадження цифровізації та різницею частки ІКТ у ВВП України та Росії.

Зважаючи на актуалізацію проблематики кібербезпеки, доцільно додатково визначати два індикатори для оцінювання впливу загроз економічній безпеці держави, пов'язаних із кібератаками та контролем над інформаційним простором. Це має бути показник цифрової вразливості, що відображатиме рівень захищеності економіки від цифрових атак з одного боку, а з іншого – індекс свободи інтернету, що характеризує ступінь обмежень у доступі до інтернету, рівень державного контролю та свободу цифрового простору. Тобто це означає, що рівень захищеності від кіберзагроз не має зростати за рахунок надлишкових обмежень прав і свобод в мережі Інтернет.

Також для ідентифікації ефективності впровадження цифровізації у питанні державного управління, обмежень та стимулів, слід скористатися трьома інтегральними рейтинговими оцінками. До методичних рекомендацій, на нашу думку, варто додати рівень розвитку цифрових послуг, розвитку цифрової держави та індекс готовності до передових технологій. Ці показники послідовно вимірюють ефективність надання державних цифрових послуг, рівень електронного урядування, тобто слугують індикатором здатності національної економіки, її суб'єктів та інфраструктури, до впровадження новітніх цифрових технологій.

Тому, доцільно розглядати інформаційно-цифрову складову економічної безпеки держави саме через діяльність суб'єктів макро-, мікро- та нанорівня (табл. 2.3). Це спричинено характерними властивостями цифровізації та значних відмінностях у прояві її загроз економічній безпеці держави, які були зазначені у підрозділі 1.2.

Для розрахунку критичних значень, спершу варто визначили їх аналогічно до вже існуючих показників методичних рекомендацій, якщо це не можливо то використовуються значення середньоєвропейських показників. І якщо аналогічні показники відсутні, то застосовується нормативне або граничне значення межі позитивного впливу.

Таблиця 2.3

Перелік індикаторів оцінювання впливу цифровізації на економічну безпеку України через діяльність суб'єктів макро-, мікро- та нанорівня національної економіки

Показник	Розрахунок	Тип	Критичне значення	Джерело
1	2	3	4	5
Макрорівень				
Коефіцієнт покриття експортом імпорту цифрових товарів	Частка експорту ІКТ товарів та послуг у загальному обсязі / Частка імпорту ІКТ товарів та послуг у загальному обсязі	Стим. Дестим.	0,85; 1,7	[130-132]
Коефіцієнт цифрової структурних деформацій економіки	Частка ІКТ України, відсоток до відповідного періоду попереднього року / Частка приросту електроенергії України до приросту ВВП, відсоток до відповідного періоду попереднього року	Дестим.	1	[100]
Розрив між провідними галузями цифрової трансформації та найбільшими секторами економіки	Рівень цифрової трансформації провідних галузей / рівень цифрової трансформації найбільших галузей за обсягом експорту	Дестим.	1	[184]
Різниця частки ІКТ у ВВП України та Росії, відсоткових пунктів	Частка ІКТ України, відсоток до відповідного періоду попереднього року – частка ІКТ Росії, відсоток до відповідного періоду попереднього року	Стим.	-5	[184, 196-198]
Показник цифрової вразливості	Число кібератак в Україні, відсоток до відповідного періоду попереднього року / Загальне число кібератак у світі, відсоток до відповідного періоду попереднього року	Дестим.	1	[148, 149]
Рівень розвитку цифрових послуг	Дані DESA	Стим.	0,783	[223]
Рівень розвитку цифрової держави	Дані DESA	Стим.	0,849	[223]
Індекс готовності до передових технологій	Дані UNCTAD	Стим.	0,7	[132]
Глобальний індекс впровадження криптовалют	Дані The Blockchain Data Platform	Стим.	0,1	[83]
Свободи Інтернету	Дані Freedom House	Стим.	70	[225]

Продовження табл. 2.3

Мікрорівень				
1	2	3	4	5
Приріст дохідності електронної комерції	(Дохідність за поточний рік, дол. США/ дохідність за попередній рік)/ індекс споживчих цін	Стим.	1	[133]
Частка підприємств, які проводили навчання ІКТ для працівників в Україні та країнах Європи	Середнє значення показника навчання ІКТ в Україні / значення показника навчання ІКТ в Європі за DESI (20%)	Стим.	1	[184]
Частка кількості підприємств, що використовують технології ІІІ в Україні та країнах Європи	Значення використання ІІІ в Україні / середнє значення показника в Європі	Стим.	1	[184, 233]
Нанорівень				
Частка населення з доступом до мережі Інтернет	Дані Державної служби статистики України	Стим.	91	[134, 184]
Частка населення з доступом до фіксованого широкосмугового зв'язку	Дані Світового банку	Стим.	32,5	[224]
Коефіцієнт цифрової грамотності населення	Частка населення з високими цифровими навичками / частка населення з середніми цифровими навичками	Стим.	1	[134]

Джерело: авторська розробка

Розрахунок індикаторів оцінювання впливу цифровізації на економічну безпеку України через діяльність суб'єктів макро-, мікро- та нанорівня національної економіки дозволяє уникнути концептуальних недоліків існуючого національного методичного інструментарію та здійснювати ідентифікацію загроз інформаційно-цифровій складові економічної безпеки держави. Варто врахувати, що поділ індикаторів на стимулятори (прямий вплив на рівень економічної безпеки) та дестимулятори (зворотній вплив на рівень економічної безпеки) дозволяє ідентифікувати дуальний вплив цифровізації, який породжує асиметрію розвитку національної економіки.

Далі, продовжуючи адаптацію національної методики до ідентифікації впливу цифровізації на формування загроз економічній безпеці держави, доцільно проводити аналіз, шляхом визначення відношення значення оцінки індикатора до граничного рівня для стимуляторів та дестимуляторів (2.1).

$$\begin{cases} \frac{x_i}{\lim_{Dst} x_i}, & x \leq \lim_{Dst} x_i \\ \frac{\lim_{St} x_i}{x_i}, & x \geq \lim_{St} x_i \end{cases}, \quad (2.1)$$

де x_i – показник за відповідний період;

$\lim_i$ – граничне значення показника;

St – значення для стимуляторів;

Dst – значення для дестимуляторів.

Отримане значення індикатора або групи близьких індикаторів у межах від 0 до 0,5 означає незначущу або відсутність загрози. Про потенційну загрозу свідчитимуть значення від 0,51 до 0,99, а про реальні загрози свідчить відхилення за межі критичного значення від 1,0 і більше. Визначення відхилення показника від граничного значення дозволить не лише оцінити рівень критичності загрози економічній безпеці держави, а й визначити місце загроз інформаційно-цифровій складової економічної безпеки серед них.

На основі розглянутих теоретичних і методичних засад доцільним є проведення інтегральної оцінки рівня економічної безпеки України. В подальшій роботі вона дозволить забезпечити інформаційною базою аналіз сучасних тенденцій впливу цифровізації на загрози економічній безпеці. Тому, попри всю недосконалість Методичних рекомендацій щодо розрахунку рівня економічної безпеки України, визначення та аналіз індикаторів є необхідною передумовою для формування комплексного уявлення про загрози економічній безпеці держави. Звісно, не всі показники дозволяють оцінити вплив цифровізації, проте всі вони загалом дозволяють виокремити загальні тенденції.

Відповідно розрахунок рівня економічної безпеки України здійснюється на основі даних Міністерства економіки України [98-99; 228]. Вона передбачає агрегування показників за напрямками, нормалізацію для усунення відмінностей у масштабах вимірювання та вагову корекцію індикаторів, аби врахувати їхній відносний вплив. Потрібно зазначити, що переваги

національної методики оцінки рівня економічної безпеки, а саме комплексність, системність та нормативна визначеність створюють умови для формування цілісної картини шляхом визначення інтегрального показника за 2010-2022 роки (табл. 2.4). Такі розрахунки є передумовою для ретроспективного аналізу основних тенденцій та визначення впливу цифровізації на загрози економічній безпеці держави в умовах війни.

Таблиця 2.4

Рівень економічної безпеки України (інтегральний та
за окремими складовими) за 2010-2023 роки, %

Складові	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Виробнича	50	55	49	49	51	47	58	59	58	57	54	56	49	н/д
Демографічна	47	56	45	46	45	43	46	40	41	39	40	37	37	н/д
Енергетична	35	32	34	39	47	45	58	54	53	49	49	52	47	н/д
Зовнішньо-економічна	35	31	24	29	32	33	35	36	36	40	44	42	37	н/д
Інвестиційно-інноваційна	33	34	36	35	30	33	30	30	31	31	31	30	28	н/д
Макро-економічна	38	48	39	39	33	30	38	37	40	45	43	41	36	н/д
Продовольча	90	92	93	86	94	92	92	91	90	89	85	88	88	н/д
Соціальна	57	59	64	62	57	55	56	59	59	60	59	61	60	н/д
Фінансова	42	47	47	50	40	35	38	40	45	42	40	40	33	31
Інтегральний показник	46	49	46	47	45	44	48	48	49	49	48	47	45	н/д

Джерело: за офіційною відповіддю Міністерства економіки України на запит щодо надання публічної інформації про показники економічної безпеки України [98-99]

*н/д – відсутність оцінки інтегрального індексу економічної безпеки в період 2022–2024 років пов'язано з тим, що органи державної статистики не мали можливості забезпечити збір, аналіз та поширення необхідної статистичної інформації в умовах воєнного стану. Тому, з урахуванням норм Закону України від 03.03.2022 № 2115-IX «Про захист інтересів суб'єктів подання звітності та інших документів у період дії воєнного стану або стану війни», розрахунок показників обмежено.

Загалом, середнє значення інтегрального показника економічної безпеки України за весь розрахований період дорівнює 47% від оптимального значення. Це вказує на незадовільний рівень економічної безпеки України.

Переходячи до більш детального аналізу індексів складових цього показника, лише значення його продовольчої складової знаходиться на оптимальному рівні, а значення соціальної та виробничої на задовільному. Утім, варто відмітити, що граничні значення індикаторів соціальної та продовольчої складових економічної безпеки держави є заниженими, що робить ці показники менш релевантними, а оцінку завищеною.

Варто зауважити, що протягом 2015-2019 рр. спостерігалася позитивна тенденція до зростання рівня економічної безпеки України, втім пандемія COVID-19 сповільнила її. В шокових умовах повномасштабного російського вторгнення у 2022 році значення інвестиційно-інноваційної (28%), демографічної (37%) та фінансової (33%) складових економічної безпеки держави досягли своїх історичних мінімумів, при цьому низькі показники макроекономічної (36%) та зовнішньо-економічної (37%) складових також зумовили зниження інтегрального показника рівня економічної безпеки України.

Найгірші середні значення індексів інноваційно-інвестиційної та зовнішньо-економічної складових у 28% та 37% відповідно, свідчать про найбільшу концентрацію загроз економічній безпеці України саме в цих сферах. Зокрема, тенденція до зростання частки експорту товарів сировинного та низького ступеня переробки з 74% у 2010 році до 87% у 2022 році від загального експорту [98-99] з відповідним зростанням частки експорту сектору ІКТ в загальному обсязі [184], можна зробити припущення про локальність сприятливого впливу цифровізації у зовнішній торгівлі та інноваціях, без масштабування на загальний інноваційний розвиток національної економіки України.

Утім, на противагу, позитивний вплив цифровізації проявляється у тенденції до зростання таких індикаторів економічної безпеки України, як питома вага підприємств, що впроваджували інновації; відношення експорту роялті, ліцензійних послуг, комп'ютерних та інформаційних послуг, наукових та конструкторських розробок, послуг у архітектурних, інженерних та інших

технічних галузях; частка осіб, які повідомили, що за останні 12 місяців користувалися послугами Інтернету (рис. 2.1).

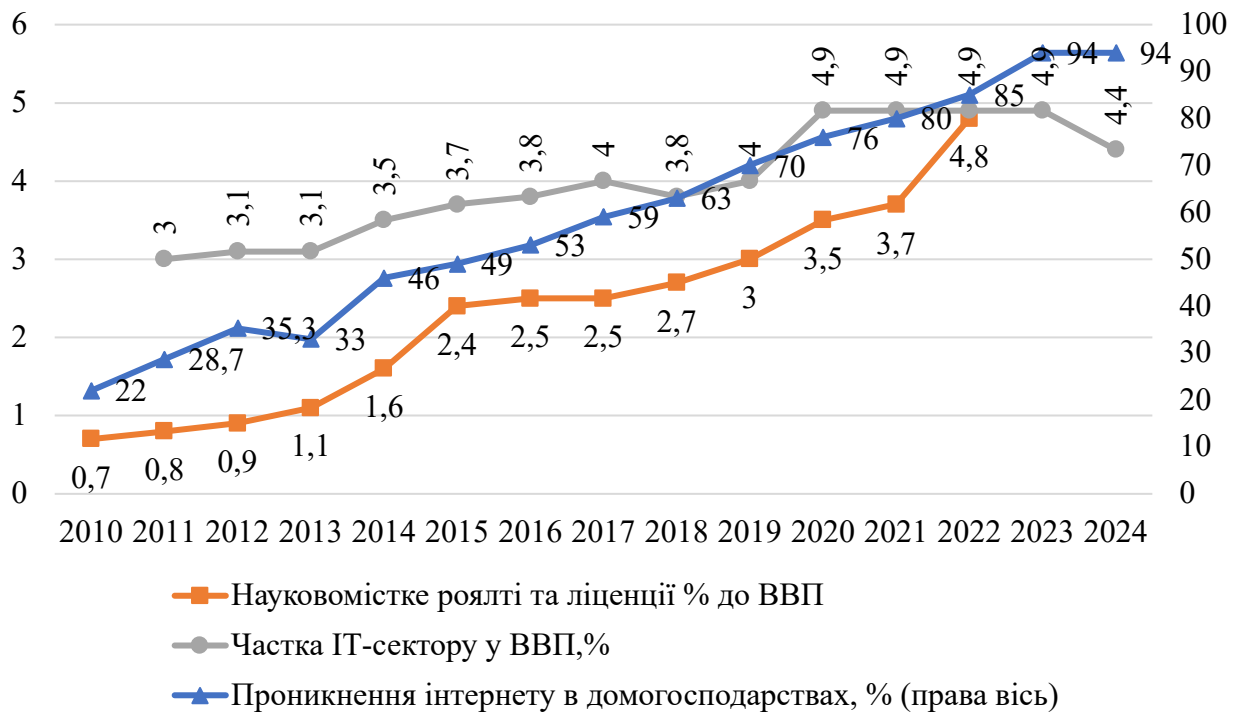


Рис. 2.1. Вплив цифровізації на інноваційну складову економічної безпеки України за 2010-2024 роки

Джерело: побудовано автором на основі [30; 98-100; 184]

За результатами аналізу виявлено взаємозв'язок приросту показників сектору ІКТ у ВВП і зростання наукомістких роялті в середньому на 0,45% за кожні 5,5% проникнення Інтернету в домогосподарствах. Це підтверджує позитивний вплив цифровізації на інноваційний розвиток економіки.

На загрозу зменшення конкурентоспроможності та інвестиційної привабливості національної економіки додатково вказують критично низькі показники реалізації інноваційної продукції у 2% та відношення чистого приросту прямих іноземних інвестицій до ВВП. Отже, нестача внутрішніх інвестиційних ресурсів призводить до подальшого падіння наукомісткого виробництва.

Значення іншого показника конкурентоспроможності національної економіки, а саме питомої ваги обсягу виконаних наукових замовлень у ВВП зменшилося з 0,75% у 2010 році до 0,41% у 2020 році, а кількість спеціалістів,

що виконують відповідні роботи на 1000 населення зменшилася відповідно з 8 до 3,5 чоловік. Такі показники підкреслюють загрозу науково-технічного і інноваційного відставання України від середньоєвропейських показників, що потребує особливої уваги в умовах євроінтеграції.

В контексті кадрового забезпечення цифровізації, варто звернути увагу на суттєве падіння індексу демографічної складової економічної безпеки України з 56% у 2011 році до 37% у 2022 році внаслідок демографічної кризи. Відзначена тенденція є наслідком, у тому числі, тривалої зовнішньої міграції, зокрема, кваліфікованої робочої сили, яка посилилася внаслідок уніфікації цифрових навичок та масштабної еміграції населення внаслідок повномасштабного вторгнення росії у 2022 році. При цьому, в умовах воєнних дій, зростає загроза фізичних втрат економічно-активного населення.

Особливо небезпечні загрози економічній безпеці України в умовах воєнного стану сконцентровані у фінансовій сфері, що послаблюють стійкість фінансової системи та ускладнюють реалізацію ефективної державної економічної політики. Про це свідчить критичне значення індикатора фінансової складової економічної безпеки держави, що становить 31% у 2023 році. Ситуація значно погіршилася, починаючи з 2022 року, через суттєве зростання дефіциту державного бюджету, а також гарантованого та державного боргу України, який збільшився до 110% від ВВП у 2024 році [100].

Як наслідок, показники боргової складової фінансової безпеки України знаходяться у найгіршому стані, внаслідок чого індекс боргової безпеки становить лише 20% від оптимального значення. В умовах тривалої війни зростає загроза боргової залежності України, що призвело до зниження її суверенного рейтингу в іноземній валюті з «ССС» до рівня «СС» з подальшим негативним прогнозом [232]. При цьому, ціна облігацій внутрішньої державної позики у національній валюті є досить високою (в середньому 15% [100]), що зумовлює подальше зростання боргового навантаження на державний бюджет України. Зазначена загроза посилюється скороченням

заощаджень, зменшенням внутрішнього інвестиційного ресурсу, про сигналізують індикатори банківської безпеки України.

Мінімізація зазначених загроз ускладнюється слабким рівнем розвитку небанківського фінансового сектору, попри те, що цифрові технології знайшли широке застосування в страхових компаніях, діяльності криптобірж та онлайн-брокерів.

Разом із цим, ситуація з валютною підскладовою фінансової безпеки України дещо краща, має середні 44% від оптимального значення і зберігає позитивну тенденцію. Також, аналізуючи волатильність гривні у 2022 році, державі вдалося стримати девальвацію в межах 35%, а у 2023-2024 рр. вона не перевищила 5-10% [100]. Проте, в сучасних умовах, показники валютної підскладової є менш репрезентативними, оскільки не враховують зростаючий в Україні попит на криптовалюту та токени «твердих» валют.

В умовах сьогодення, варто відмітити потенційну загрозу структурного безробіття під впливом цифровізації внаслідок змін у структурі економіки через впровадження цифрових технологій.

Також, протягом досліджуваного періоду, стійким залишається тренд «тінізації» економіки, про що сигналізує значення індикатора частки населення, зайнятого в неформальній економіці, на рівні 20-30% від загальної кількості [100]. Разом із цим, цифровізація має значний негативний вплив на «тінізацію» економіки, що є загрозою економічній безпеці держави, оскільки кримінальні та «сірі» цифрові інструменти є зручними для функціонування паралельних фінансових систем, зокрема, використання криптовалютних розрахунків за заборонені товари та формування мережі цифрових посередників для відмивання коштів, отриманих злочинним шляхом.

На незадовільному рівні також знаходиться індекс виробничої складової економічної безпеки держави, значення якого становить 49% у 2022 році. Утім, інтеграція цифрових технологій у діяльність великого бізнесу імовірно мала вплив на зростання рентабельності операційної діяльності підприємств сектору ІКТ, а значення частки високотехнологічної продукції в загальному

обсязі реалізованої промислової продукції було в межах 40-60% і зберігало позитивний тренд до 2022 року.

Наостанок, варто зауважити, що енергетична складова економічної безпеки держави, індекс якої становить 47% та відповідає незадовільному рівню, тісно пов'язана з процесами цифровізації і має на них суттєвий вплив, хоча жоден з її індикаторів не відображає прямої залежності цифрової інфраструктури від енергетичної. Утім, стрімке нарощення використання комп'ютерів, мобільного- та інтернет-зв'язку створює потребу в безперервному енергозабезпеченні всіх суб'єктів національної економіки. Тобто широке використання цифрових технологій в бізнес-процесах та державному управлінні суттєво ускладнюють, а в окремих випадках унеможливають стабільне функціонування національної економіки без доступу її суб'єктів до мережі Інтернет та стабільного енергозабезпечення.

Разом із цим, фізична руйнація енергетичної інфраструктури внаслідок ракетних атак ускладнила протидію загрозі енергозалежності національної економіки в умовах цифровізації. Так, попри скорочення ВВП на 20,9% [184], протягом 2022-2024 рр. була актуальною потреба обмеження споживання електроенергії для розвантаження енергетичної системи. У цьому контексті, прослідковується відмінність між традиційними енергоємними секторами великого виробництва, які потребують значних обсягів електроенергії для забезпечення технологічних процесів, та сектору ІКТ, який споживає мало електроенергії, проте критично залежний від її безперервного постачання.

Отже, за результатами проведеного аналізу рівня економічної безпеки України за національною методикою варто відмітити, що сучасні прояви цифровізації знаходяться поза межами оцінювання. Тому, далі, в межах роботи, доцільно розглянути вплив цифровізації на загрози економічній безпеці України крізь призму виокремлених індикаторів інформаційно-цифрової складової.

2.2. Ідентифікація потенційних та реальних загроз економічній безпеці держави в умовах цифровізації

У процесі ідентифікації загроз економічній безпеці держави в умовах цифровізації актуальним питанням залишається їх ранжування у відповідності до потенційної небезпеки, яку вони становлять. Такий підхід дозволяє акцентувати зусилля держави на протидії найбільш небезпечним загрозам, зважаючи на обмежені ресурси та можливості.

Так, у питанні категоризації загроз економічній безпеці держави важливу практичну цінність має їх поділ на потенційні та реальні. Згідно з визначенням О. Пугач [45] за потенційних загроз існує ймовірність завдання певної шкоди національній економічній системі, але її обсяги і масштаби не становлять значної небезпеки. Натомість, реальні загрози можуть завдати значної шкоди, що перешкоджає реалізації національних економічних інтересів. Цілком погоджуючись із таким поділом, у продовження, вважаємо за доцільне розглядати загрози економічній безпеці держави через діяльність суб'єктів на макро-, мікро- і нанорівнях національної економіки. Такий підхід, на нашу думку, щонайкраще дозволить ідентифікувати джерело та специфіку загроз інформаційно-цифровій складовій економічної безпеки держави.

З використанням запропонованої у підрозділі 2.1 цієї роботи переліку індикаторів інформаційно-цифрової складової економічної безпеки держави доцільно здійснити ідентифікацію реальних і потенційних загроз економічній безпеці України (табл. 2.5-2.7).

Утім, розрахунок показників індикаторів інформаційно-цифрової складової економічної безпеки України за 2022 рік є ускладненим, зважаючи на специфіку збору статистичних даних в Україні Державною службою статистики [184] та Національним банком України [100] з 2022 року в умовах воєнних дій, періодичністю публікації звітів Міністерства цифрової трансформації [134] та окремих показників UNCTAD [132] раз на два роки.

Таблиця 2.5

Фактичні значення індикаторів інформаційно-цифрової складової економічної безпеки України на макрорівні діяльності суб'єктів національної економіки

Показник	Критичне значення	Фактичне значення		Відхилення показника	
		2021	2023	2021	2023
Коефіцієнт покриття експортом імпорту цифрових товарів	0,85; 1,7	0,12	0,13	7,03	7,01
Коефіцієнт цифрової деіндустріалізації реального сектору	1	0,95	3,57	0,05	3,57
Різниця частки ІКТ у ВВП України та росії, відсоткових пунктів	-5	1,9	0,1	0	0
Розрив між провідними галузями цифрової трансформації та найбільшими секторами економіки	1	1,88	1,89	1,88	1,89
Показник цифрової незахищеності	1	2,041	1,557	2,041	1,557
Рівень розвитку цифрових послуг	0,783	0,814	0,985	0,96	0,79
Рівень розвитку цифрової держави	0,849	0,802	0,884	1,05	1,16
Індекс готовності до передових технологій	0,7	0,6	0,6*	1,16	1,16
Глобальний індекс впровадження криптовалюти	0,101	0,694	0,407	0,14	0,1
Свободи Інтернету	70	59	59	1,18	1,18

Джерело: побудовано автором за даними джерел [100; 132-134; 184; 198]

*періодичність публікацій частини вхідних даних не включає 2022 рік

Розраховані значення індикаторів свідчать про загрозу втрати загальної конкурентоспроможності сектору ІКТ на внутрішньому ринку України, відхилення коефіцієнту покриття експортом імпорту цифрових товарів у 7 разів від критичного значення сигналізує про недостатнє забезпечення попиту на цифрові товари національним виробником. Відхилення коефіцієнта цифрової деіндустріалізації реального сектору у більш ніж 3,5 разів та відхилення показника розриву між провідними галузями цифрової трансформації та найбільшими секторами економіки у 1,8 разів свідчить про те, що джерелом структурних

деформацій національної економіки є асиметричний вплив цифровізації на розвиток суб'єктів макrorівня національної економіки.

На противагу, показники цифрової держави та сервісів, готовності до передових технологій, технологічної конкурентоспроможності і впровадження криптовалюти знаходяться у помірковано оптимальних межах. Так, відхилення показників, в межах 0,79-1,16, свідчить про сприятливі умови для інноваційного розвитку національної економіки. Утім, визначені загрози інформаційно-цифровій складовій економічної безпеки України на макrorівні, а саме залежність від імпорту цифрових технологій та структурні деформації обмежують реалізацію інноваційного потенціалу, підвищують вразливість цифрової інфраструктури та турбулентність національної економіки.

Тому на більш низьких рівнях національної економіки важливим фактором забезпечення економічної безпеки є активна участь самих суб'єктів та розвитку інституцій захисту цифрової інфраструктури та регулювання електронної торгівлі. Так, суб'єкти сектору ІКТ не лише забезпечують власну економічній й інформаційну безпеку, а й створюють інструменти та механізми захисту від загроз цифровізації економіки. Тому, далі варто перейти до розгляду індикаторів інформаційно-цифрової складової економічної безпеки України на мікрорівні діяльності суб'єктів національної економіки (табл. 2.6).

Таблиця 2.6

Фактичні значення індикаторів інформаційно-цифрової складової економічної безпеки України на мікрорівні діяльності суб'єктів національної економіки

Показник	Критичне значення	Фактичне значення		Відхилення показника	
		2021	2023	2021	2023
Приріст дохідності електронної комерції	1	2,77	1,91	2,77	1,91
Середнє співвідношення підприємств, які проводили навчання ІКТ для працівників в Україні та країнах Європи	1	4,54	4,25	4,54	4,25
Частка кількості підприємств, що використовують технології ІІІ в Україні та країнах Європи	1	0,65	0,4	0,65	0,4

Джерело: побудовано автором за даними джерел [134; 184]

*періодичність публікацій частини вхідних даних не включає 2022 рік

Варто відмітити, що показник приросту дохідності електронної комерції у 2-3 рази свідчить про зміну не лише процесу споживання, а й формування ринкових процесів у торгівлі. Активний розвиток бізнесу, пов'язаного з цифровими технологіями, прискорює зменшення частки сектору традиційного виробництва у ВВП.

Разом із тим, загрози структурних деформацій інформаційно-цифрової складової економічної безпеки України на мікрорівні діяльності суб'єктів національної економіки набувають вираження і в питанні кваліфікації робочої сили. Так, зважаючи на співвідношення підприємств, які проводили навчання ІКТ для працівників в Україні та країнах Європи, можна відмітити відставання України за цим показником у понад 4 рази. У свою чергу, відсутність у працівників нових навичок призводить не лише до зменшення конкурентоспроможності національної економіки, а й до зростання залежності від технологічного імпорту. А супутній розвиток цифрової інфраструктури для електронної комерції може генерувати загрозу зростання інтернет-злочинності та значно збільшити економічні втрати від кібератак та кібершахрайства (рис. 2.2).

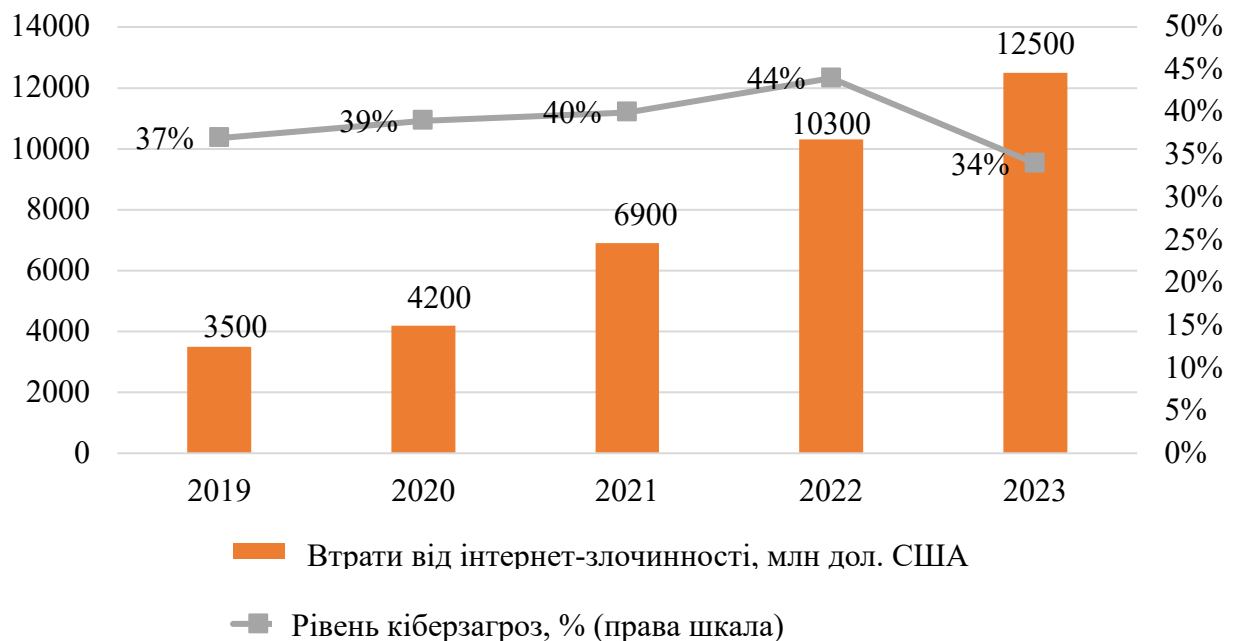


Рис. 2.2. Індикатори кіберзагроз економічній безпеці держави за 2019-2023 роки

Джерело: побудовано автором на основі [112-115]

Не зважаючи на падіння рівня кіберзагроз на 10% у 2023 році за результатами експертного опитування Allianz Risk Barometer [112], відмічається щорічне зростання втрат від кіберзлочинності [113], що у 2023 році збільшилися більш ніж в 3,5 рази порівняно 2019 роком.

Варто виділити, диспропорцію сальдо цифрової торгівлі України (рис. 2.3), оскільки частка імпорту в 4 рази переважає частку експорту ІКТ сектору, а це, в свою чергу, може свідчити про падіння конкурентоспроможності сектору ІКТ. І хоча виявлено позитивну тенденцію до зменшення розвитку з понад 6 до 4,5 разів протягом 2019-2023 рр., утім, приріст частки експорту ІКТ товарів є незначним та становив лише 0,08 в.п. за відповідний період.

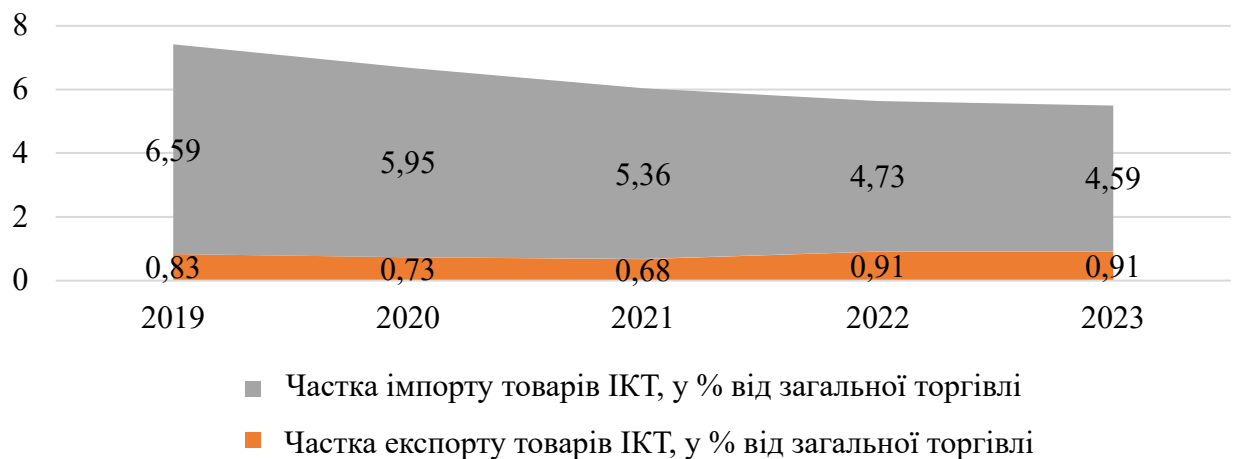


Рис. 2.3. Показники торгівлі товарами ІКТ України за 2019-2023 роки
Джерело: побудовано автором на основі [100]

Також ідентифіковано загрозу когнітивних упереджень та завищених очікувань від цифрових технологій. Так, попри увагу приділену цифровізації в національних стратегіях, дохід від електронної комерції пропорційний індексу ділових очікувань (рис. 2.4). Тому, погоджуємося з думкою Б.Б. Кларка, К. Роберта та С.А. Гемптона [221], що відзначають схильність до інвестицій у технологічні галузі, попри однакові фінансові очікування. А це, в свою чергу, підкреслює асиметричний розвиток національної економіки в умовах цифровізації у напрямку зростання сектору ІКТ.

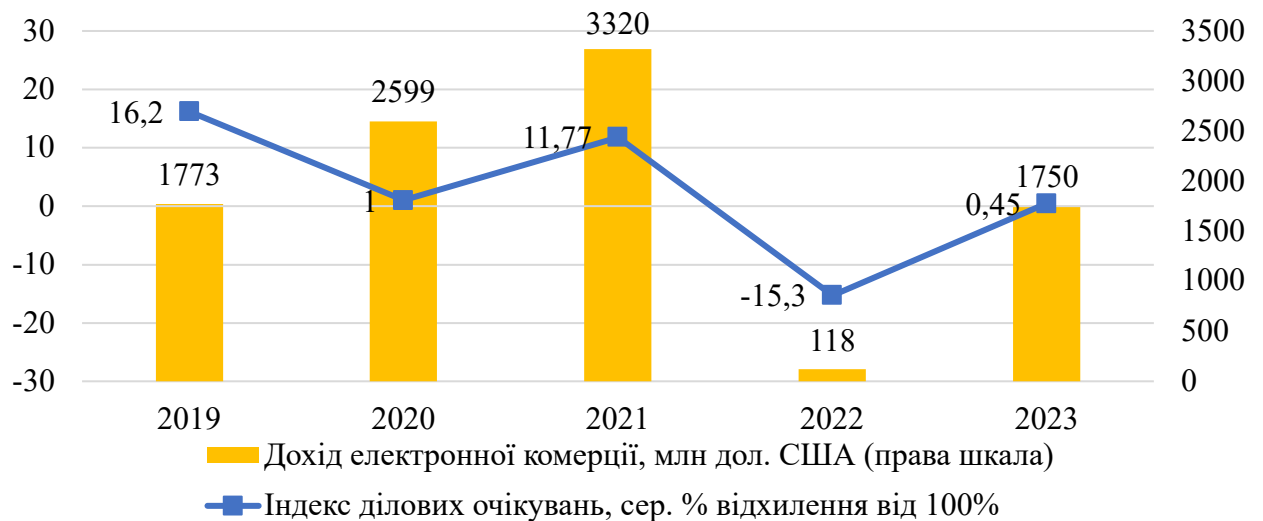


Рис. 2.4. Показники електронної комерції та ділових очікувань в Україні за 2019-2023 роки

Джерело: побудовано автором на основі [130-134]

Варто зауважити про ще одну загрозу діяльності суб'єктів мікрорівня за даними Банку Англії [111], а саме вразливості систем кібербезпеки малого бізнесу через недостатній рівень моніторингу та контролю кіберінцидентів порівняно з середнім та великим бізнесом, тоді як малий бізнес значно частіше зіштовхується або стає посередником для організованої транскордонної цифрової злочинності. Так, середні та великі компанії повідомляють про кіберінциденти на 20% та 24% частіше і здійснюють аудит систем цифрової безпеки на 32% та 43% частіше за середній показник відповідно [111].

За опитуванням американських компаній, проведеним International Business Machines Corporation у 2024 році [74], лише третина порушень даних були виявлені службами внутрішньої безпеки компаній, а 27% були розкриті самими зловмисниками. Значна частка невиявлених порушень може свідчити про нестачу кваліфікації у забезпеченні економічної безпеки на мікрорівні, разом із зростанням кіберризиків і кіберзагроз в умовах цифровізації.

Отже, зважаючи на переважання цифрового імпорту, нестачу професійного навчання для працівників та макроекономічну нестабільність, активний розвиток цифровізації мав позитивний вплив для бенефіціарів

ризикової поведінки, які експлуатують вразливості національної економіки та генерують загрози економічній безпеці держави з метою отримання власної вигоди.

Окремо варто зауважити, що у випадку глобальних криз (пандемій, війн, стихійного лиха) першочерговим для суб'єктів діяльності на мікрорівні є виживання, що призводить до довгострокового падіння рівня безпеки цифрового середовища, погіршення цифрових навичок та утворенню сприятливого середовища для виникнення та поширення загроз вже на рівні діяльності суб'єктів нанорівня національної економіки.

Загалом, найсприятливішим середовищем для формування та поширення загроз економічній безпеці України в умовах цифровізації є нанорівень національної економіки, зважаючи на обмежені ресурси, компетенції, заходи реагування та ієрархічну підпорядкованість домогосподарств. Так, діяльність суб'єктів нанорівня економічної безпеки держави розглядається через захист добробуту громадян, що полягає у виявленні, попередженні та мінімізації загроз особистим фінансам.

Разом із цим, кінцевими бенефіціарами безпекозабезпечувальної діяльності держави, згідно Стратегії національної безпеки України «Безпека людини – безпека країни» [121] визначається людина, її життя і здоров'я, честь і гідність, недоторканність і безпека як найвища цінність в Україні. Саме тому здатність ідентифікувати та протидіяти загрозам на цьому рівні є критичною складовою, а тому існує відповідна потреба визначення індикаторів інформацій-цифрової складової економічної безпеки на нанорівні діяльності суб'єктів національної економіки (табл. 2.7).

За результатами розрахунків можна зробити висновок про поглиблення цифровізації серед домогосподарств. Про це свідчить динаміка показника покриття мережею Інтернет, значення якого досягло 94% у 2023 році, що вказує на залученість понад 28 мільйонів українців до використання цифрової інфраструктури.

Таблиця 2.7

Фактичні значення індикаторів інформаційно-цифрової складової економічної безпеки України на нанорівні діяльності суб'єктів національної економіки

Показник	Критичне значення	Фактичне значення		Відхилення показника	
		2021	2023	2021	2023
Покриття домогосподарств Інтернетом	91	85	94	1,08	0,96
Частка населення з доступом до мережі Інтернет	32,5	17,54	19,68	1,85	1,65
Частка населення з доступом до фіксованого широкосмугового зв'язку	1	1,13	1,47	0,88	0,68

Джерело: побудовано автором за даними джерел [134; 184; 224]

*періодичність публікацій частини вхідних даних не включає 2022 рік

Утім, показник широкосмугового зв'язку покриває усього 20% домогосподарств, що в умовах зростаючих потреб населення призводить до уповільнення розвитку цифрових компетенцій користувачів цифрових послуг та технологічного відставання постачальників цих послуг. Разом із тим, за результатами опитування у «Дія.Сіті» у 2023 році [229] виявлено, що частка населення з високими і середніми цифровими компетенціями складає 53%, що є недостатнім показником в умовах цифровізації та потребує подальшого розвитку їх цифрових навичок.

Необхідно також зазначити, що значна кількість загроз, зумовлених цифровізацією, не може бути кількісно оцінена, а також можуть бути проблеми із ідентифікацією окремих із них. Для прикладу, саме на мікро- та нанорівні діяльності суб'єктів національної економіки, особливої уваги потребує фішинг – один із методів шахрайства з використанням соціальної інженерії, який полягає в тому, що зловмисники, імітуючи діяльність реально існуючих компаній та банків-емітентів та використовуючи неголосові засоби комунікації, під різними приводами намагаються отримати у держателів платіжних карток їх реквізити та іншу конфіденційну інформацію [107].

Наслідком скомпрометованої інформації можуть бути: доступ злочинців до банківських акаунтів, конфіденційної інформації, отримання адміністраторських повноважень, інсайдерська торгівля тощо.

Так, фішинг складає понад 80% зареєстрованих інцидентів кібербезпеки, а згідно зі звітом CISCO [104], близько 90% порушень даних відбуваються через фішинг. Що стосується цілеспрямованих атак, то 65% загроз з активною складовою поклалися на «списовий фішинг» (спеціально персоналізований, підготовлений та націлений на конкретну особу), як основний вектор компрометації програмного забезпечення [105]. Про це свідчить і те, що половина фішингових вкладень електронної пошти мають форму документів Microsoft, таких як Word (39,3%), Executable (19,5%), Rich Text (14%) та Excel (8,7%), майже 32% фішингових веб-сайтів використовували протокол «https», щоб імітувати безпечність [108].

На нашу думку, це означає, що проникнення цифровізації значно випереджає здатність населення до набуття відповідних цифрових навичок, особливо в питаннях ідентифікації і мінімізації загроз, що робить все середовище вразливим. Утім, цифрова грамотність має позитивну тенденцію зростати із поширенням мережі Інтернет (рис. 2.6).

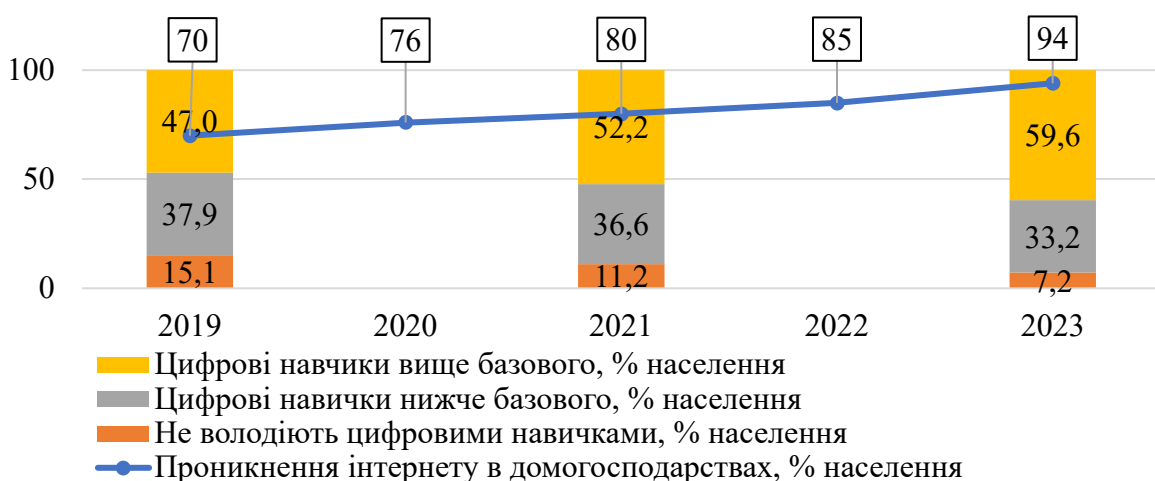


Рис. 2.5. Показники цифрової грамотності населення України та покриття Інтернету за 2019-2023 роки

Джерело: побудовано автором на основі [100; 134]

*періодичність публікацій частини вхідних даних не включає 2020, 2022 роки

Варто відзначити, що кризи, зумовлені COVID-19 та війною, сприяли підвищенню рівня цифрових навичок у населення, внаслідок необхідності дистанційної освіти й роботи, перекваліфікації, зростання попиту на ІКТ послуги та товари, структурні зміни й зростання соціально-побутових цифрових потреб на нанорівні. В результаті ринок праці поповнювався вивільненими фахівцями з ІКТ-галузі, включаючи як досвідчених спеціалістів, так і початківців. Це призвело до поглиблення загрози занепаду традиційного виробничого сектору економіки на користь сектору ІКТ, погіршенню умов оплати праці, надмірній концентрації трудових ресурсів у окремих галузях національної економіки.

Таким чином, суб'єкти нанорівня визначають загрози економічній безпеці через призму власних майнових прав, бюджету, резервів та загальної можливості для заощаджень, а також особистих фінансових цілей. Отже, процес забезпечення економічної безпеки на рівні домогосподарств передбачає фізичну і цифрову безпеку власного майна, фінансових та інвестиційних активів. Утім, недоліком безпекозабезпечувальної діяльності суб'єктів нанорівня є їх нераціональна поведінка внаслідок недостатньої фінансової чи цифрової грамотності, когнітивних та соціально-політичних упереджень.

Специфікою цифрових загроз економічній безпеці держави з активною складовою на мікро- та нанорівні соціальної ієрархії є імітування під загальні процеси цифровізації економіки. Сюди відносяться загрози електронного листування, цифровий обіг документів, присутність у мережі Інтернет тощо. Така ситуація підкреслює взаємозв'язок ключових чинників вразливості на нанорівні національної економіки, а саме недостатнього рівня цифрової грамотності суспільства та дефіциту робочої сили з ІКТ кваліфікацією у роботі з інформацією та цифровими технологіями на загальнодержавному рівні.

Підсумовуючи, окремої уваги потребує міжсистемний вплив цифровізації на формування загроз в окремих складових економічної безпеки держави, який складно оцінити. У цьому контексті, важливим є визначення впливу цифровізації на трансформацію традиційних загроз економічній безпеці держави за її складовими (табл. 2.8).

Таблиця 2.8

Вплив цифровізації на трансформацію загроз економічній безпеці України

Складова економічної безпеки держави	Традиційна загроза	Вплив цифровізації	Трансформована загроза
Макро-економічна	Низька конкуренто-спроможність економіки	Ускладнення виробничих процесів цифровими технологіями	Падіння конкуренто-спроможності внаслідок технологічного відставання
	Вразливість стратегічної інфраструктури	Підключення критичних систем до мережі Інтернет, використання інтернету речей	Кібератаки на енергетичну, транспорту, цифрову державну інфраструктуру
	Тіньова економіка	Технології блокчейну, криптовалюти	Цифровізація тіньової економіки
		Анонімність та поширення кримінальних практик в мережі Інтернет	Глобалізація тіньової економіки, поширення транскордонної злочинності
Зовнішньо-економічна	Від'ємне сальдо імпорту товарів з доданою вартістю	Потреба в цифрових товарах та послугах	Від'ємне сальдо імпорту цифрових товарів та послуг
Демографічна	Деформації на ринку праці	Аутсорс, внутрішня міграція та робота ІКТ-галузі на експорт товарів та послуг	Дефіцит кадрів у національній економіці, внаслідок їх перетікання в ІКТ-галузь та міграції
	Депопуляція та міграція населення		
Енергетична	Руйнація енергетичної інфраструктури	Переорієнтація ринку енергетики з об'ємів на сталість постачання	Конфлікт енергетичних потреб виробничого та цифрового сектору
Виробнича	Деформація структури виробництва	Утворення нових інвестиційно привабливих ринків ІКТ-товарів та послуг	Занепад традиційного виробничого сектору на користь ІКТ-галузі
	Шпіонаж у промисловості	Хакерські атаки на корпоративні мережі	Викрадення інтелектуальної власності, кібернетичні диверсії
Фінансова	Дефіцит бюджету, втрата податкових надходжень	Цифрові платформи, надання послуг без фізичної присутності	Ухилення від податків через цифрові юрисдикції та віртуальні гаманці
	Нерівномірне розподілення бюджетних видатків	Державне стимулювання ІКТ-галузі	Навантаження на бюджет через необхідність державної підтримки сектору ІКТ
Соціальна	Низький рівень освіти та компетенцій	Поширення цифрових технологій на побутовий рівень	Вразливість населення до дезінформації та неготовність до технологій

Джерело: складено автором

Завершальним етапом ідентифікації потенційних та реальних загроз економічній безпеці в умовах цифровізації є визначення місця та класифікація цифрових загроз у загальній сукупності. Користуючись адаптованою формулою відхилення для оцінки прояву загрози можна здійснити ранжування загроз на потенціальні та реальні, а серед останніх варто додатково виділити помірні та критичні.

Так, за результатами проведеного аналізу (табл. В.1, додаток В) можна зазначити, що 52 індикатори сигналізують про відсутність загрози, 44 – про потенційні загрози і 59 – про реальні, в тому числі про критичні, якщо їх оцінка більша за значення 1,25. Разом із цим, виявлені загрози економічній безпеці України в умовах цифровізації розподілені як 3 потенційного, 2 помірних реальних та 7 критичного рівня.

Утім, національна методика орієнтована на оцінювання складових та інтегрального рівня економічної безпеки України і не передбачає механізму ідентифікації загроз. Тому, пропонується здійснювати ідентифікацію і групування загроз на реальні та потенційні за відхиленням їх індикатора від граничного значення. Результати проведеного аналізу наведено у таблиці В.2 (додаток В) та на рис 2.6. Так, за проведеними розрахунками, до потенційних загроз економічній безпеці України слід відносити дисбаланс торгових відношень, соціальну нерівність, вимивання капіталу, низьку конкурентоспроможність ринку праці, а до реальних – тінізацію економіки, боргову залежність, структурні деформації економіки, геополітичну економічну слабкість, технологічну відсталість економіки, інфляційні загрози, бюджетний дефіцит.

Порівняння відхилень індикаторів інформаційно-цифрової складової економічної безпеки держави з аналогічними показниками традиційних складових дозволяє визначити роль та місце загроз, спричинених цифровізацією, в економічній безпеці України. З огляду на те, що 56% виокремлених реальних загроз мають цифрове походження, можна стверджувати про їх суттєвий вплив на економічну безпеку держави.

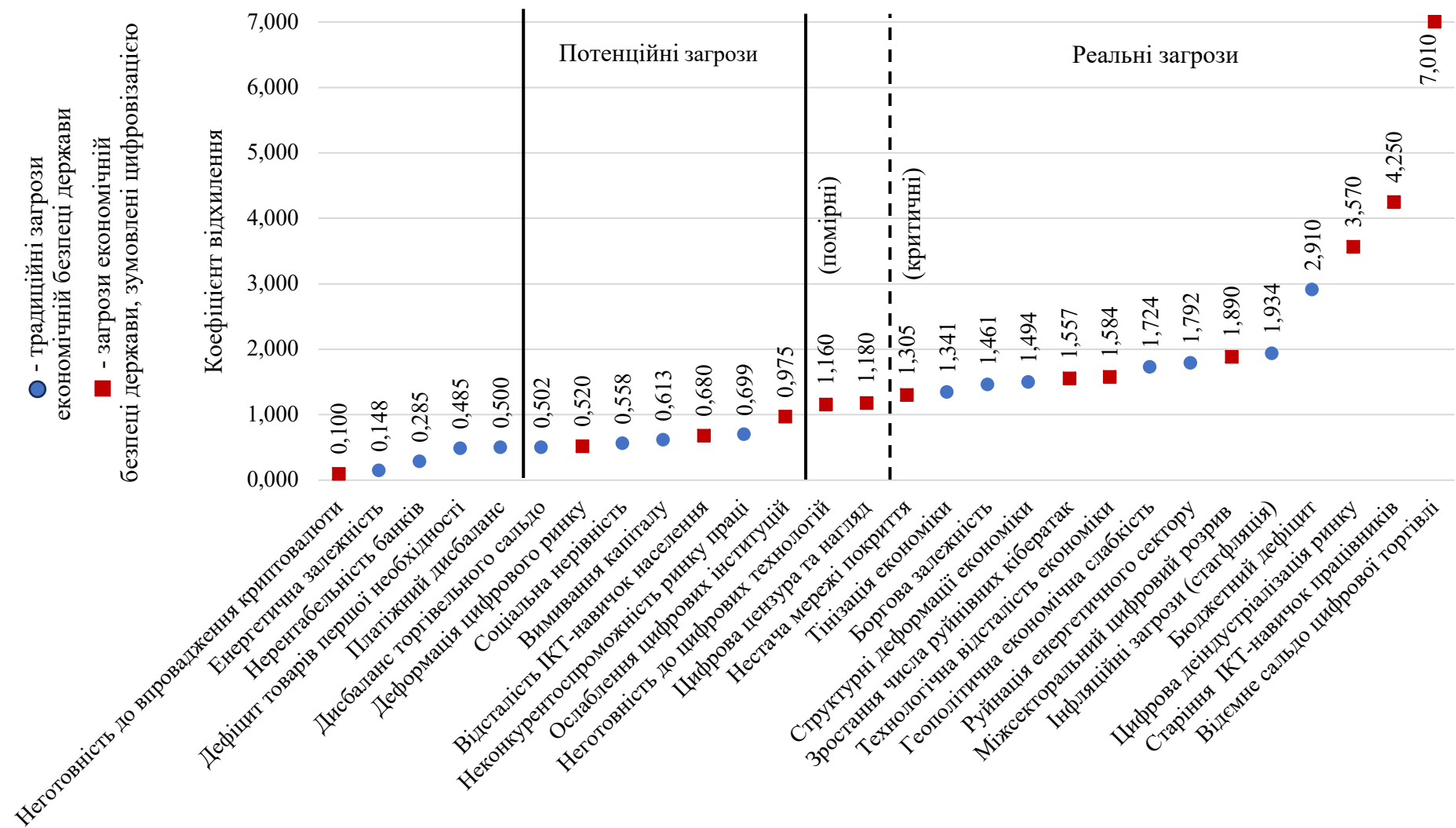


Рис. 2.6. Результати ідентифікації та ранжування загроз економічній безпеці України в умовах цифровізації

Джерело: побудовано автором

Отже, враховуючи властивості цифровізації, можна засвідчити, що вона збільшує кількість реальних загроз. Це підтверджує гіпотезу про дуальний характер впливу цифровізації на загрози економічній безпеці України.

Так, серед реальних загроз, зумовлених цифровізацією, особливої уваги потребують загрози від'ємного сальдо торгівлі цифровими продуктами, недостатній рівень покриття мережею Інтернет, низька готовність до цифрових технологій та технологічна відсталість національної економіки. У аспекті впровадження цифрових технологій виникають такі загрози, як втрата кваліфікації в ІКТ-навичках та занепад традиційного виробничого сектору, викликаний неконкурентним перетіканням ресурсів. На макрорівні цифровізація генерує загрози деіндустріалізації, відтоку кадрів, зростання тіньового сектору економіки. Особливої актуальності набувають загрози, пов'язані з асиметричним розвитком економіки, зумовлені нерівномірним розподілом ресурсів між реальним і цифровим секторами економіки. Загалом на мікро- та нанорівні актуальними є кіберзлочинність, фішинг, нестача конкретних кваліфікацій та відсутність доступу до передових цифрових інструментів.

Проведені ідентифікація та оцінювання потенційних та реальних загроз економічній безпеці держави в умовах цифровізації підтверджує наявність нових загроз, а також трансформацію вже існуючих загроз інформаційно-цифрової складової економічної безпеки України. У цьому контексті особливої актуальності набувають питання аналітичної спроможності вчасної ідентифікації та протидії загрозам на макро-, мікро і нанорівні діяльності суб'єктів національної економіки. Тому, подальше дослідження впливу цифровізації на економічну безпеку держави додатково потребує виокремлення сучасних тенденцій цифровізації на економічну безпеку України.

2.3. Аналіз впливу сучасних тенденцій цифровізації України на загрози її економічній безпеці

Цифровізація як об'єктивний незворотній процес світового соціального-економічного розвитку призводить до формування ряду трансформаційних тенденцій, як у глобальному, так і в національному вимірі. При цьому бенефіціари сучасних тенденцій цифровізації отримують нові інструменти взаємодії від ефективності використання яких, а також від адаптивності та гнучкості самих економічних суб'єктів залежить напрям впливу цифровізації. Слід відмітити, що важливою особливістю цифровізації є неефективність директивних регуляторних обмежень на детермінанти дальнього зовнішнього середовища національної економіки та обмежений їх вплив на ближнє середовище, де і формуються основні глобальні тенденції та виклики. Натомість жорстка регуляція у внутрішньому середовищі національної економіки негативно впливає на конкурентоспроможність та розвиток цифрових технологій.

Тому, виходячи з наведеного у попередніх двох підрозділах аналізу рівня економічної безпеки України можна визначити наступні чотири тенденції цифровізації, які мають найбільший вплив на економічну безпеку України, а саме: зміна підходів до ведення воєнних дій; гібридне протистояння в кіберпросторі, викликане повномасштабним російським вторгненням; внутрішні диспропорції впровадження цифровізації; прискорення процесів цифровізації під впливом чинників зовнішнього та внутрішнього середовища. Перші дві тенденції можна віднести до впливу детермінант зовнішнього середовища, тоді як другі дві є наслідком внутрішніх детермінант, а саме державної політики збереження конкурентоспроможності, стимулювання технологічного та економічного розвитку держави шляхом стимулювання цифровізації.

Починаючи з 2022 року, основним чинником генерування загроз економічній безпеці є російське вторгнення, що призвело до втрати населення і території, вимушеної міграції, руйнації підприємств, енергетичної інфраструктури, кібератак, обмеження логістики, мінування територій, поширення дезінформації, а також посилення інших проявів гібридного протистояння в мережі Інтернет.

У цих умовах, у питанні впливу цифровізації на економічну безпеку держави, низка науковців, як от І. Назаренко [109], І. Шевчук, А. Шевчук [127], Т. Моряк [133] відстоює думку, що підприємства галузі інформаційних технологій (далі – ІТ) України, попри нові виклики, завдяки властивостями цифровізації (мобільності та адаптивності) здатні успішно пристосовуватися до нових реалій. Цьому сприяє незначна частина реальної інфраструктури ІТ-галузі, велика гнучкість та безбар'єрні виходи на міжнародні ринки, що може становити резервний потенціал для забезпечення економічного розвитку в умовах воєнних викликів. Утім, дуальний вплив цифровізації зумовлює посилення негативних тенденцій і загроз економічній безпеці держави, що потребує глибшого аналізу.

З одного боку, притримуємося позицій науковців, які вбачають у ІТ-галузі певний резерв, тобто запас ресурсу, що зберігається для використання в разі потреби. Резерв також трактують як невикористані можливості, засоби для здійснення чого-небудь [187]. На рівні держави, до резервів життєздатності економіки відносяться золотовалютні та ресурсо-енергетичні запаси, а також невикористані ринкові можливості перепрофілювання та залучення додаткових коштів на випадок непередбачуваних подій. Важливими аспектами для визначення резервів економіки є висока ринкова ціна і ліквідність, легкість відтворення, можливість використання за несприятливих умов, достатньо велика кількість запасів ресурсу. Варто відмітити, що використати резерви можна також з різною метою, як для захисту від стихійних лих так і для страхування від економічних шоків та санкцій.

Оглядаючи більш ніж 30-річну історію становлення, розвитку і поширення цифровізації існує обмежене коло криз і конфліктів, яке дозволяє дослідити питання впливу ІТ-галузі, як складової ІКТ сектору, на її можливість виступати резервом життєздатності економіки.

Одним із таких прикладів є кібератаки проти Естонії 2007 року, а іншим – кібератаки у війни росії проти Грузії у 2008 році. Кібератаки були зосереджені на медіа-ресурсах, комунікаціях й мали на меті нанести соціально-політичну шкоду, завдати економічних збитків та додатково послабити економіку противника. Захист національної безпеки від кібервійни означав не допустити хакерів до важливих урядових комп'ютерних систем і менше уваги приділялося ризикам, пов'язаним з широкомасштабним порушенням роботи Інтернету загалом.

Можна зазначити, що через відносно невелику складову цифрової економіки Естонія у 2007 році та Грузія у 2008 році не мали достатнього досвіду захисту цифрової інфраструктури, а тому зазнали значного кібертиску під час війни. Аналізуючи роль цифрової економіки у захисті, відновленні та відбудові Грузії після війни та Естонії після короткотривалої кібервійни варто відмітити, що частка цифрових технологій у ВВП Грузії у 2007 року до початку кіберпротистояння складала 3,13%, і вносила близько 18% приросту ВВП, а проте після воєнних дій склала 14,5% приросту у частці ВВП і була другою за величиною приросту. Це обумовлено розвитком ІТ-галузі із одночасним спадом всіх інших галузей, внаслідок війни, окрім видобування руди, торгівлі та державного сектору [191]. На противагу, у період кризи сектор ІТ в Естонії складав близько 4,5% і зазнав незначного спаду у 2008 році, втім також не мав значного впливу на економічний розвиток держави [184].

Значення частки ІТ сектору Естонії та Грузії у 2007-2008 роках (рис. 2.7). Проте у абсолютному вимірі їх ВПП був у три-чотири рази меншим лише за обсяг ринку цифрових послуг у росії. А тому, така диспропорція не дозволяла країнам

ефективно протидіяти організованим кібератакам внаслідок браку ресурсів та кадрів.

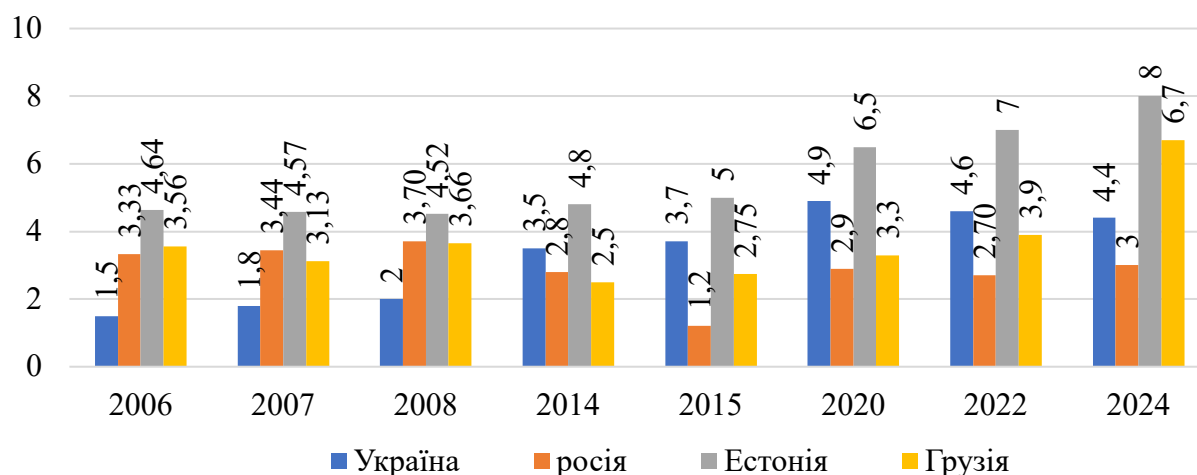


Рис. 2.7. Порівняння частки ІТ сектору у ВВП України, Грузії, Естонії та росії протягом 2006-2024 рр.

Джерело: побудовано автором на даних джерел [184, 193-198]

Дійсно, як резервна галузь ІТ змогла швидко відновитися і, хоча дещо втратила потенціал, все одна була складовою відновлення Грузії після війни. Зараз частка ІТ у структурі ВВП Грузії складає близько 10%, є важливою галуззю в економіці і привертає до себе багатьох спеціалістів. Натомість Естонія пішла іншим шляхом розвитку після кібератаки у 2007 році, зменшуючи частку ІКТ у ВВП, попри зростання користувачів мережі та розвитку Інтернету речей.

Натомість, для росії, з ознаками енергоресурсної моделі економіки, сектор ІТ є допоміжним джерелом доходів та середовищем для вербування спеціалістів, а також розвитку цифрової мережі для інформаційних операцій та сфери застосування м'якої сили.

Зазначимо, що найбільшим відомим протистоянням у сучасній історії кіберсфери є російсько-українська кібервійна. Перед початком повномасштабного вторгнення, росія очікувала повторити успіх грузинської кампанії, оскільки проросійські пропагандисти і хактивісти розраховували на

втрату керованості і банківської системи та інформаційної безпеки України 24 лютого 2022 року, що дозволило б поширити паніку серед населення. При цьому, порівнюючи частку ІТ сектору в економіці (рис. 2.8), Україна розвивала технологічну перевагу над росією (рис. 2.7), проте усе одно знаходилася під постійними атаками і потребує зміцнення кібербезпеки.

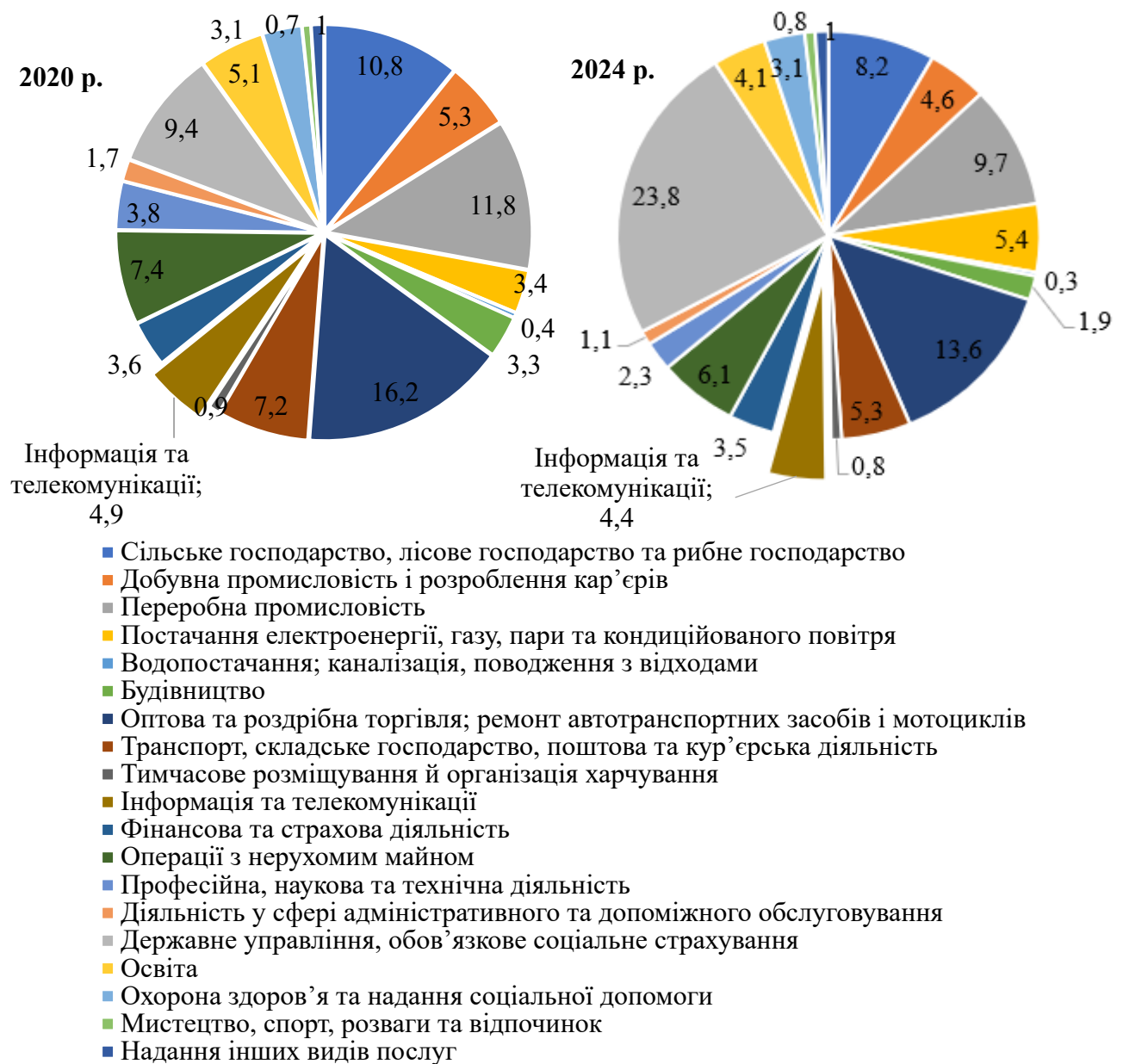


Рис. 2.8. Частка сектору ІКТ в структурі національної економіки України у 2020 та 2024 рр., у % до ВДВ

Джерело: розраховано та побудовано автором за даними Державної служби статистики [184]

Усупереч тезі науковців про резервність цифрової економіки, ІКТ у структурі ВВП України складала в 2014 році 3,5%, а протягом 2015-2016 років зростання становило усього 0,3-0,1% [100]. Варто відзначити, що частка ІКТ сектору значно зросла у період кризи COVID-19 до 4,9% у 2020 році. Експорт ІКТ-послуг у 2021 році складав 36%, а у кінці 2022 року частка ІКТ-послуг у експорті була єдиною, з усіх галузей орієнтованих на експорт, що зросла на 5,8% [189]. Проте, станом на 2025 рік частка ІКТ у ВВП склала 4,4% у 2-3 рази поступаючись агропромисловому комплексу (далі – АПК) та переробній промисловості [100]. Так, в умовах обмеженого доступу до джерел зв'язку та фахівців, а також на фоні глобального спаду в цій галузі, сектор ІКТ у економіці України у 2023 році вперше за понад 20 років зазнав зниження показників експорту на 8,5% [100].

Отже, виходячи з досвіду минулих кібервоєн, сектор ІКТ у короткостроковій перспективі може забезпечувати певний рівень життєздатності економіки у турбулентний період. Окрім того стратегічне значення для питань оборони та забезпечення кібербезпеки має наявність на внутрішньому ринку праці достатньої кількості кваліфікованої робочої сили, яка потрібна усім секторам економіки, зважаючи на те, що сама ІТ галузь не створює додаткових економічних переваг.

Що стосується російського сектору ІКТ, то у 2014 році ринок та експорт ІКТ-послуг значно скоротилися на 38% та 12% відповідно [196; 198], що стало наслідком введених санкцій, посилення авторитарних тенденцій і початку відтоку спеціалістів та бізнесу. Сектор ІКТ росії відновився після падіння і стагнації лише у 2021 році, причиною чому стала пандемія COVID-19 та потреба у цифровізації, що спричинила зростання на 8%. Проте цей сектор залишився одним з небагатьох, що не зазнав значного спаду після у повномасштабного вторгнення та має приріст близько 6-8% на квартал до попереднього показника [196]. В контексті російсько-української війни такі тенденції створюють додаткові виклики для забезпечення економічної безпеки України, адже розвиток цифрових технологій потребує інтеграції цивільних та військових підходів.

Разом із тим, аналіз джерел [196-198] дозволяє визначити природу зростання попиту на ІКТ послуги, що припав на державні воєнні замовлення або російський бізнес, який мав на меті перебудову та імпортозаміщення. Разом із тим, це не лише зменшило ефективність економічних і технологічних санкцій накладених на росію внаслідок вторгнення в Україну у 2022 році, але й створило додатковий фінансовий та кадровий потенціал для розвитку сектору ІКТ агресора.

Потрібно зауважити, що іншим важливим впливом цифровізації, в умовах сучасної кібервійни, є використання криптовалют. Така валюта, як стеблкоїн, вид криптовалюти, прив'язаний до курсу реальних валют, став засобом обходу санкцій для росії, оскільки методи контролю за подібними розрахунками обмежені. І хоча сучасні криптобіржі є набагато більш прозорими та діють у відповідності до національних систем моніторингу, а контрагенти росії неохоче приймають або взагалі обмежують подібний ресурс, тому його резервний потенціал можна визначити допоміжним, аніж повноцінною альтернативою для уникнення економічних санкцій.

Підсумовуючи, сучасні тенденції цифровізації України, передусім тісно пов'язані з війною та гібридним протистоянням. Необхідно відмітити, що резервний потенціал сектору ІКТ формується за рахунок імпортозаміщення та потреб воєнного часу. При цьому, безпекові аспекти, високі ризики інвестицій та співпраці з агентами у зоні бойових дій та в умовах воєнного стану не дозволяють сектору ІКТ бути рівноцінною заміною енергоресурсів чи продукції АПК, оскільки попит на них лише зростає внаслідок катастрофи чи кризи.

На основі цього можна зробити висновок, що резервний потенціал сектору ІКТ залежить від рівня попиту на цифрові послуги, рішення та товари, як у світі загалом, так і на внутрішньому ринку. Втім, за несприятливих умов зовнішнього середовища, сектор ІКТ не лише не виступає резервом життєздатності економіки, а й посилює негативний вплив загроз економічній безпеці держави внаслідок руйнації енергетичної й цифрової інфраструктури, які є пріоритетною ціллю в умовах воєнних дій.

Розглянуті події змусили низку військових організацій по всьому світу переглянути важливість мережевої безпеки для сучасної військової доктрини, внаслідок цього було створено Центр передового досвіду НАТО з питань кооперативного кіберзахисту (CCDCOE) [188] та затверджено «Талліннський посібник», покликаний забезпечити глобальну норму в кіберпросторі, застосовуючи існуюче міжнародне право до кібервійни. При цьому держави не мають суверенітету над мережею Інтернет загалом, але вони мають суверенітет над її компонентами на своїй території. А найбільш руйнівні атаки слід розглядати як «збройні атаки» і тому вони дозволяють державам реагувати на них у порядку самозахисту [188]. Проте, цей документ залишився суто консультативним і не спричинив утворення правил та звичаїв ведення кібервійни, розширюючи можливості для безкарної агресії, зменшуючи відповідальність бенефіціарів ризикової поведінки та сприяючи поширенню кіберзагроз.

Іншою значущою тенденцією, поза воєнними діями та гібридним кіберпротистоянням, є прискорення цифровізації бізнесу (рис. 2.9).



Рис. 2.9. Показники цифровізації бізнесу України за 2018-2023 рр.

Джерело: розраховано та побудовано автором за даними Державної служби статистики [184]

Насамперед про поширення цифровізації на мікрорівні свідчить зростання частки підприємств, які використовують фіксований доступ до мережі Інтернет, з 62,1% у 2018 році до 88,8% у 2023 році у загальній кількості підприємств. Показники частки зайнятих працівників, які мають доступ до мережі Інтернет та частка підприємств, які здійснюють електронну торгівлю, також підтверджують визначену тенденцію прискорення цифровізації бізнесу.

Разом із тим, цифровізація сприяє інноваційному розвитку, пожевваленню комерції, покращенню якості життя та наданих послуг, знижує ринкові бар'єри. А проте стикається з гальмуванням, внаслідок недосконалості та повільності державного регулювання, що значно зменшує позитивний вплив цифровізації. Доказом цього є низхідна тенденція значення індексу цифрової трансформації України (рис 2.10), що відображає спроможність органів виконавчої влади впроваджувати розроблені державні цифрові рішення.

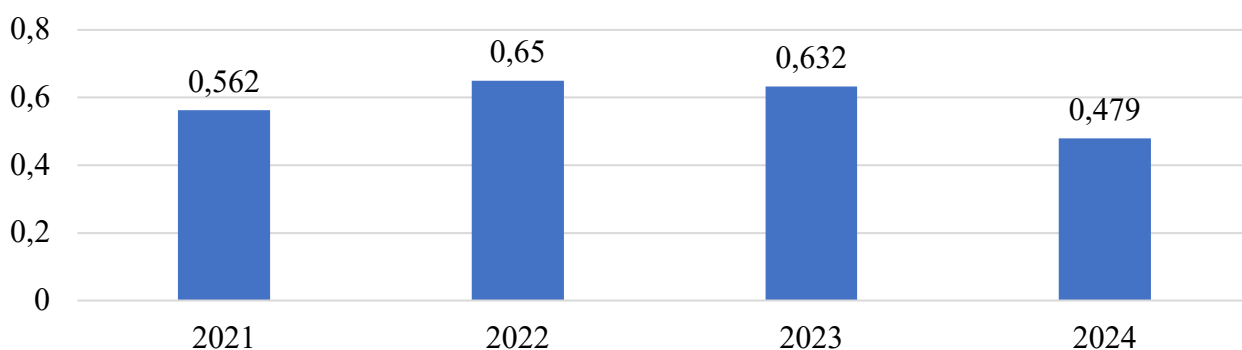


Рис. 2.10. Значення індексу цифрової трансформації України за 2021-2024 роки

Джерело: побудовано автором на даних [262-266]

Так, існує концепція повної цифровізації підприємства, установи або інституції. Вона передбачає перехід всього документообігу у цифровий вигляд, створення електронних підписів та печаток, використання комп'ютерної техніки для автоматизованого чи спрощеного обліку, аудиту та контролю за ресурсами, встановлення касових апаратів, безготівкові розрахунки, системи онлайн

продажів та зворотного зв'язку, які дозволяють швидко обробляти замовлення та ввідні дані, контрагентів, підрядників, співробітників. Утім, варто виділити три ключові перешкоди, що заважають реалізації зазначеного концепту.

По-перше згідно ст. 13 Закону України «Про електронні документи та електронний документообіг» від 2003 року [267] існують вимоги для подвійного обігу і аналогового зберігання документів. Другою перешкодою є потреба забезпечення цифровими ключами та підписами персоналу, їх навчання та створення відповідних процедур. Третя перешкода є наслідком недостатньої кваліфікації та забезпечення контрагентів, оскільки кінцеві форми документообігу найчастіше ведуться в дуальному вигляді. Відсутність можливості ефективного використання цифрового документообігу та неспроможність органів виконавчої влади впроваджувати розроблені державні цифрові рішення значно сповільнюють впровадження цифровізації в бізнес-процеси підприємств (рис. 2.11).

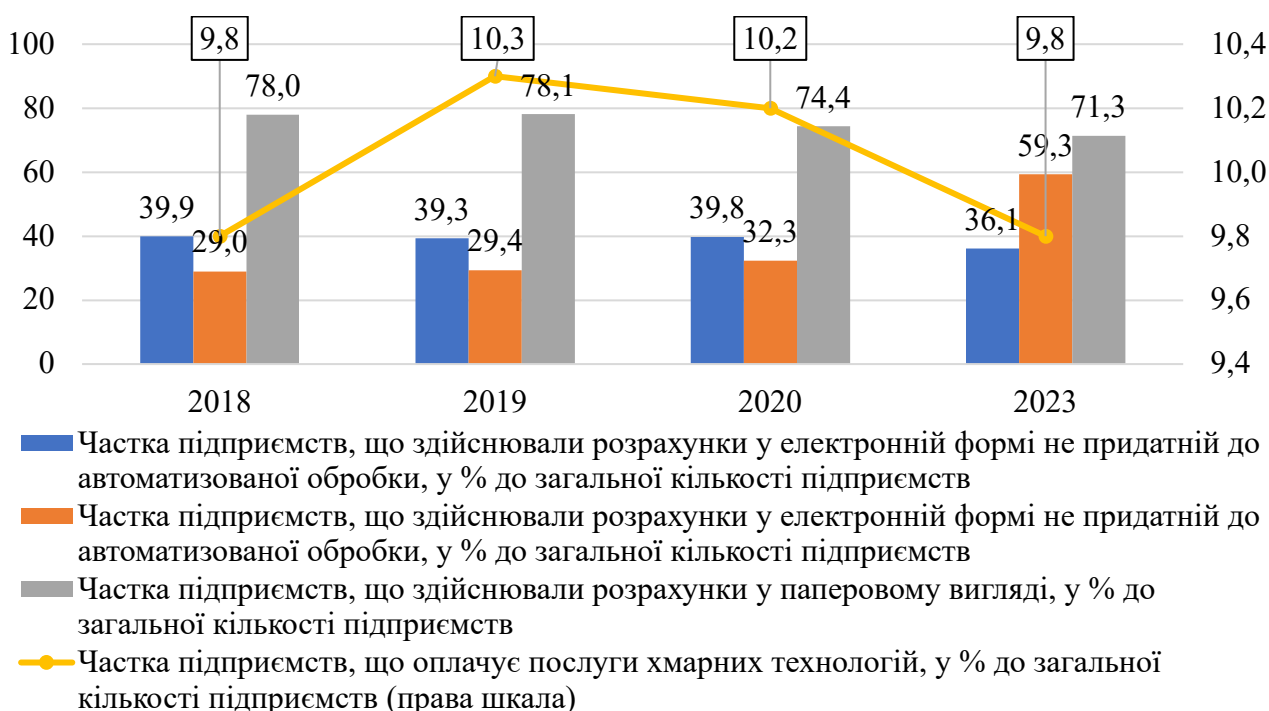


Рис. 2.11. Показники впровадження цифрового документообігу та використання хмарних технологій бізнесом в Україні за 2018-2023 рр.

Джерело: розраховано та побудовано автором за даними Державної служби статистики [184]

Тому концепт повної цифровізації є виключенням для окремих проєктів, галузей та сфер, адже діюче законодавство, кваліфікація персоналу і умови діяльності призводять до різного рівня проміжних етапів гібридної та неповної цифровізації суб'єктів економічної діяльності. Разом із тим, зберігання цифрових документів за допомогою хмарних сервісів збільшує ризики витоку даних і, відповідно, витрати на забезпечення кібербезпеки бізнесу, а тому частка підприємств, що оплачує ці цифрові послуги становить не більше 10% [184].

Підсумовуючи, можна зазначити, що прискорення цифровізації бізнесу потребує формування відповідних умов та розвитку інституційного забезпечення з метою спрощення процесів цифрової трансформації підприємств. В іншому випадку стимулювання окрім локального розвитку, буде посилювати вразливість середовища та створювати «сірі зони», що сприятимуть негативному впливу цифровізації на загрози економічній безпеці держави. Також тенденція внутрішніх диспропорцій впровадження цифровізації України призводить до структурних деформацій та посилення навантаження на державний апарат. Тому, доцільно здійснити розрахунки темпів цифровізації економіки, з метою визначення загрози поглиблення тенденції внутрішніх диспропорцій. Для цього використаємо співвідношення окремого показника використання інформаційно-комунікаційних технологій на підприємствах до його значення попереднього року (2.2). Також, порівняємо середній приріст показників із приростом ВВП, щоб оцінити темпи зростання цифровізації державного або комерційного сектору економіки загалом (2.3).

$$\Delta TI = \frac{TI_{year}}{TI_{year-1}} \times 100, \quad (2.2)$$

$$InTI_{\frac{p}{b}} = \frac{\overline{\Delta TI}}{\Delta ITGDP}, \quad (2.3)$$

де ТІ – окремий показник використання інформаційно-комунікаційних технологій на підприємствах за даними Державної служби статистики;

$\Delta ITGDP$ – зростання сектору ІКТ у ВВП;

$InTIp/b$ – індикатор зростання цифрової трансформації державного/бізнес-сектору економіки.

Так, індикатор зростання цифрової трансформації державного сектору економіки за 2022 рік становить $0,818 < 1$, а $\overline{\Delta TIp}$ – 99,83%, що свідчить, про низьку ефективність державних заходів прискорення цифровізації бізнесу і, як наслідок, відтоку інноваційного капіталу. В свою чергу, індикатор зростання цифрової трансформації бізнес-сектору економіки за 2022 рік становить $0,885 < 1$, а $\overline{\Delta TIp/b}$ – 107,99%, що свідчить про значний кумулятивний ефект провідних суб'єктів ринкової діяльності в питанні цифровізації, який рухає економіку набагато швидше, ніж за ним встигають інші. Це додатково підтверджує думку про нестачу інвестиційно-інноваційних активів, асиметрії розвитку національної економіки і є передумовою зменшення позитивного впливу цифровізації.

Також, за даними Індексу цифрової економіки та суспільства (DESI) 2021, варто порівняти підприємства, що надавали послуги з навчання ІКТ в Україні та країнах ЄС (рис. 2.12).

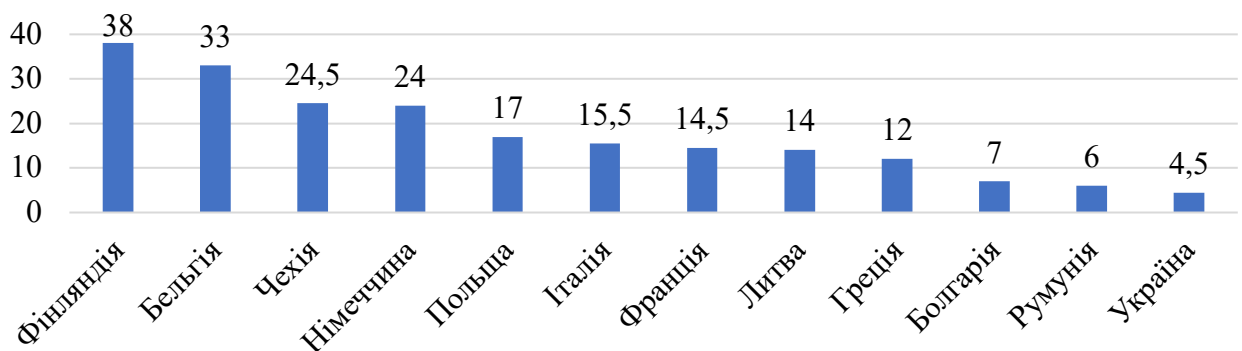


Рис. 2.12. Показник частки підприємств, що проводили навчання у сфері ІКТ в Україні та країнах ЄС, у % до всіх підприємств

Джерело: побудовано автором на даних [184; 266]

Так, загалом український показник у 4,5% відстає від усіх країн ЄС, замикаючи трійку лідерів Болгарію з 7% та Румунію з 6%. Також варто порівняти показник частки підприємства, що проводили навчання у сфері ІКТ в Україні за галузевою структурою (рис. 2.13).

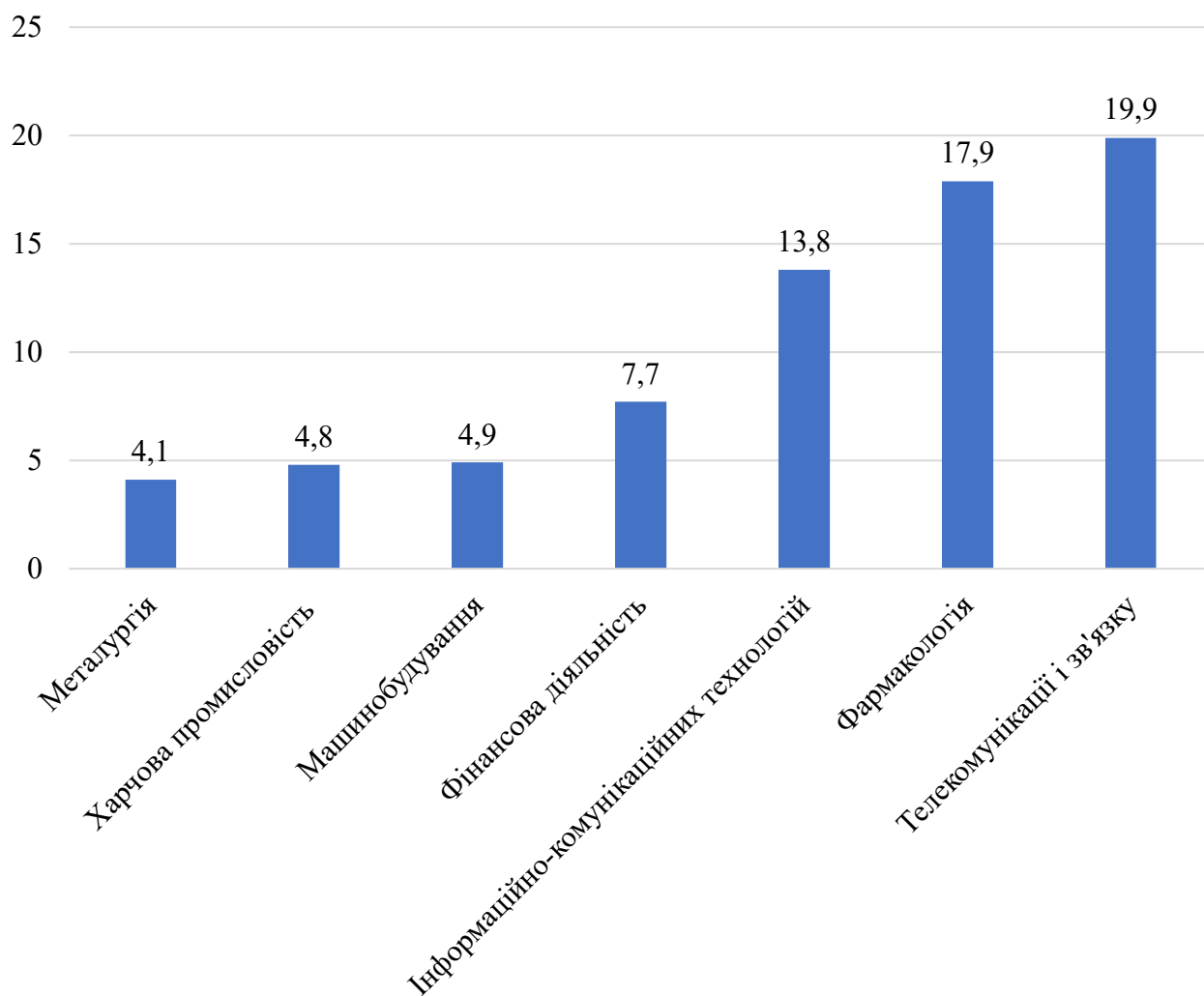


Рис. 2.13. Показник частки підприємств, що проводили навчання у сфері ІКТ в Україні за окремими галузями, у % до всіх підприємств

Джерело: розраховано та побудовано автором за даними Державної служби статистики [184]

Отже, реальна загроза неготовності до цифрових технологій посилюється тенденціями цифровізації, що збільшують силу негативного впливу цифровізації, внаслідок поглиблення структурних деформацій між галузями економіки. Тому,

для оцінки розриву проникнення та поширення цифровізації між групою провідних галузей та групою секторів економіки з найбільшою долею в структурі ВВП варто скористатися формулами 2.4 та 2.5.

$$GapTI = \frac{\overline{TI}_T}{\overline{TI}_L}, \quad (2.4)$$

$$GapTI = \frac{\left(\frac{\frac{\sum_T(TIx)}{N_{Tx}} + \frac{\sum_T(TIy)}{N_{Ty}} + \dots}{\frac{\sum_L(TIx)}{N_{Lx}} + \frac{\sum_L(TIy)}{N_{Ly}} + \dots} \right)}{N_{TI}}, \quad (2.5)$$

де $GapTI$ – розрив між провідними галузями цифрової трансформації та найбільшими секторами економіки;

TI_T – рівень цифрової трансформації провідних (топових) галузей;

TI_L – рівень цифрової трансформації найбільших галузей;

$TI_{x,y,\dots}$ – показник використання інформаційно-комунікаційних технологій на підприємствах за даними Державної служби статистики;

$N_{T/L}$ – кількість підприємств у вибірці;

N_{TI} – номер окремого індикатора трансформації у вибірці.

Розрахунок базувався на наступних індикаторах цифровізації: частка кількості підприємств, які здійснювали електронну комерцію, від загальної кількості підприємств; частка кількості підприємств, які надсилали рахунки-фактури; частка кількості підприємств, які проводили аналіз великих даних; частка кількості підприємств, які проводили навчання з розвитку навичок, пов'язаних з ІКТ.

У розрахунок, до найбільших галузей включені такі види економічної діяльності, як харчова промисловість, металургія та нафтопереробка, зважаючи на їх вагомий внесок до ВВП, орієнтацію на експорт та критичною роллю у формуванні промислового потенціалу України. А до топових за показниками цифровізації, віднесено фармакологію, комп'ютерне програмування, телекомунікації, оскільки саме вони демонструють найкращі результати впровадження цифрових технологій за розглянутий період. Результати варто порівняти з рівнем ІКТ-технологій у ВВП (рис. 2.14).

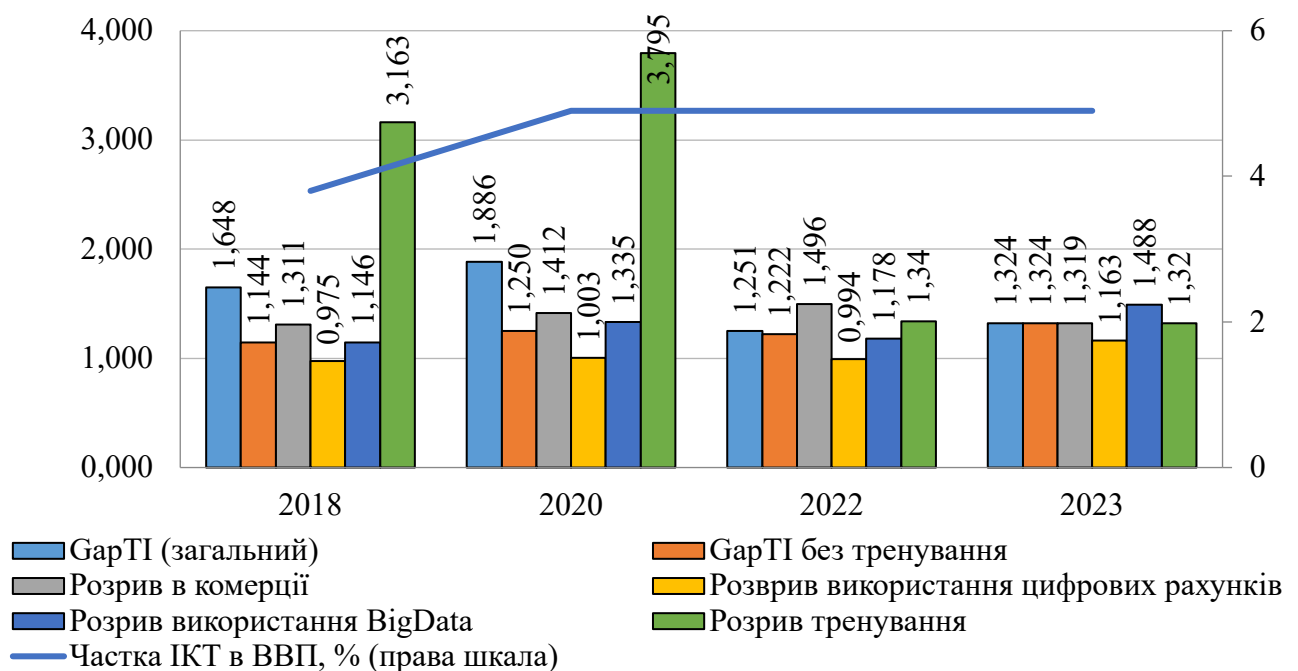


Рис. 2.14. Розрив між провідними галузями цифрової трансформації та найбільшими секторами економіки за 2018-2023 роки

Джерело: розраховано та побудовано автором за даними Державної служби статистики [184]

Значення індексу GapTI на рівні 1,6-1,9 означає двократний розрив між провідними та найбільшими галузями національної економіки України. При загалом низьких показниках порівняно з ЄС, це свідчить про загрозу прийняття неправильних рішень, технологічного відставання традиційних виробничих галузей, особливо в питанні використання провідних цифрових технологій.

Такий розрив частково сформований впливом ІКТ сектору, що орієнтується на експорт. Так, за рахунок різниці якості життя та оплати праці, ІКТ сектор здатний забезпечувати кращі умови для кваліфікованих кадрів та отримувати державну підтримку. Втім, він не виробляє реальних благ, не створює конкурентних технологій та не займає достатньої частки у ВВП, а тому не може існувати самостійно. Загалом таке позиціонування галузі є наслідком реалізації загрози «пастки середніх доходів».

Згідно визначення Світового банку «середнім рівнем доходу» визначають країни з ВВП на душу населення, який залишався між 1000 і 12000 дол. США в постійних цінах [100]. Україна якраз є однією з країн, що мають подібну тенденцію з показниками в межах 2124,7-5750 дол. США на душу населення [184]. Загроза пастки середнього доходу означає втрату цінової конкурентоспроможності ринку праці і відсутність можливості конкурувати як з провідними державами, так і з низьким рівнем заробітної плати і дешевим виробництвом промислових товарів. А це, в свою чергу, означає потенційну втрату конкурентоспроможності та переваг сектору ІКТ внаслідок низької інвестиційної привабливості економіки України та слабку диверсифікацію виробництва.

Підсумовуючи, тенденція внутрішніх диспропорцій внаслідок цифровізації має значний довгостроковий негативний вплив, який без належної регуляції може глибше деформувати економіку, посилити наявні загрози економічній безпеці держави та, у підсумку, перекрити весь позитивний вплив цифровізації внаслідок неповоротних економічних, демографічних та технологічних втрат.

Також варто відмітити, що остання визначена тенденція, а саме зовнішнього та внутрішнього прискорення процесів впровадження цифровізації посилює інші негативні прояви сучасних ризиків і загроз, зокрема воєнних дій та внутрішньої еміграції, гібридного протистояння в кібернетичному просторі та посилення внутрішньої асиметрії впровадження цифровізації.

У результаті прискореної цифровізації зростає роль критичної інфраструктури, зокрема енергетичної та цифрової, яка є важливою як для великих промислових виробництв, так і для безперебійної діяльності суб'єктів ІКТ-сектору. При цьому стимулювання цифровізації супроводжується політикою надання преференцій, податкових пільг, протекціоністської підтримки, встановлення вищих рівнів оплати праці в секторі ІКТ порівняно з іншими галузями, що додатково поглиблює структурні деформації та спричиняє перерозподіл обмежених ресурсів на користь сектору ІКТ, однак не призводить створення стійких мультиплікативних стимулів для економіки загалом. Тому, для об'єктивної оцінки вище вказаних процесів варто здійснити кореляційний аналіз між обсягами споживання електроенергії, як показником стану економічної активності традиційного виробничого сектору та часткою сектору ІКТ у ВВП.

Важливо, що обсяги споживання електроенергії виступають індикатором економічної активності традиційного виробничого сектору, оскільки найбільші промислові сектори економіки в Україні, металообробка, машинобудування, а також транспортна інфраструктура та будівельна галузь безпосередньо залежать від інтенсивного використання енергоресурсів для здійснення виробничих процесів, тому доцільно використовувати доступний показник, що відображає загальні тенденції розвитку сектору традиційного виробництва, яким є обсяги споживання електроенергії.

Так, досліджуючи показник споживання електроенергії, варто відмітити, що його значення зменшувалося постійними темпами в середньому у розмірі 1,5% щорічно (табл. 2.9). Загалом, частка комерційного та комунального споживання електроенергії в економіці України складає близько 75%, не виділяючи діяльності фізичних осіб-підприємців. Станом на 2021 рік частка енергоспоживання промисловістю, будівництвом та агропромисловим комплексом складала 36% та 6% іншими підприємствами, домогосподарствами та комунальним сектором [184]. Варто враховувати, що в умовах руйнації

української енергетики, внаслідок ракетних атак росії, вся вироблена енергія споживається домогосподарствами та бізнесом.

Тому доцільно визначити та розглянути залежність зростання частки сектору ІКТ у ВВП до зменшення споживання електроенергії (табл. 2.9) з метою визначення загрози впливу цифровізації, як детермінанти занепаду сектору традиційного виробництва.

Таблиця 2.9

Показники споживання електроенергії та частки сектору ІКТ у ВВП України за 2011-2024 роки

Показник	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Частка ІКТ-сектору у ВВП, %	3	3,1	3,1	3,5	3,7	3,8	4	3,8	4	4,9	4,9	4,9	4,9	4,4
Споживання електроенергії, млрд кВт/год	194	198	194	182	163	154	155	159	153	148	156	113	52,4	53

Джерело: систематизовано автором на основі [184-185]

Виявлена тенденція зменшення споживання електроенергії з 194 млрд кВт/год до 53 млрд кВт/год свідчить про стрімке зменшення сектору традиційного виробництва. У цьому контексті, доцільно проаналізувати та розглянути залежність зростання показника частки сектору ІКТ у ВВП до зменшення споживання електроенергії України. При цьому достатній рівень кореляції між цими показниками буде свідчити про існування загрози впливу цифровізації, як прямого чи опосередкованого чинника процесу стрімкого зменшення сектору традиційного виробництва України.

Варто зауважити, що джерелом цієї кореляції може бути не лише деструктивний вплив цифровізації, а й приховані змінні. Також варто дослідити і протилежну гіпотезу, що саме падіння реального сектору стимулює розвиток сектору ІКТ, сприяючи перетіканню кадрів та зміні пропозиції на ринку. Для з'ясування форми регресійного зв'язку, зважаючи на наявність однієї змінної та

мультиплікативний тип зв'язку, варто скористатися рівнянням парної нелінійної регресії (2.6).

$$y = b \times x^a, \quad (2.6)$$

де y – споживання електроенергії, млрд кВт/год;

x – частка ІКТ у ВВП, %.

Для розрахунку здійснимо перетворення нелінійної регресії $y=b*x^a$ до лінійної, тому розрахуємо логарифми від обох частин рівності: $\ln(y)=\ln(bxa)$, $\ln(y)=\ln(b)+a*\ln(x)$. Позначимо $y_1=\ln(y)$, $x_1=\ln(x)$, $b_1=\ln(b)$, $a_1=a$. Одержимо рівняння допоміжної лінії регресії $Y_1=a_1x_1+b_1$. Із рівностей $b_1=\ln(b)$ та $a_1=a$ маємо, що $a=a_1$ та $b=\exp(b_1)$ (табл. 2.10).

Таблиця 2.10

Логарифмічно перетворені показники для розрахунку парної нелінійної регресії залежності споживання електроенергії від частки ІКТ-сектору в національній економіці за 2011-2024 роки

Рік	Y	X	Y ₁	X ₁	Y ₁ *X ₁	X ₁ ²	Y _{1P}	(Y ₁ -Y _{1P}) ²	Y _P	(Y-Y _P) ²	(Y-Y _C) ²	(X ₁ -X _{1C}) ²
1	2	3	4	5	6	7	8	9	10	11	12	13
2011	194	3	5,27	1,10	5,79	1,21	5,345	0,006	209,52	240,779	2100,26	0,075
2012	198	3,1	5,29	1,13	5,98	1,28	5,295	0,000	199,31	1,720	2482,89	0,058
2013	194	3,1	5,27	1,13	5,96	1,28	5,295	0,001	199,31	28,214	2100,26	0,058
2014	182	3,5	5,20	1,25	6,52	1,57	5,110	0,009	165,68	266,390	1144,37	0,014
2015	163	3,7	5,09	1,31	6,66	1,71	5,025	0,005	152,23	115,896	219,89	0,004
2016	154	3,8	5,04	1,34	6,72	1,78	4,985	0,003	146,18	61,220	33,97	0,001
2017	155	4	5,04	1,39	6,99	1,92	4,907	0,019	135,19	392,365	46,63	0,000
2018	159	3,8	5,07	1,34	6,77	1,78	4,985	0,007	146,18	164,464	117,26	0,001
2019	153	4	5,03	1,39	6,97	1,92	4,907	0,015	135,19	317,132	23,32	0,000
2020	148	4,9	5,00	1,59	7,94	2,53	4,598	0,160	99,25	2376,6	0,03	0,047
2021	156	4,9	5,05	1,59	8,03	2,53	4,598	0,205	99,25	3220,6	61,29	0,047
2022	113	4,9	4,73	1,59	7,51	2,53	4,598	0,017	99,25	189,1	1237,03	0,047
2023	52,4	4,9	3,96	1,59	6,29	2,53	4,598	0,408	99,25	2194,9	9172,17	0,047
2024	53	4,4	3,97	1,48	5,88	2,20	4,762	0,626	116,93	4086,6	9057,60	0,012

Джерело: побудовано автором

Для визначення параметрів a_1 і b_1 моделі за методом найменших квадратів використаємо систему нормальних рівнянь (2.7).

$$\begin{cases} a_1 \sum_i x_{1i}^2 + b_1 \sum_i x_{1i} = \sum_i x_{1i} y_{1i} \quad (i = \overline{1, n}); \\ a_1 \sum_i x_{1i} + b_1 n = \sum_i y_{1i} \quad (i = \overline{1, n}). \end{cases}, \quad (2.7)$$

де n – кількість періодів дослідження;

y – споживання електроенергії, млрд кВт-год;

x – частка ІКТ у ВВП, %.

У матричному вигляді система нормальних рівнянь має вигляд $Z^*A=T$. Матричний розв'язок цього рівняння буде виконано методом найменших квадратів (2.8-2.10) для визначення параметрів a_1 та b_1 . Таким чином, отримаємо рівності $a_1=-1,52$, а $b_1=7,02$.

$$Z = \begin{pmatrix} \sum_i x_{1i}^2 & \sum_i x_{1i} \\ \sum_i x_{1i} & n \end{pmatrix}, \quad (2.8)$$

$$T = \begin{pmatrix} \sum_i x_{1i} y_{1i} \\ \sum_i y_{1i} \end{pmatrix}, \quad (2.9)$$

$$A = T * Z^{-1} = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}, \quad (2.10)$$

де n – кількість періодів дослідження;

Z – матриця коефіцієнтів системи;

T – матриця правих частин рівняння;

Z^{-1} – обернена матриця коефіцієнтів системи;

A – матриця параметрів регресії.

Повернемо показники a_1 та b_1 до лінійної розмірності, тобто $b_1 = \ln(b) = \ln(7,02) = 1116,42$ та $a_1 = a$. Тому, можна зазначити, що розрахунок рівняння парної нелінійної регресії залежності падіння реального сектору економіки від розвитку економіки цифрових послуг має мультиплікативну форму (2.11).

$$y = 1116,42 \times x^{-1,52}, \quad (2.11)$$

де y – споживання електроенергії, млрд кВт/год;

x – частка ІКТ у ВВП, %.

З метою оцінки адекватності вибраної математичної моделі експериментальним даним визначимо оцінку тісноти та значимості зв'язку змінних у регресійній моделі. Так, розрахунок показника кореляції (2.12) складає 0,71.

$$R = \sqrt{1 - \frac{\sum (y_i - y_{pi})^2}{\sum (y_i - \bar{y})^2}}, \quad (2.12)$$

де R – показник кореляції;

y_i – споживання електроенергії за період i .

Для оцінки тісноти зв'язку між змінними моделі розраховано коефіцієнт детермінації, визначивши її як R^2 , а отримане значення 0,51 свідчить про сильний зв'язок між економічними показниками цієї функції. Для перевірки кореляції та адекватності моделі виконаємо розрахунок F-критерію (формула 2.10) для ймовірності 0,95. Так, $F_{роз} = (0,51 / (1 - 0,51)) \times (14 - 2) = 12,43$ і оскільки його значення більше за табличне 5,12 можна свідчити про адекватність моделі.

$$F_{роз} = \frac{R^2}{1-R^2} \times (n - 2), \quad (2.13)$$

де R^2 – показник детермінації;

$F_{роз}$ – фактичне значення критерію Фішера;

n – кількість періодів дослідження.

Виходячи, з прогнозованих значень виробництва електроенергії на 2025 рік [143], можна розрахувати зворотну формулу для визначення частки ІКТ сектору у ВВП (2.14), яка є елементом вразливості та детермінантою занепаду українського сектору традиційного виробництва.

$$x = a \sqrt{\frac{y}{b}} \quad (2.14)$$

$$x = {}^{-1,52} \sqrt{\frac{55}{1116,5}} = 7,24\%$$

де a та b – параметри рівняння регресії;

y – споживання електроенергії, млрд кВт-год;

x – частка ІКТ у ВВП, %.

На основі проведених розрахунків, можна зробити висновок, що цифровізація негативно впливає на традиційний виробничий сектор. Про це свідчить зростання частки сектору ІКТ у ВВП до 7,24%, що відповідає зменшенню рівня енергоспоживання.

За результатами аналізу можна виділити такі основні виклики економічній безпеці України в умовах прискорених процесів цифровізації: зростання тиску на традиційний виробничий сектор; дефіцит спеціалістів з ІКТ-кваліфікацією на ринку праці; збільшення навантаження на державні інституції.

У цьому контексті особливо високою є небезпека латентних загроз, які розвиваються в проміжку часу між появою структурних деформацій та, як наслідок, виникненням загроз. Це є результатом складного характеру механізму негативного впливу цифровізації на загрози економічній безпеці держави. Таким чином, на першому етапі компанії ІТ-сектора галузі ІКТ створюють робочі місця, доходи та технологічні рішення, згодом відбуваються зміни в економіці під впливом переваг цифровізації та зростання інфраструктури, а також залучення кваліфікованих кадрів. Утім, це призводить до отримання неконкурентних переваг та збільшення вразливості, що веде до збільшення загальних втрат, а позитивний ефект залишається локалізованим лише в окремих секторах економіки.

Таким чином, сучасні тенденції цифровізації формують незворотній вплив на загрози економічній безпеці України, який значною мірою посилює руйнівні негативні явища, завдає шкоди національним економічним інтересам та збільшує вразливість національної економіки до негативних чинників зовнішнього середовища (табл. 2.11).

Таблиця 2.11

Вплив сучасних тенденцій цифровізації на загрози економічній безпеці
України

Тенденції	Загрози
Зміна підходів до ведення воєнних дій	Кібератаки на комерційні фінансові та медіа, державні установи та підприємства логістики. Фізичне руйнування критичної цифрової та енергетичної інфраструктури. Дефіцит спеціалістів з ІКТ-навичками внаслідок релокації або мобілізації кваліфікованих кадрів. Уникнення санкцій агресором, проведення агентської діяльності за допомогою використання криптовалют. Поширення дезінформації та інформаційно-психологічних операцій через соціальні мережі та месенджери. Менша ефективність захисту військових об'єктів внаслідок використання соціальних мереж для розвідки з відкритих джерел.
Гібридне протистояння в кіберпросторі	Безкарність, поширення транскордонних загроз, злочинності та надзвичайна ефективність кібератак. Крихкість та критичність цифрової інфраструктури, інституційно-інструментальної та техніко-технологічної складових. Залежність ефективності забезпечення кібербезпеки від міжнародної партнерської підтримки. Низький резервний потенціал цифровізації для економіки-жертви і більший для економіки-агресора. Надмірна незалежність та гнучкість цифрової економіки.
Внутрішні диспропорції впровадження цифровізації	Виникнення помилок та недосконалостей внаслідок дуального ведення документообігу. Зростання ціни забезпечення систем безпеки на підприємствах, організаціях та інституціях. Структурна диспропорція проникнення технологій між галузями. Зростання навантаження на персонал при роботі з цифровими технологіями. Прийняття неправильних техніко-технологічних рішень внаслідок недостатньої кваліфікації спеціалістів. Сприяння утворенню скомпрометованого чи недосконалого законодавства задля експлуатації економіки. Недосконалість цифрових посередників.
Зовнішнє та внутрішнє прискорення процесів цифровізації	Зменшення сектору традиційного виробництва та структурні деформації національної економіки. Залежність економіки від цифрового експорту. Зменшення конкурентоспроможності традиційного виробничого сектору на внутрішньому та зовнішньому ринках. Втрата інвестиційно-інноваційного, техніко-технологічного і наукового потенціалу. Виникнення «пастки середнього доходу». Зростання залежності від якості та безперебійності енергопостачання. Руйнація кадрової конкурентоспроможності великих індустрій.

Джерело: авторська розробка

Отже, сучасні тенденції цифровізації призводять до утворення нових та трансформації традиційних загроз економічній безпеці держави, при цьому посилюючи негативні явища, викликані зовнішніми та внутрішніми детермінантами. Як бачимо, загалом тенденції ближнього зовнішнього середовища, а саме воєнні дії, вимушена міграція, гібридне протистояння в кібернетичному просторі, мають найбільший вплив та ускладнюють забезпечення економічної безпеки держави. Натомість, тенденція прискорення та стимулювання цифровізації на державному рівні може призвести до втрати конкурентоспроможності традиційного виробничого сектору на внутрішньому та зовнішньому ринках. Потрібно відмітити, що асиметрія у впровадженні цифровізації призводить до збільшення вразливості критичної інфраструктури та утворення сприятливого середовища для загроз.

А тому, для забезпечення економічної безпеки держави в умовах цифровізації необхідно враховувати її вплив на трансформацію сучасних тенденцій та виникнення нових загроз. Властивості цифровізації змінюють логіку забезпечення економічної безпеки держави, оскільки існує потреба не лише в досягненні позитивних значень за окремими показниками економічної безпеки держави, а й в управлінні процесами та основними тенденціями розвитку національної економіки, а також в збереженні балансу між прогресивними цифровими галузями та традиційним виробничим сектором, нормативному забезпеченні та регулюванні, формуванню надійних інституцій протидії загрозам цифровій та енергетичній інфраструктурі, обмеженій раціональній підтримці сектору ІКТ та забезпеченню стійкості від втручання бенефіціарів ризикової поведінки на прийняття політичний і економічних рішень.

Висновки до розділу 2

1. Здійснено критичний аналіз методичного інструментарію оцінювання рівня економічної безпеки України та виявлено його концептуальні недоліки, а саме: застарілість, суперечливість нормативного забезпечення, надмірна кількість індикаторів, фіксованість порогових значень, обмежена адаптивність до глобальних змін, що унеможливлюють ідентифікацію реальних загроз економічній безпеці держави.

2. Удосконалено методичні засади оцінювання рівня економічної безпеки держави, що, на відміну від існуючих підходів, ураховують вплив цифровізації на макро-, мікро- та нанорівнях національної економіки на основі індикаторної оцінки використання цифрових технологій, готовності до їх впровадження, вразливості до кіберзагроз та інших чинників дуального впливу цифровізації, що породжують асиметрію розвитку національної економіки, виникнення та трансформацію загроз інформаційно-цифровій складовій економічної безпеки держави в сучасних соціально-економічних умовах.

3. Здійснено аналіз рівня економічної безпеки України та її системоутворюючих складових, який протягом 2010-2023 роки знаходиться у зоні небезпечного стану. Ідентифіковано глибинні диспропорції у інвестиційно-інноваційній, макроекономічній, фінансовій, зовнішньоекономічній та демографічній сферах, що свідчить про концентрацію загроз з максимальним рівнем впливу на національну економіку. Виявлено домінуючий вплив воєнних дій та трансформаційних наслідків цифровізації на всі структурні складові економічної безпеки держави.

4. Проведено ідентифікацію потенційних і реальних загроз економічній безпеці України на основі аналізу відхилень індикаторів інформаційно-цифрової складової від їх критичних значень. Здійснено ранжування загроз цифровізації, серед яких, системний вплив на економічну безпеку справляє вразливість до

кібератак, залежність від імпорту цифрових технологій, низький рівень цифрових компетенцій, асиметрія розвитку національної економіки у напрямку надмірної концентрації ресурсів в секторі ІКТ.

5. За результатами дослідження сучасних тенденцій цифровізації, а саме, стимулювання процесів цифровізації, внутрішніх диспропорцій впровадження цифрових технологій, зміни підходів до ведення воєнних дій, поширення гібридного протистояння у кібернетичному просторі, проаналізовано дуальний вплив цифровізації на економічну безпеку держави. Доведено, що, попри стимулювання економічного розвитку, впровадження цифрових технологій в умовах воєнних викликів, створює підґрунтя для виникнення нових форм загроз та трансформації існуючих.

6. На основі кореляційно-регресійного аналізу тенденцій зростання сектору інформаційно-комунікаційних технологій та динаміки реального сектору, виявлено загрози структурних деформацій і асиметричного розвитку національної економіки в умовах цифровізації. Обґрунтовано, що переваги цифровізації локалізуються у кількох галузях національної економіки, тоді як вплив загроз, які вона генерує, проявляється в усіх складових економічної безпеки держави, що посилює внутрішні дисбаланси та ускладнює забезпечення стійкості, стабільності й адаптивності національної економіки до зовнішніх і внутрішніх викликів.

Основні результати дослідження відображені у наукових працях автора [57; 186; 199; 200; 202; 206; 210; 211; 217; 218; 226].

РОЗДІЛ 3

СТРАТЕГІЧНІ ПРІОРИТЕТИ МІНІМІЗАЦІЇ ЗАГРОЗ ЕКОНОМІЧНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ЦИФРОВІЗАЦІЇ

3.1. Розвиток інституційного забезпечення економічної безпеки України в умовах цифровізації

Мінімізація загроз економічній безпеці України ускладнюється характерними властивостями цифровізації, активізацією кіберзагроз, структурними змінами економіки, зростаючою вразливістю інфраструктури та діями бенефіціарів ризикової поведінки. У таких умовах традиційні підходи до забезпечення економічної безпеки держави втрачають свою ефективність та потребують докорінного перегляду. Такий підхід, у свою чергу, вимагатиме не лише адаптації до нових реалій, а й посилення ролі інституційного забезпечення як системного чинника, який здатний забезпечити стабільність, передбачуваність та стійкість економічної системи до внутрішніх і зовнішніх цифрових загроз. На нашу думку, саме інституційна спроможність держави, її здатність оперативно формувати, впроваджувати та адаптувати відповідні нормативно-правові, організаційні й аналітичні інструменти визначає ефективність реагування та регулювання нових та трансформованих загроз економічній безпеці в умовах цифровізації.

Потрібно відмітити, що забезпечення економічної безпеки держави в умовах глобальних викликів, зумовлених цифровізацією, вимагає комплексного підходу, який передбачає вдосконалення правового поля, підвищення компетентності державних органів, створення ефективних механізмів міжвідомчої координації, впроваджувати моніторинг ризиків та здійснювати запобігання загрозам. Особливої актуальності набуває потреба у формуванні

прозорих, адаптивних та стійких інституцій, які будуть швидко реагувати на зміни технологічного середовища та підвищувати ефективність заходів із забезпечення економічної безпеки держави. Важливо відмітити, що протидія негативному впливу цифровізації на загрози економічній безпеці держави має здійснюватися одночасно на міжнаціональному, національному, регіональному, галузевому рівні, а також на рівні бізнесу й домогосподарств.

Питання визначення категорії інституційного забезпечення економічної безпеки України є широким та знаходить чимало трактувань серед економістів-інституціоналістів. Утім, звертаючи увагу саме на безпековий аспект варто відзначити підхід Г. Колеснікової [152], яка визначає інституційне забезпечення як динамічний процес формування формальними та неформальними утвореннями правил, які впливають на поведінку учасників ринку. Основним є організаційне оформлення системи правил і норм, консолідованої у формі підприємств, інфраструктури, державних органів, а також закону та функцій-правил (ринок, ціноутворення, конкуренція, праця, власність, підприємництво). Втім, А. Пустоваров [153] уточнює, що питання інституційного забезпечення цифровізації національної економіки є результатом функціонування сукупності нормативно-правових, економічних і соціальних інститутів, що відбувається з метою докорінної, революційної зміни бізнес-моделей суб'єктів господарювання, моделей публічного управління, систем загальнонаціональних, корпоративних та особистісних цінностей на основі ефективного використання цифрових технологій.

На думку Т. Желюк [190] інституційне забезпечення економічної безпеки України має містити насамперед інституційну архітектуру, яку утворюють наднаціональні та національні інститути, що забезпечують функціонування економічної системи як єдиного цілого. Також важливою є інституційна матриця, яка представляє взаємодію формальних та неформальних інститутів економічної безпеки держави, створюючи відповідне інституційне середовище. При цьому в

процесі забезпечення економічної безпеки держави має відбуватися модернізація діючих і створення нових інститутів, які матимуть для України стратегічне значення та забезпечуватимуть збалансований розвиток національної економіки.

Саме остання точка зору щодо інституційного забезпечення економічної безпеки держави видається найбільш прийнятною, проте цей науковий підхід не уточнює механізму, яким має здійснюватися розвиток інституційного забезпечення. Тому, перспективним, на нашу думку, є підхід З. Гбур [101], за яким посилення інституційного вектору в забезпеченні економічної безпеки держави має відбуватися шляхом модернізації діючих та створення нових економічних і соціальних інститутів, які, в свою чергу, забезпечуватимуть економічне зростання та підвищення продуктивності праці на якісно новій основі. Зрозуміло, що доповнення потребує формування інституційно-правового базису на різних рівнях ієрархії національної економіки, що забезпечується шляхом виконання інститутами функцій прийняття рішення, інформування та мотивації. Так, побудова цілісної системи економічної безпеки в умовах цифровізації вимагає узгодження окремих політик на основі модернізації її підсистем. Це передбачає створення інституцій для моніторингу цифрових ризиків, розподіл повноважень суб'єктів різних рівнів системи та забезпечення функціонування дієвих мотиваційних механізмів для реалізації компетентних управлінських рішень у питаннях цифровізації.

На наш погляд, в умовах значного негативного впливу цифровізації на економічну безпеку України помірне напрацювання та адаптація інституцій є нерезультативним. Тому існує необхідність залучення інвестицій, адаптації міжнародного досвіду, а також посилення інтеграції у існуючі інституції забезпечення економічної безпеки на регіональному рівні з метою інтенсифікації розвитку інституційного забезпечення економічної безпеки України в умовах цифровізації.

За оцінками експертів Світового банку [154], вплив цифровізації на економічну безпеку країн світу залежить від низки визначених інституційних умов, таких як нормативно-правова база, яка забезпечує можливість фірмам використовувати переваги цифрових технологій для конкуренції та інновацій. Утім, використання позитивного впливу цифровізації можливе лише за умови достатньої кваліфікації державних службовців, що супроводжують організаційно-правові процеси. Саме тому підзвітність державних установ і організацій забезпечує оперативне реагування держави на загальносуспільні потреби і вимоги громадян.

Тому, доцільно провести аналіз досвіду країн, які є географічно або економічно близькими до України, щодо розвитку інституційного забезпечення економічної безпеки в умовах цифровізації. Це дозволить виокремити регіональні інституційні здобутки, переваги та недоліки, приділяючи особливу увагу досвіду ЄС та її країн-учасниць. Як зазначалося у підрозділі 2.1, порівняння інституційного забезпечення економічної безпеки на національному рівні в Україні та на наднаціональному рівні в Європейському Союзі зумовлене рядом об'єктивних чинників. Зокрема, країни-члени ЄС передають елементи забезпечення своєї економічної безпеки у виняткову або спільну компетенцію, що, в свою чергу, формує уніфіковану регіональну нормативно-правову та інституційну модель.

З огляду на курс України на євроінтеграцію, адаптація європейського законодавства є продовженням розвитку інституційного забезпечення. Тому, з метою мінімізації негативного впливу цифровізації на загрози економічній безпеці держави, доцільно розглядати та адаптувати саме досвід ЄС.

Утім, потрібно відмітити, що розвиток інституційного забезпечення економічної безпеки на наднаціональному рівні в Європейському Союзі почав набувати системного характеру лише в останні роки. Цей процес у 2023 році активізувався на тлі геополітичних змін, зокрема, повномасштабного російського

вторгнення в Україну, що суттєво вплинуло на перегляд стратегій енергетичної, військової та економічної безпеки по всьому світу.

На відміну від цього, затримка розвитку інституційного забезпечення економічної безпеки у ЄС, на наш погляд, пояснюється п'ятьма системними факторами.

По-перше, складність інституційної структури економічної безпеки в ЄС (табл. 3.1) зумовлює фрагментацію інституцій на національні та наднаціональні. Так, більшість питань оборони залишаються під контролем національних урядів, а втім, аспекти економічної безпеки делегуються до міжнародних інституцій, що перешкоджає розробці цільної стратегії. Як наслідок, суттєво зменшується здатність ЄС оперативно реагувати на виклики та впроваджувати спільні дії.

Таблиця 3.1

Багаторівнева структура компетенцій у сфері економічної безпеки в ЄС

Рівень компетенції ЄС	Опис компетенції	Складові економічної безпеки держав-членів ЄС
Виняткова	Виключні повноваження інституцій ЄС над національним законодавством країн-учасниць	Виробнича, енергетична, зовнішньоекономічна та продовольча безпека в аспектах митного контролю та загальної торгової політики. Грошово-кредитна та валютна безпека для країн Єврозони. Бюджетна безпека самого Євросоюзу та ключових інституцій та інструментів.
Спільна	Країни-учасниці мають компетенцію в тій мірі, в якій інституції ЄС не скористалися своєю	Екологічна, транспортно-інфраструктурна, демографічна, продовольча, енергетична, соціальна безпека загалом. Бюджетна безпека країн-учасниць у відповідності до загальноєвропейської політики.
	Інституції ЄС здійснюють заходи в мірі, в якій не перешкоджають країнам-учасникам	Інвестиційно-інноваційна та виробнича безпека в передових наукомістких галузях, а також пов'язані з ними дослідження. Безпекові проти економічного примусу та втручання третіх країн.
	Інституції ЄС визначають умови за якими діють країни-учасниці	Загальна економічна (окрім перелічених вище елементів), оборонна та зовнішня політика. Міграційна безпека. Цифрова безпека та захист від викрадення передових технологій.
Допоміжна	Інституції ЄС підтримують та доповнюють заходи країн-учасниць	Демографічна та виробнича безпека загалом в аспектах промисловості. Громадська оборона та національні збройні сили. Банківська безпека.

Джерело: складено автором на основі [72; 163-167; 226]

Другим фактором є балансування принципів та переваг відкритого ринку проти витрат і обмежень протекціоністських заходів безпеки. Втім, сучасний геополітичний ландшафт потребує щоб інструменти стратегічного контролю, будь то експортний контроль або перевірка прямих іноземних інвестицій, були додатково посилені. Це призводить до дилеми, оскільки ефективне забезпечення економічної безпеки держави може порушити принципи відкритого ринку, а це, в свою чергу, спричиняє політичний і соціальний спротив.

Третім фактором є тривале і надмірне покладання на оборонні програми НАТО та військовий потенціал США, що зменшувало потенціал побудови автономних оборонних ініціатив, таких як PESCO. Натомість недостатнє інвестування у спільну європейську оборонну інфраструктуру підсилило вразливість перед гібридними кібернетичними та військовими загрозами з боку росії та Китаю.

Четвертий фактор обґрунтовується суперечливими інтересами країн-учасниць ЄС у питаннях економіки, оборони, геополітики, енергетики, виробництва, інвестицій та соціальних питань, що зумовило утворення прогалин та «сірих зон» на рівні різних національних законодавств. Такі прогалини дозволяють менш добросовісним країнам, зокрема, бенефіціарам ризикової поведінки, покращувати своє фінансове становище шляхом експлуатації недоліків безпекової системи та умисно підтримувати їх.

І наостанок, п'ятим фактором є складна демократично-політична система, що покладається на добровільність заходів, довготривалі переговори між учасниками і роботою різноманітних комісій, а також недосконалістю механізмів забезпечення справедливого розподілу видатків і отриманих доходів від цифровізації економіки ЄС.

Тому, попри значний економічний та політичний потенціал ЄС, розвиток інституційного забезпечення економічної безпеки, зокрема, в умовах цифровізації, був ускладнений внутрішніми протиріччями та недосконаlostями

демократичних процесів. Це, в свою чергу, виявило вразливість національних економік до низки новітніх загроз, зокрема, енергетичної залежності від росії та її втручання у вибори, технологічного шпигунства та фінансових інтервенцій Китаю. Утім, російська агресія, зміна геополітичних векторів та досвід України актуалізували питання розвитку інституційного забезпечення економічної безпеки держави.

Так, український досвід у сфері економічної безпеки відрізняються фокусом на безпосередньому протистоянні загрозам агресора та відновленню після атак, тоді як ЄС більше акцентує увагу на стратегічній протидії глобальним загрозам. Зокрема, Європейська стратегія економічної безпеки [163] підкреслює збереження відкритого ринку при одночасному посиленню власної технологічної переваги. Водночас, інститути ЄС координують міждержавні підходи, що сприяє встановленню єдиного рівня кіберзахисту, розробляються спільні схеми сертифікації та підвищенню стійкості європейської інформаційно-цифрової складової економічної безпеки. Україна ж здебільшого спирається на власні інститути, що зумовлено рівнем інтеграції у міжнародні процеси, масштабами загроз економічній безпеці і відсутністю наднаціональних інструментів із силовими повноваженнями.

Загалом, український досвід поєднує імплементацію європейських принципів з урахуванням воєнних реалій та загроз, притаманних унікальній безпековій ситуації країни. Національна система демонструє достатній рівень ефективності, але у порівнянні з ЄС (табл. 3.2) потребує вдосконалення підходів у контексті сучасних викликів за потенційної підтримки партнерів.

Порівняльний аналіз інституційного забезпечення економічної безпеки України та ЄС дозволяє визначити, що з одного боку, національні інститути характеризуються фрагментарністю та обмеженою координацією. А з іншого – наднаціональні рішення є занадто негнучкими для урахування національної специфіки окремих країн-учасниць.

Таблиця 3.2

Порівняння інституційного забезпечення економічної безпеки України та ЄС
в умовах цифровізації

Характеристики	Україна	ЄС
Рівні інституційного забезпечення	2-рівнева система (внутрішня та зовнішня безпека)	3-рівнева система (зовнішня безпека ЄС, внутрішня безпека ЄС, національна безпека країн-учасниць)
Стратегічні документи	Стратегія економічної безпеки України 2021 року, Стратегія цифрового розвитку інновацій до 2030 року.	Стратегія економічної безпеки ЄС від 2024 року
Цілі та орієнтири	Сталий розвиток національної економіки, інтеграція України в європейський економічний простір, розвиток рівноправного взаємовигідного економічного співробітництва з іншими державами.	Мінімізація ризиків, у контексті посилення геополітичної напруженості та прискорених технологічних зрушень, зберігаючи при цьому максимальний рівень економічної відкритості та динамізму.
Головні напрями	Захист від усесторонньої агресії з боку росії та її союзників; забезпечення ефективності бюджетних та гармонізація економічних процесів; захист та збереження наявної та формування ефективної інноваційної наукомісткої економіки і торгівлі.	Стійкість ланцюгів поставок, включаючи енергетичну безпеку; фізична- та кібербезпека критичної інфраструктури; технологічна безпека та захист критичних технологій; захист від економічної залежності та економічного примусу.
Інституції	Президент України, Верховна Рада України, Кабінет міністрів України, Рада національної безпеки і оборони України, Національний банк України, Бюро економічної безпеки України, Спеціалізована антикорупційна прокуратура, НАБУ, Головне управління розвідки, Генеральна прокуратура.	Високий представник ЄС, Європейська комісія, Європейський центральний банк, Європейський інвестиційний банк, Прокуратура Європейського союзу, Європейський центр компетенцій з кібербезпеки, Європейська рада із захисту даних, Європейський консорціум цифрової інфраструктури, Постійна структурована співпраця.
Нормативно-правове забезпечення	ЗУ «Про національну безпеку України», Стратегія національної безпеки України, Національна економічна стратегія на період до 2030 року, ЗУ «Про боротьбу з корупцією», ЗУ «Про критичну інфраструктуру», Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом [...] з іншої.	NextGenerationEU, Промислова стратегія ЄС, Європейська інноваційна програма, RepowerEU, Закон про критичні сировинні матеріали, Регламент про іноземні субсидії; Закон про кіберсолідарність, Угоди про вільну торгівлю, «Global Gateway», Програма «Digital Europe», The European Chips Act, Dual-use export controls.
Інструменти	Бюджет, валютні інтервенції, підтримка галузей, облікова ставка, ліцензування, фінансовий моніторинг, антимонопольне регулювання, розвиток інновацій,	Інструмент відновлення та стійкості SURE, антимонопольні розслідування, фінансовий нагляд, регулювання обміну даних між членами, The Anti-Coercion Instrument, The EU toolbox for 5G security.

Джерело: складено автором на основі [30-31; 34; 59;72; 121; 162-167; 178; 226]

Отже, ефективна протидія загрозам економічній безпеці держави в умовах цифровізації можлива лише за міжнародної співпраці на рівні спільних інституцій. Такий підхід спрямований на мінімізацію впливу стрімкого зростання транскордонної злочинності, яка використовує анонімність у мережі та хмарні платформи для ухилення від юрисдикції національних систем правопорядку. Внаслідок неефективної діяльності державних інституцій, а також недосконалості внутрішнього інституційного забезпечення, детермінанти дальнього зовнішнього середовища є ключовим джерелом виникнення загроз, таких як кібератаки, викрадення даних, технологічне шпигунство.

Тому подальший розвиток інституційного забезпечення економічної безпеки України, на наш погляд, має покладатися на консолідацію інформаційних ресурсів, а також технічних, аналітичних та оперативних ресурсів багатьох держав. Включно із гармонізацією стандартів безпеки інформаційно-цифрової складової, створенням спільних протоколів реагування на кіберзагрози та уніфікацією правових інструментів мінімізації негативного впливу цифровізації.

Таким чином, інституційна архітектура ЄС може бути прикладом для розвитку інституційного забезпечення економічної безпеки України в умовах цифровізації, де існує інституція, що виконує роль координатора, а спеціалізовані агентства забезпечують технічну та експертну підтримку. Так, для України, що знаходиться у процесі гармонізації з європейським законодавствами та вимогами, участь у наднаціональних ініціативах створює можливості для підвищення ефективності регулювання впливу цифровізації на загрози економічній безпеці. Це дозволяє здійснювати обмін розвідданими та розгортати спільні стратегії для захисту критичної інфраструктури та національних економічних інтересів.

Отже, для цілей дослідження потрібно дослідити ініціативи, подані до стратегії економічної безпеки ЄС. Серед них варто виокремити найважливіші пріоритети та відповідні способи підтримки інформаційної та цифрової складової економічної безпеки в Європі (табл. Г.1, додаток Г).

На підставі проведеного аналізу, варто виділити декілька пріоритетних напрямів розвитку інституційного забезпечення економічної безпеки, зокрема, посилення контролю за рухом інвестицій та коштів третіх сторін, удосконалення експортного контролю, протидія недобросовісному впливу на науково-дослідні установи.

Тим часом, ЄС зосереджується на створенні архітектури безпеки за рахунок протекціонізму національних виробників через застосування інструментів захисту цифрової інфраструктури, посиленні заходів фінансового моніторингу та координації спільних дій проти економічного примусу з боку третіх держав. Паралельно, питання подальшого партнерства відкриває багато довгострокових можливостей і не лише серед членів ЄС. Це відбувається шляхом поглиблення співпраці з країнами, що розділяють спільні безпекові цінності, зміцнення ланцюгів постачання, а також через просування угод про вільну торгівлю та інвестування у розвиток партнерських країн. Такий комплексний підхід поєднує традиційне інституційне забезпечення з адаптивними механізмами, що дозволяють швидко реагувати на нові виклики.

Отже, інституційне забезпечення економічної безпеки ЄС є багаторівневим, спрямованим на захист економічного суверенітету країн-учасниць та союзу загалом, а також сприяє стійкості та інноваційному розвитку в умовах глобальних викликів та трансформацій. Основними його складовими є захист інвестицій та стратегічних активів через посилений фінансовий моніторинг, координацію експорту для контролю над товарами подвійного призначення та військовими технологіями, збереження технологічного лідерства у високотехнологічних галузях. Особлива увага

приділяється безпеці наукових розробок та технологій, що поєднує відкритість досліджень із захистом від шпигунства, підвищення конкурентоспроможності шляхом інвестування в інновації, розвиток людського капіталу та диверсифікацію ланцюгів постачання.

З огляду на специфіку України, по-перше, можна відзначити необхідність створення комплексної системи інституційного забезпечення економічної безпеки. Такий підхід має враховувати як європейський досвід, так і національні потреби, зокрема в умовах війни та гібридних загроз. По-друге, вони відкривають перспективи для інтеграції України у європейський економічно-безпековий простір через стратегічне партнерство. Зокрема, через спільну розбудову цифрових та військових технологій, адаптації систем експортного контролю, а також захисту інновацій. Це, в свою чергу, створює передумови для підвищення економічної стійкості, захисту критичної інфраструктури та зміцнення загальнонаціональної безпеки.

Інституційне забезпечення економічної безпеки ЄС базується на таких інструментах, як тарифний протекціонізм національного виробника, моніторинг субсидій, протидія економічному примусу та співпраця в межах міжнародного партнерства. Зазначимо, що оновлений підхід дозволяє нейтралізувати негативний вплив цифровізації, геополітичного суперництва та кризових явищ і забезпечувати стійке економічне зростання, стабільність та суверенітет ЄС.

Оцінюючи архітектуру інституційного забезпечення економічної безпеки Європейського Союзу в умовах цифровізації (рис. 3.1), варто відзначити, що її структура передбачає як вертикальну підпорядкованість, так і горизонтальну координацію між незалежними відомствами.

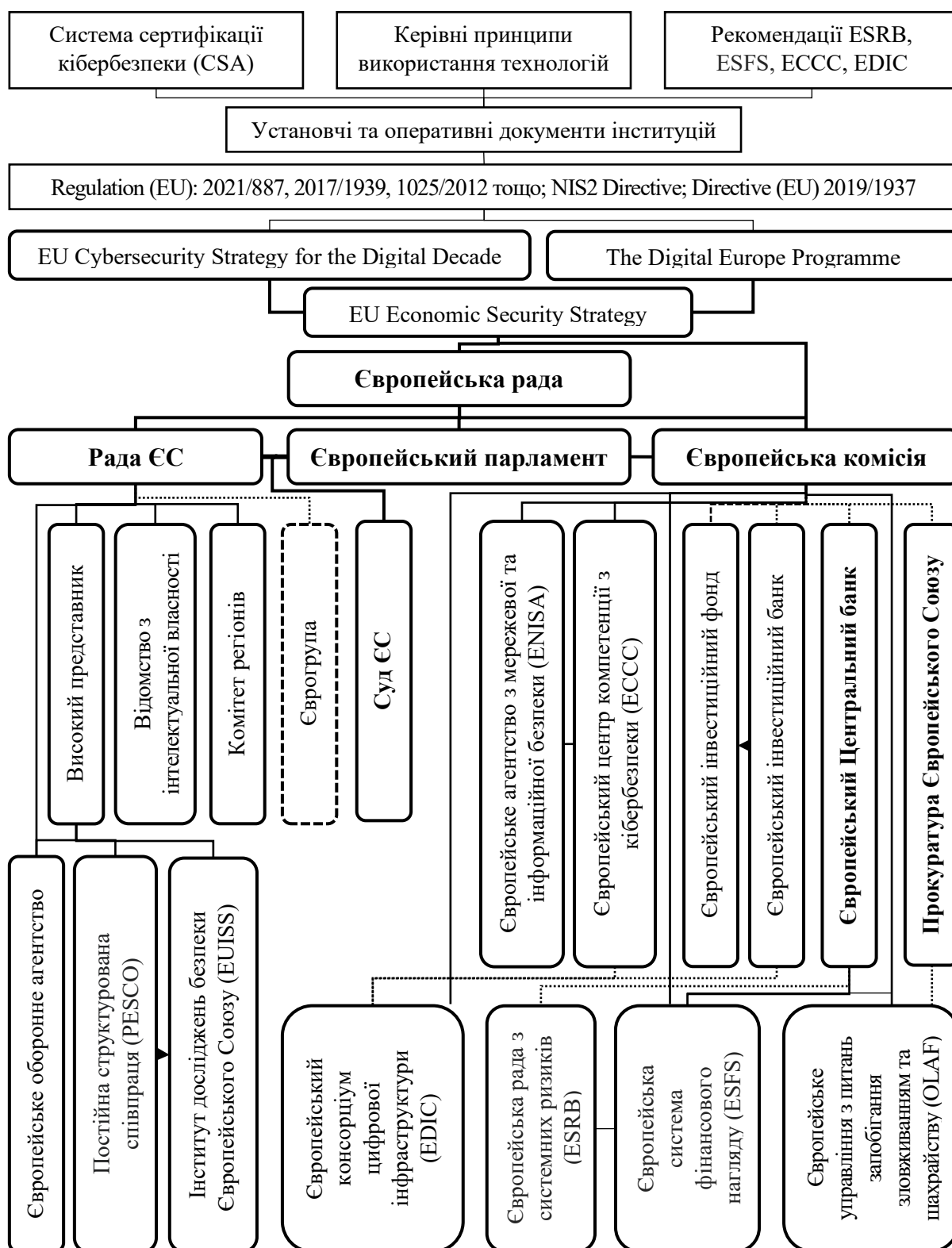


Рис. 3.1. Архітектура інституційного забезпечення економічної безпеки Європейського Союзу в умовах цифровізації

Джерело: авторська розробка

Отже, Європейська Рада є органом, який визначає загальний політичний напрямок і пріоритети ЄС щодо забезпечення економічної безпеки. Тим часом Європейська Комісія представляє виконавчу гілку влади та має право законодавчої ініціативи. Рада ЄС та Європейський Парламент функціонують як законодавчі органи та спільно ухвалюють закони щодо забезпечення економічної безпеки. На відміну від цього, Суд ЄС та підпорядковані йому суди забезпечують тлумачення й застосування права ЄС та здійснюють правовий контроль за діяльністю інших інституцій. Основне навантаження інституційного забезпечення економічної безпеки покладається на Європейську комісію, яка або прямо контролює, або співпрацює з незалежними відомствами і агенціями у сфері забезпечення економічної безпеки.

Зазначена архітектура інституційного забезпечення економічної безпеки ЄС дозволяє не лише протидіяти загрозам, але й розподіляти повноваження між різними інституціями, запобігаючи надмірній концентрації влади. Втім, такий рівень насичення інституціями на національному та наднаціональному рівні потребує глибокого узгодження політики та застосування єдиної стратегії. Позаяк неузгодженість нормативно-правового забезпечення діяльності суб'єктів на національному та наднаціональному рівні призводить до загрози утворення «сірих зон». Такі зони мають певний рівень безконтрольності, що зумовлює появу та трансформацію загроз економічній безпеці держав та ЄС загалом. На противагу розробляються комплексні рішення і закони спрямовані на заповнення інституційних прогалин. Серед яких особливу увагу слід приділити тим, що стосуються впливу цифровізації. Так, варто здійснити аналіз нормативно-правового забезпечення економічної безпеки Європейського Союзу та їх складових в умовах цифровізації (табл. Г.2, додаток Г).

Отже, виходячи з проведеного аналізу, можна зазначити, що цифровізація виступає визначальним чинником розвитку інституційного забезпечення економічної безпеки в Європейському Союзі. Застосування цифрових

інструментів сприяє підвищенню спроможності держав до своєчасного виявлення, реагування та нейтралізації зовнішніх і внутрішніх загроз. Зокрема, Друга директива про мережеву та інформаційну безпеку [177] передбачає уніфікацію стандартів кіберзахисту, розширення сфери регулювання на вразливі сектори економіки та запровадження суворішої відповідальності за інциденти.

Європейський Акт про напівпровідники [165] формує технологічну основу економічної безпеки, фокусуючись на стійкості ланцюгів постачання, створенні науково-технічної інфраструктури та реалізації стратегії фінансових інвестицій. Аналогічно, Європейський набір інструментів безпеки мереж 5G [164] забезпечує системну відповідь на загрози, пов'язані з поширенням інфраструктури для мереж нової якості.

У межах політики протидії негативному впливу детермінант зовнішнього середовища виокремлюється інструмент протидії економічному тиску [166], що поєднує дипломатичний механізм стримування з практикою економічних санкцій у випадку порушення норм міжнародного права з боку третіх країн. Він базується на узгодженості колективної відповіді, посиленні економічної ізоляції агресора, а також правовому інструментарії відшкодування завданих збитків. Потрібно відмітити, що експортний контроль за товарами подвійного призначення [157; 158], у свою чергу, є стратегічним елементом захисту критичних технологій і передбачає систему ліцензування, транзитних обмежень та механізми співпраці між державами-членами для ідентифікації ризикових транзакцій.

Натомість, особливу роль у підвищенні інституційної стійкості системи економічної безпеки відіграють цифрові інформаційні платформи та антикризові механізми. Так, система ORBIS [168] дозволяє здійснювати фінансову аналітику щодо приватних компаній, їх власників та транзакційної поведінки, що посилює інструменти фінансової розвідки та сприяє мінімізації ризиків економічних правопорушень. У свою чергу, тимчасовий інструмент SURE [167],

запроваджений для боротьби з безробіттям під час пандемії COVID-19, вже продемонстрував ефективність саме гнучких інституцій. Його структурними компонентами були фінансова підтримка, координаційні механізми та розподіл ризиків, що заклало прецедент застосування тимчасових інструментів у якості засобів довгострокової стабілізації економічної системи в умовах цифрових викликів.

Також на національному рівні в різних країнах ЄС існують інституції, діяльність яких спрямована на протидію загрозам економічній безпеці, специфічних для цих країн. Доцільно, на наш погляд, розглянути деякі з них, що мають значний суб'єктний вплив у питаннях інституційного забезпечення економічної безпеки на національному, регіональному або галузевому рівнях.

Так, у Німеччині діє Закон про захист персональних даних, який встановлює правила збору, зберігання та використання персональних даних і має на меті захист приватної інформації та забезпечення безпеки обробки даних [171, 172]. Він додатково удосконалює загальноєвропейське положення, забезпечуючи надійніший рівень збереження персональних даних в умовах зростаючих загроз витоку конфіденційної інформації. А у Франції, Національне агентство безпеки інформаційних систем, у свою чергу, забезпечує захист інформаційної безпеки не лише державних структур, але й приватних компаній. Такі дії важливі для забезпечення стійкого розвитку економіки країни загалом [172]. Важливу роль у забезпеченні економічної безпеки Польщі відіграють різні державні органи та установи, зокрема, діяльність Міністерства розвитку, праці та технологій спрямована на забезпечення розвитку економіки країни, створення сприятливих умов для розвитку бізнесу [172], в тому числі є важливою інституцією забезпечення цифровізації національної економіки.

Варто виділити інституції Великої Британії, вже не учасниці ЄС, а проте регіонального лідера. Так, в питанні забезпечення її кібербезпеки ключовою інституцією є Національний центр кібербезпеки, що керується широким

спектром регуляторного забезпечення, а саме Законом про захист даних та Законом про безпеку в Інтернеті, які формують проактивну політику запобігання зовнішньому втручанню та небезпечному використанні цифрової інфраструктури [175].

Поєднання архітектури наднаціональних, національних інституцій та окремих інструментів створює унікальну своєрідну модель, яка відповідає принципам вільного ринку й демократичності ЄС та створює гнучку систему протидії ризикам і загрозам у динамічних умовах прискореної цифровізації. Однією з визначальних переваг нової стратегії економічної безпеки ЄС, на нашу думку, є спроможність до впровадження радикальних рішень без необхідності здійснення тривалої структурної трансформації. Зокрема, поєднання трьох складових: уніфікації регуляторного забезпечення, розвитку технологічних інструментів, глибшій інтеграції країн на рівні ЄС та залучення третіх країн.

Натомість українська модель, попри наявність напрацьованого практичного досвіду та низки якісних рішень, характеризується концептуальною, інструментальною та змістовною незбалансованістю. Так, аналізуючи досвід ЄС, перш за все, варто виділити цільове поєднання інструментів, відповідних інституцій та регуляторного забезпечення. Таке поєднання дозволяє протидіяти загрозам економічній безпеці в умовах цифровізації, зокрема кібератакам, втрати технологічної переваги та цифрового суверенітету, втручанню третіх країн, нестачі мережі покриття, безробіття, використання цифрової інфраструктури для ухилення від податків та фінансування тероризму.

По-друге, це законодавчий, технічний та інституційний дисбаланс у розвитку інституційної підтримки України, що посилює вже наявний негативний вплив цифровізації на загрози економічній безпеці держави. Зокрема, вже існуючі цифрові створюють додаткові перешкоди для інтеграції систем моніторингу в єдину концепцію, яка дозволила б вільно, повно та прозоро регулювати надходження, витрати, використання та цілі міжнародної допомоги.

Отже, варто визначити позитивні та негативні аспекти уніфікації та інтеграції нормативно-правових та інформаційно-технологічних рішень (табл. 3.3).

Таблиця 3.3

Позитивні та негативні аспекти інституційного забезпечення економічної безпеки України шляхом уніфікації та інтеграції цифрових і нормативних рішень

	Позитивні аспекти	Негативні аспекти
Нормативні рішення	Уніфікація сприяє зменшенню суперечливості законодавства, ризиків корупції та розміру «сірих зон». Зменшення кількості різночитання закону призводить до менших можливостей для легального уникнення від сплати податків чи подання звітності. Зрозуміле законодавство сприяє позитивному іміджу державних інституцій, спрощує взаємодію з органами державної влади для громадян та бізнесу.	Інституції та департаменти за інерцією чинитимуть супротив, а впровадження нових актів вимагатиме часу. Опрацювання нових законів збільшить навантаження на державних посадовців, потребу в кваліфікованих кадрах, при обмежених ресурсах. Облік аналогових форм збору інформації призводить до технічних помилок у первинній інформації.
Цифрові рішення	Автоматизація призводить до зменшення людського фактору та прискорення оперативних процесів, а їх утилітарність до прозорості діяльності суб'єктів економіки. Цифрові сервіси зменшують навантаженість держслужбовців, забезпечують доступ до якісної інформації та уможливають використання існуючої цифрової інфраструктури для зменшення бюджетних витрат.	Масштабна діджиталізація з використанням різних технічних рішень призводить до виникнення непов'язаних між собою цифрових баз даних. Розробка та уніфікація програмного забезпечення обліку може бути ускладнена конфліктністю різних мов програмування та існуючих систем.

Джерело: авторська розробка

Утім, уніфікація та інтеграція цифрових і нормативних рішень мають доповнюватися архітектурою інституційного забезпечення економічної безпеки України (рис. 3.2). Так, для розуміння можливості застосування, адаптації чи запозичення рішень ЄС варто розуміти, що національна система хоч має схожі елементи, проте є не лише неспівставною, а і не відповідає вимогам сучасності. Цьому сприяли загальна недосконалість інституцій, законодавства, різноманіття застосованих технічних рішень, але найголовніше – відсутність уніфікованої стратегії розвитку. Всі ці фактори у поєднанні створюють додаткові виклики подальшому розвитку інституційного забезпечення економічної безпеки в умовах цифровізації.

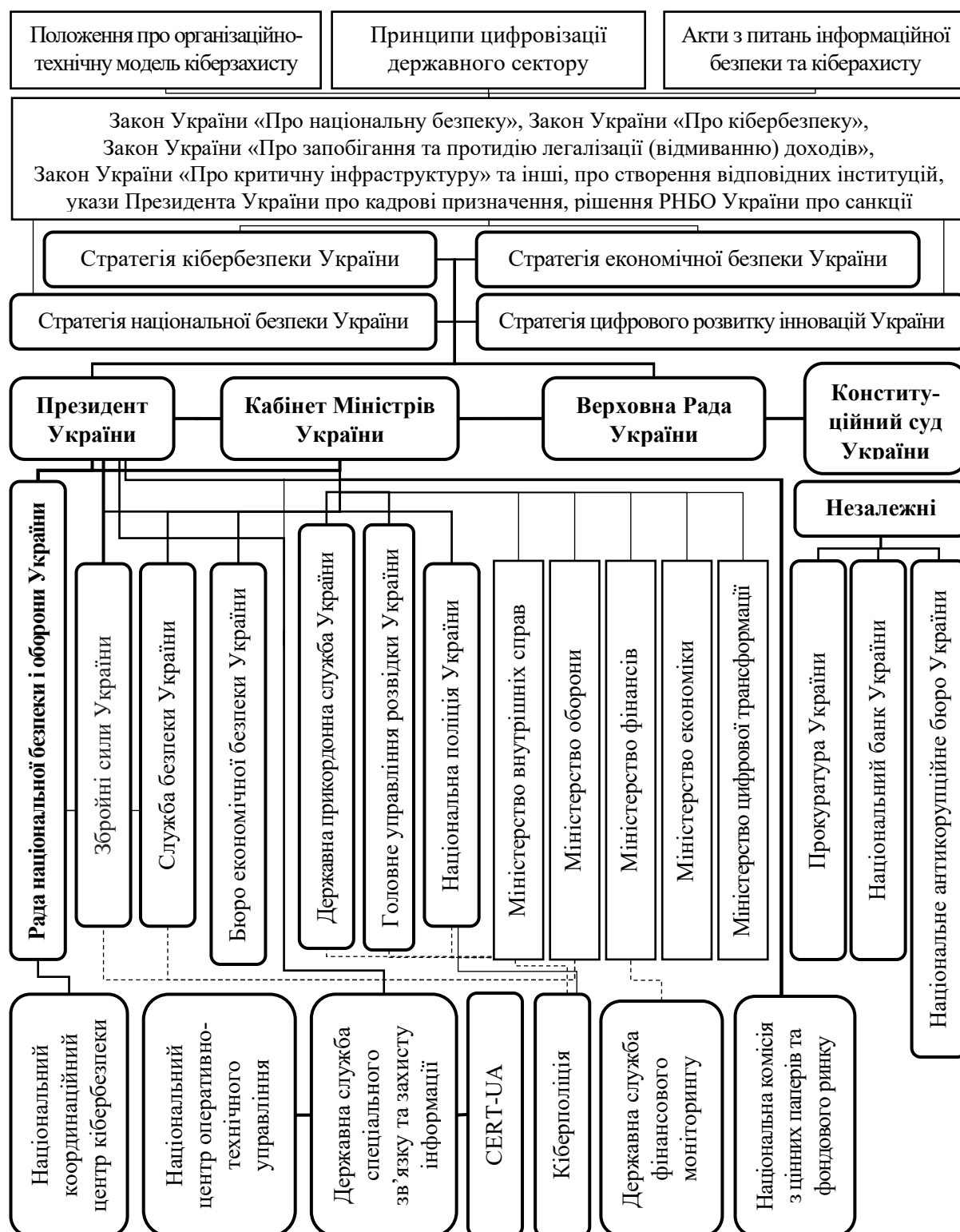


Рис. 3.2. Архітектура інституційного забезпечення економічної безпеки України в умовах цифровізації

Джерело: авторська розробка

Головним недоліком української архітектури інституційного забезпечення економічної безпеки порівняно з ЄС, на нашу думку, є концентрація функцій контролю та регулювання на Кабінеті Міністрів України, тоді як Європейська комісія делегує окремі питання із забезпечення економічної безпеки на нижчі рівні інституційної ієрархії. Також можна відслідкувати спільні рішення на національному рівні України, Франції та Польщі та наднаціональному рівні ЄС. Натомість національні системи забезпечення економічної безпеки Німеччини та Великої Британії демонструють інший підхід, де більшу роль відіграють розвинені фінансові інституції. Такий підхід дозволяє здійснювати проактивні заходи захисту національних економічних інтересів без директивного державного втручання. Утім, цей шлях розвитку є малоімовірним сценарієм для України, зважаючи на вже існуючу модель зосереджену на інституціях виконавчої влади, а трансформація потребуватиме значного часу та наявності високого рівня економічної безпеки.

Утім, зважаючи на сучасні воєнні виклики український досвід із забезпечення економічної безпеки держави є унікальним та цінним для євроінтеграційних процесів, оскільки жодна з країн ЄС не має досвіду інституційного забезпечення економічної безпеки в умовах воєнних дій із одночасним активним сприянням цифровізації та розвитком цифрових технологій. Так, в умовах інтенсивної цифровізації український уряд попри воєнні виклики впроваджує та вдосконалює цифрові технології для захисту критичної інфраструктури, протидії кіберзагрозам, посилення обороноздатності країни та підтримки макроекономічної стабільності. Отже, визначена в стратегії ЄС орієнтація на формування регіональної економічної безпеки є передумовою для поєднання сильних сторін обох підходів та компенсації їх недоліків.

Далі, варто скористатися SWOT-аналізом підходів до інституційного забезпечення економічної безпеки України та ЄС (табл. 3.4). Він дозволить наочно продемонструвати спільні елементи, переваги і недоліки окремих

підходів до інституційного забезпечення економічної безпеки та їх взаємної інтеграції.

Таблиця 3.4

SWOT-аналіз підходів до інституційного забезпечення економічної безпеки України та

ЄС

	Сильні сторони	Слабкі сторони
Україна	Досвід протистояння економічному тиску та формування економічної безпеки держави в умовах жорсткої економії ресурсів. Розвинений сектор ІКТ, сприяє впровадженню цифровізації та зменшує витрати на забезпечення економічної безпеки держави.	Слабкість та політична заангажованість інституцій зменшує ефективність рішень із забезпечення економічної безпеки держави. Диспропорція ресурсів, сил та повноважень між різними інституціями та агенціями призводить до слабого розвитку інструментів економічної безпеки держави.
ЄС	Значні фінансові ресурси, перестрахування та хеджування фінансових ризиків відкриває ширші можливості для забезпечення економічної безпеки держави. Розвинена інфраструктура та гнучка система інструментів є основою для подальшого розвитку інституційного забезпечення. Достатній рівень нормативного забезпечення економічної безпеки в умовах цифровізації, що дозволяє стимулювати її позитивний вплив.	Потреба в глибокій кооперації та комунікації між великою кількістю учасників з різними цілями сповільнює розвиток та реагування на загрози. Нерівнозначність учасників ускладнює комунікацію та спільні заходи із забезпечення економічної безпеки держави.
	Можливості	Загрози
Україна	Орієнтація на євроінтеграцією слугує підґрунтям для послідовного розвитку інституційного забезпечення та використання досвіду ЄС та країн-учасниць. Орієнтація на захист та стабілізацію ставить простіші, більш досяжні цілі та не потребує значного збільшення витрат.	Загальна слабкість економіки, бюджетні диспропорції створюють вразливе середовище для втручання третіх сторін в цифрову інфраструктуру. Використання цифрових інструментів зі злочинними мотивами призводять до зменшення ефективності державного управління.
ЄС	Орієнтація на науку та розвиток, здобуття технологічної переваги дозволяє послідовно забезпечувати економічну безпеку держави та сприяти інноваційному розвитку. Широкий простір для формування власної політики, з урахуванням нової світової системи економічної безпеки держав на принципах демократії та відкритого ринку.	Залежність від США в питаннях обороноздатності. Недостатня сформованість єдиного бачення партнерів між країнами різних регіональних блоків, що створює вразливе середовище для дій третіх сторін, технологічного шпигунства, економічного тиску та диверсій. Велика вартість утримання, дублювання функцій інституцій.

Джерело: авторська розробка

Отже, можна зазначити, що Україна має перевагу в оперативних рішеннях із протидії критичним загрозам. Водночас інституційні диспропорції призводять до дублювання функцій, зростання витрат та зниження ефективності управління. На заваді стає також відсутність кваліфікованих кадрів, обмеженість фінансування та декларативність окремих ініціатив.

Натомість ЄС демонструє інтегрований підхід до інституційного забезпечення економічної безпеки. Утім, певна асиметрія між рівнем фінансового розвитку та проникнення цифровізації окремих держав-членів, а також повільний процес гармонізації національних стратегій з єдиною політикою ЄС залишаються вагомими проблемами, що зменшують кумулятивну ефективність заходів забезпечення економічної безпеки.

У питанні запозичення існуючих інструментів Україна вже зобов'язалася привести своє законодавство у відповідність до директиви NIS2, Закон України «Про основні засади забезпечення кібербезпеки України» також має на меті гармонізацію законодавства із ЄС. Налагоджено взаємодію між ENISA, CERT-EU та CERT-UA, активно вивчається та впроваджується система ORBIS для збільшення ефективності агенцій фінансового моніторингу і розслідування злочинів. Важливим і можливим, на нашу думку, є запозичення європейського набору інструментів безпеки мереж 5G, щоб сприяти розвитку інфраструктури у відповідності до європейських вимог. Утім, інші вищезазначені інструменти потребують глибшої інтеграції між Україною та ЄС.

А отже, розвиток інституційного забезпечення економічної безпеки України в умовах цифровізації має здійснювати в контексті інтеграції України у безпековий простір ЄС шляхом регуляторного удосконалення через гармонізацію нормативно-правового забезпечення економічної безпеки, посилення інституцій і компетенцій з одночасним стимулюванням техніко-технологічного розвитку (рис. 3.3).

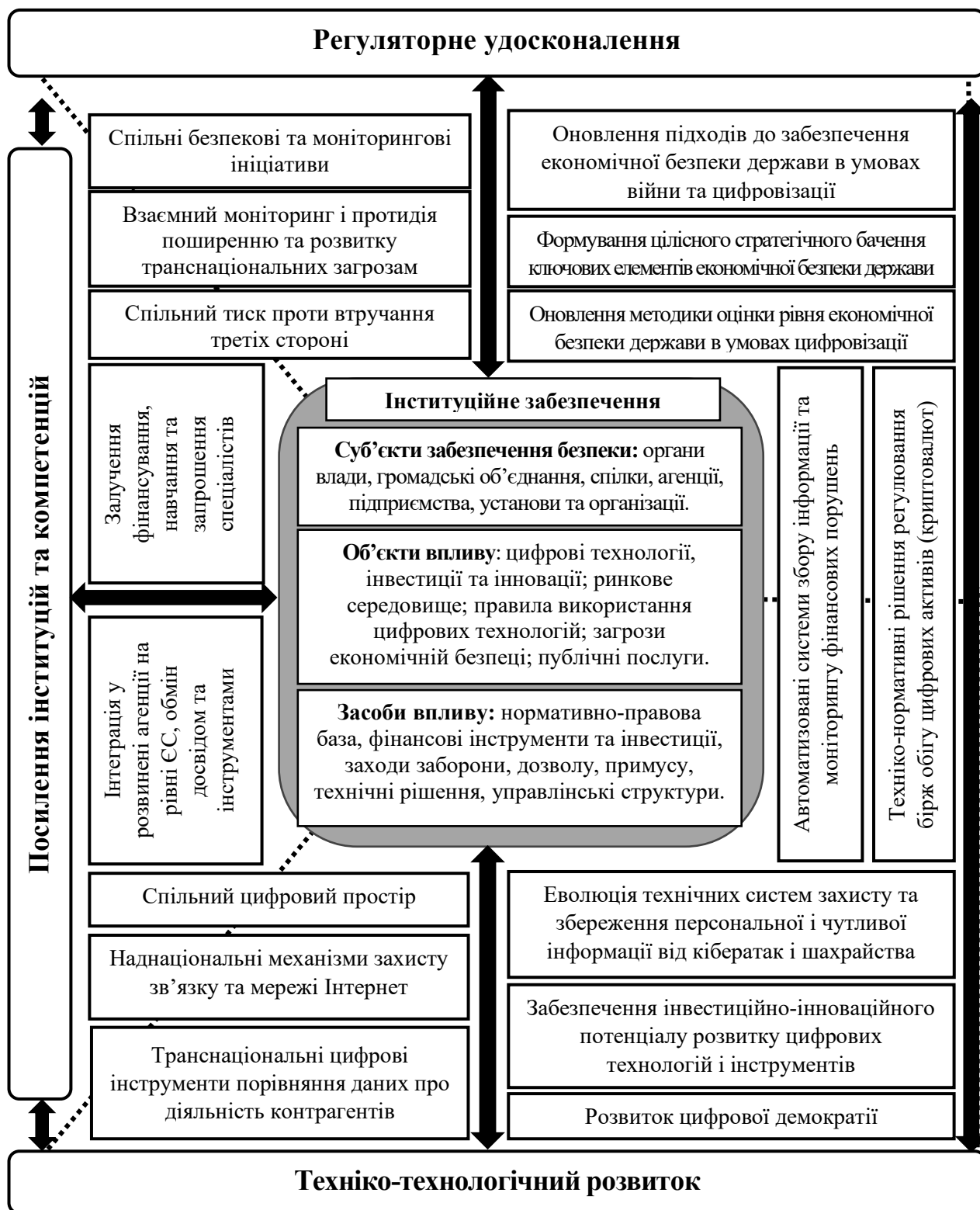


Рис. 3.3. Концептуальні засади розвитку інституційного забезпечення економічної безпеки України в умовах цифровізації на основі досвіду ЄС

Джерело: авторська розробка

Відповідно, запропонована трикомпонентна система розвитку інституційного забезпечення економічної безпеки України передбачає неконфліктне поєднання розвитку цифрових інструментів, гармонізацію законодавчого забезпечення та сприяння євроінтеграції. Зокрема, це представляється можливим, шляхом адаптації положень Загального регламенту захисту даних [176], що передбачає широкий спектр нормативно-правових заходів для захисту цифрових технологій, а також Директиви про заходи для високого спільного рівня кібербезпеки в ЄС [177], яка передбачає кооперацію країн-учасниць для технічного, технологічного та оперативного забезпечення безпеки цифрової інфраструктури.

Важливими, на нашу думку, є заходи із децентралізації повноважень безпекових агенцій з метою уникнення перевантаження та дублювання функцій, розробка безпекових алгоритмів, забезпечення підготовки кадрів до конкретних загроз, а також подальша співпраця із залученням іноземних грантів та інвестицій для модернізації цифрової інфраструктури. Україна має активізувати участь у європейських ініціативах, що сприятиме не лише технічному прогресу, але й інтеграції у загальноєвропейську цифрову екосистему, збільшуватиме позитивний вплив цифровізації на економічну безпеку держави та її поширення на традиційні сектори економіки.

Утім, досягнення стійкого рівня економічної безпеки передбачає не лише структурне оновлення інститутів, а й здійснення прогнозування позитивного та негативного впливу цифровізації, пов'язаного із цифровими викликами як наступний крок у формуванні ефективної та гнучкої системи забезпечення економічної безпеки держави. Такий підхід дає змогу визначити зони зростання та критичні недоліки функціонування національної економіки в умовах цифровізації.

3.2. Моделювання впливу цифровізації на загрози економічній безпеці України

Всеохопна цифровізація національної економіки в умовах турбулентності та невизначеності зовнішнього середовища зумовлює необхідність моделювання її потенційного впливу на формування і трансформацію загроз економічній безпеці держави. Це дасть змогу передбачити тенденції соціально-економічного розвитку, зважаючи на властивість цифровізації генерувати, трансформувати та масштабувати загрози економічній безпеці держави.

Утім, цифровізація є комплексним явищем, що за рахунок своїх властивостей адаптивності, мультиплікативності та масштабування набуває різноманітних форм та проявів у залежності від суб'єктів, об'єктів та предметів, на які вона має вплив. Тому сформулювати модель впливу цифровізації на загрози економічній безпеці України лише макроекономічними показниками є складним завданням та потребує розширеного підходу. Так, запропоновані у підрозділі 2.1 індикатори оцінки інформаційно-цифрової складової економічної безпеки слугують підґрунтям для моделювання впливу цифровізації на загрози економічній безпеці держави через діяльність суб'єктів на макро-, мікро- та нанорівні національної економіки. Варто зауважити, що мезорівень, з огляду на відсутність специфічних механізмів реагування на цифрові загрози, має радше просторовий, а не суб'єктний рівень, що не є визначальним в межах дослідження.

До того ж динамічний характер загроз економічній безпеці держави в умовах цифровізації, таких як ескалація кібератак або розповсюдження шкідливого програмного забезпечення, суттєво ускладнює побудову прогнозних моделей впливу цифровізації на економічну безпеку держави та потребує багатокрокового аналізу, де кожний наступний етап враховує дані, отримані на попередньому. В свою чергу, статичні моделі, які ігнорують часовий чинник,

здатні надавати лише ретроспективні оцінки та не відповідають потребам проактивного реагування.

Так, для ідентифікації та моделювання прямих цифрових загроз економічній безпеці держави використовують такі методи, як Attack surface, STRIDE, P.A.S.T.A, Trike, VAST, MITTRE ATT&CK, що дозволяють виявляти, аналізувати, оцінювати та зменшувати негативний вплив цифрових загроз (віруси, кібератаки, витік даних) у інформаційних системах. Натомість, для оцінювання загроз економічній безпеці в умовах цифровізації доцільно використовувати моделі Мертона, McKinsey&Co та різноманіття моделей типу PF: PF-MEREC-SWARA, PF-GLDS, PF-MEREC-SWARA-GLDS [146] призначені для оцінки ризиків, рівня фінансової стійкості, стратегічного позиціонування та прийняття рішень в умовах невизначеності. Також доцільним є використання інтегральних та регресійних моделей часових рядів.

Зважаючи на складність прогнозування загроз цифровізації доцільним є використання комбінованих моделей, що поєднують оцінювання прямих, опосередкованих та трансформованих загрози економічній безпеці держави в умовах цифровізації, що здебільшого побудовані на експертному методі. Утім, основним недоліком такого підходу є слабкість його математичного апарату. У розрахунку ці моделі зводяться до формули мінімізації суми граничних збитків (3.1). Утім, вони потребують додаткового налаштування, яке має враховувати когнітивні упередження, у тому числі зумовлені впливом цифровізації.

$$LF = \sum_{1-10} \lim_i D_i \rightarrow \min; \quad D_i \geq 0, \quad (3.1)$$

де LF – оцінка втрат від впливу цифрових загрози;

D1, D2,... – підсумкові показники прямих і непрямих збитків від кібератак, порушення цифрової інфраструктури, тощо;

D1 – порушення конфіденційності інформації;

D2 – втрата цінності інформаційного ресурсу через його компрометацію, амортизацію або нерелевантність;

D3 – знищення інформаційного ресурсу при несанкціонованому вторгненні та взаємодії суб'єктів і об'єктів доступу;

D4, D5, D6, D7, D8 – знищення, повна або часткова втрата, порушення різних баз даних, недоступність або недосяжність інформаційного ресурсу на певний період часу;

D9 – несанкціонований збір, обмін, постачання та передача даних, спотворення інформаційних ресурсів;

D10 – виявлення скомпрометованих та випадкових помилок у програмному забезпеченні, непередбачувані помилки [139-140].

Так, першим етапом для формування моделі є дослідження та прогнозування рівня економічної безпеки держави за її складовими, що дає змогу виявити основні сфери концентрації загроз.

Зважаючи, що комплексні явища складно передбачити, доцільно використовувати лінійну регресію там, де це можливо із забезпеченням достатнього рівня апроксимації. Оскільки простота, стійкість до перенавантаження даними та відзначення більш наочного вектору надає перевагу для моделювання загальних тенденцій розвитку економічної безпеки України в умовах цифровізації. Утім, поліноміальна регресія має низку суттєвих переваг, які роблять її корисним інструментом для аналізу складної нелінійної залежності між змінними. Важливим аспектом є можливість варіювання ступеня полінома. Він дозволяє налаштовувати модель для досягнення оптимальної точності. Тобто треба обирати мінімальний поліном (до 3), який дозволить досягти кращої точності за інші моделі, залишаючи адекватні значення прогнозу. Водночас, цей

підхід має практичні обмеження, зокрема ризик перенавчання за високих ступенів полінома, що може знижувати релевантність моделі у нових вибірках даних.

І тому, оскільки вихідні дані мають неоднорідну структуру і залежні від чисельних детермінант дальнього зовнішнього середовища, моделювання складників економічної безпеки шляхом використання лінійної регресії вкрай обмежене. Що приводить до частого використання поліноміальної регресії.

Звертаючись до прогнозу складових рівня економічної безпеки України прийнятні показники детермінації у енергетичної, зовнішньо-економічної, демографічної та інвестиційно-інноваційної складової інтегрального показника економічної безпеки України (рис. 3.4), залежно від попередніх коливань показника.

Тому, виходячи з доступних показників періоду, можна визначити негативний прогноз для енергетичної, демографічної, інвестиційно-інноваційної складових рівня економічної безпеки України, що узгоджується з наявними даними. Утім, варто зауважити, що реальні значення показників можуть бути ще менші. Так, руйнація енергетичного сектору, зменшення експортного потенціалу, трудова міграція, мобілізація, зростання інвестиційних ризиків та зменшення видатків на науку, внаслідок військової агресії росії, свідчать про більш песимістичні очікування.

Вплив цифровізації, зважаючи на її властивості мультиплікативності, адаптивності та мобільності, на наш погляд, лише посилюватиме існуючі загрози. Про це сигналізує залежність цифрової інфраструктури та обігу інформації від стабільного енергопостачання та умови, які призводять до все більшого відтоку інноваційного потенціалу та наукових розробок сектору ІКТ закордон.

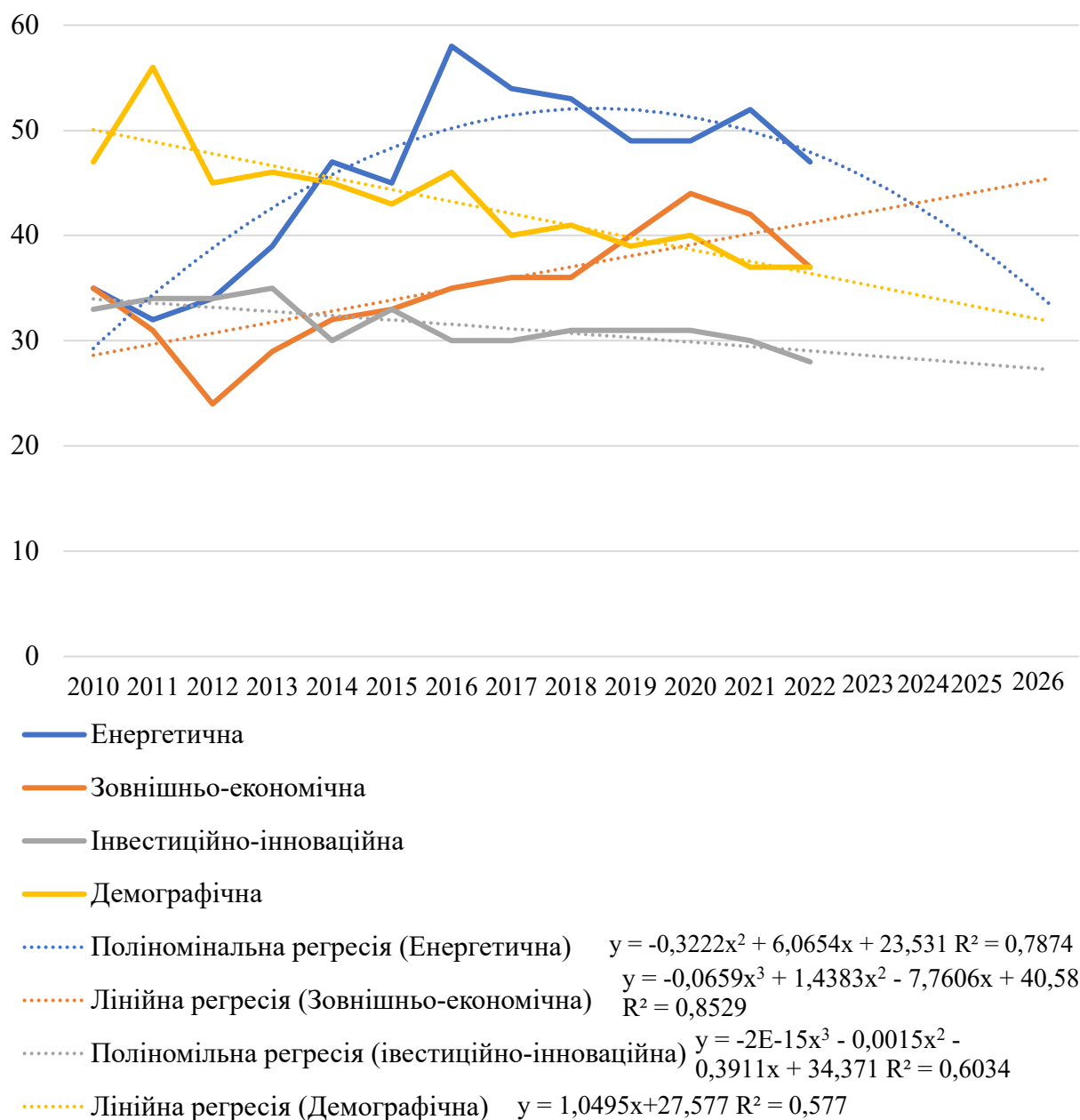


Рис. 3.4. Прогнозування показників енергетичної, зовнішньо-економічної, інвестиційно-інноваційної та демографічної складових економічної безпеки України на 2023-2026 роки

Джерело: складено автором на основі [98-99]

*оцінка інтегрального індексу економічної безпеки України з 2022 року не може бути здійснена через відсутність в органів державної статистики можливості забезпечити збір, аналіз та поширення статистичної інформації в умовах введення в Україні воєнного стану.

Тому, зважаючи на активний відтік ІТ-стартапів, релокацію кваліфікованої робочої сили сектору ІКТ, руйнацію енергоінфраструктури, негативний прогноз впливу цифровізації залишатиметься до реалізації безпекових заходів. Наприклад глибшій інтеграції в енергетичну мережу ЄС та захисту наявної інфраструктури від атак, збільшення експорту, реалізації державної політики захисту інвестицій та кадрового потенціалу економіки. Це передбачає потребу в комплексних системних реформах, які, в свою чергу, є довгостроковими проєктами. Натомість існуюча політика сприяння цифровізації лише покриватиме відтік ресурсів з сектору.

Утім, прогнозуванню показників заважають схильність лінійної та поліноміальної регресії до перенавантаження вихідними даними. Тому для розрахунку релевантного прогнозу виробничої, макроекономічної, продовольчої, соціальної та фінансової складових економічної безпеки України (рис. 3.5) варто зменшити часовий період. Для цього, замість 13 періодів використаємо 7, виключивши 2010-2015 рр., оскільки вони пов'язані з турбулентними економічними змінами внаслідок початку гібридної війни та окупації частини територій України. Так, зменшення часового проміжку дозволить забезпечити кращу апроксимацію, збільшивши показник детермінації від мінімального значення у 0,13 при використанні 13 часових інтервалів до 0,67 при використанні 8.

Трендові моделі виробничої та продовольчої складової економічної безпеки України показують низхідну динаміку до 2026 року і лише соціальна має висхідну. Можна зробити припущення, що негативний вплив цифровізації і далі знаходить своє вираження у структурних диспропорціях сектору традиційного виробництва та асиметрії розвитку національної економіки.

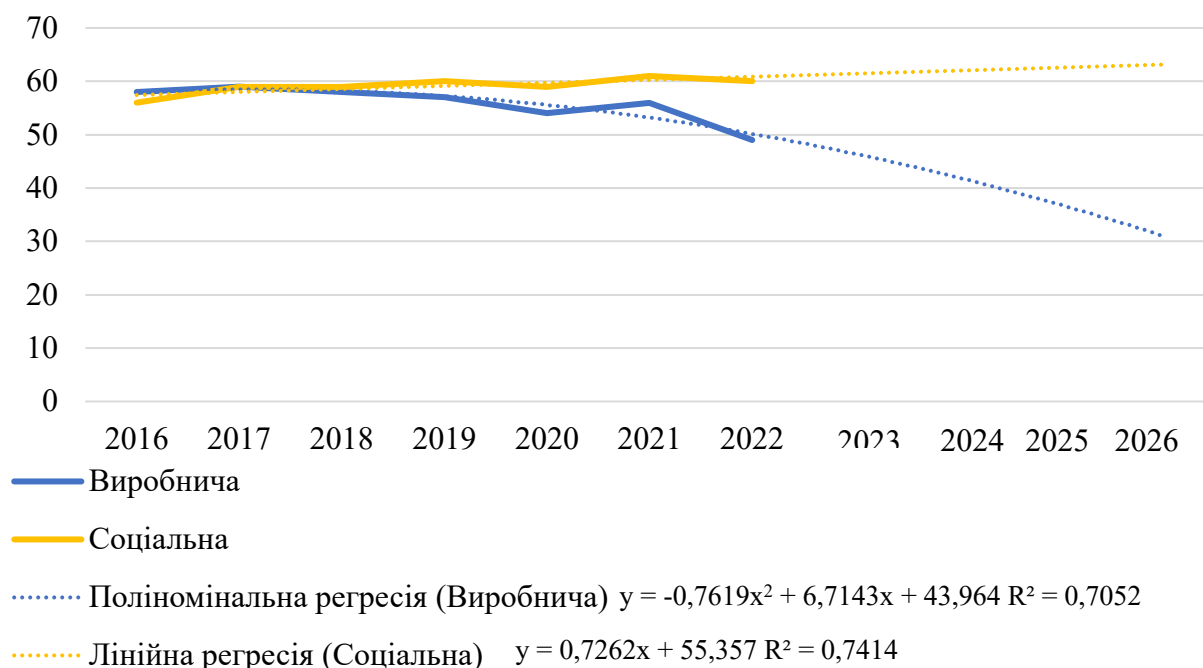


Рис. 3.5. Показники виробничої, продовольчої та соціальної складових рівня економічної безпеки України з трендовим прогнозом на 2023-2026 роки

Джерело: складено автором на основі [98-99]

*оцінка інтегрального індексу економічної безпеки України з 2022 року не може бути здійснена через відсутність в органів державної статистики можливості забезпечити збір, аналіз та поширення статистичної інформації в умовах введення в Україні воєнного стану.

Утім, попри високі показники апроксимації поліноміальної регресії макроекономічної та фінансової складових економічної безпеки держави в межах 0,7-0,9, відсутність стабільної динаміки призводить до викривлення показників. Так, математична логіка, закладена в Методичних рекомендаціях щодо розрахунку рівня економічної безпеки України [30], призводить до гіперболічного вираження, нижчих за граничне значення індикаторів. Тобто динаміка падіння показника буде сповільнюватися при наближенні значень до нуля, а цього не відображають розраховані лінійні та поліноміальні тренди макроекономічної та фінансової складових, тому вони були виключені з графіку.

Отже, три показника складових економічної безпеки України знаходяться в «небезпечному», ще чотири в «незадовільному» і два в «задовільному» рівні.

Варто врахувати, що показник соціальної складової має бути додатково погіршений внаслідок впливу трудової та вимушеної міграції, мобілізації, зменшення рівня соціального захисту вразливих верств населення. Тому, можна зробити припущення про загалом негативний прогноз.

Аналогічно, поліноміальною регресією, можна визначити прогноз інтегрального показника рівня економічної безпеки України на базі 8 часових інтервалів (формула 3.2). Коефіцієнт детермінації прогнозовної моделі складає 0,906, що свідчить про достатню її релевантність.

$$y = -0,3488x^2 + 3,1798x + 41,861, \quad (3.2)$$

де y – інтегральна оцінка рівня економічної безпеки України;

x – кількість часових інтервалів від 2022 року.

Здійснивши розрахунок за формулою 3.2, можна визначити стійкий прогноз до зменшення інтегральної оцінки рівня економічної безпеки України протягом 2023-2026 рр. (рис. 3.6).

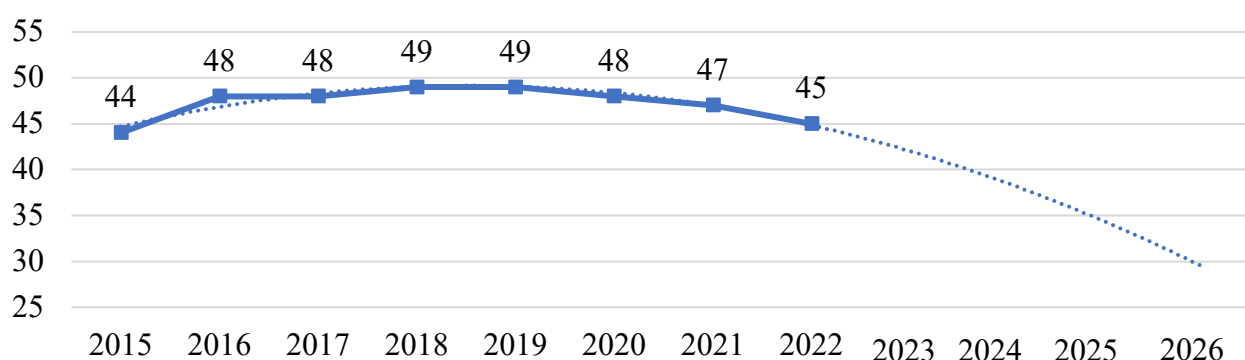


Рис. 3.6. Прогноз інтегральної оцінки рівня економічної безпеки України на 2023-2026 роки

Джерело: складено автором на основні [98-99]

Утім, здійснене прогнозування не враховує впливу цифровізації на загрози економічній безпеці держави через виявлені критичні недоліки національної методики оцінювання її рівня. Зокрема, за результатами оцінювання сучасних тенденцій цифровізації, у моделі впливу цифровізації на загрози економічній безпеці держави варто відобразити посилення явищ трудової міграції, перенесення представництв та потужностей сектору ІКТ, структурні деформації у економіці, зростання вразливості цифрової інфраструктури, цифровізації тіньової економіки тощо.

Далі, переходячи до моделювання впливу цифровізації на забезпечення економічної безпеки держави через діяльність суб'єктів мікрорівня, доцільно використати результати проведеного у підрозділі 2.3 кореляційного аналізу між ключовими показниками енергетичної, виробничої та інформаційно-цифрової складової економічної безпеки. Він дозволить спрогнозувати зростання частки сектору ІКТ у ВВП, оскільки цей процес супроводжується не лише збільшенням економічної залежності від енергетичної інфраструктури, а й перерозподілом обмежених фінансових та ресурсних потоків на користь сектору ІКТ без створення системних мультиплікативних ефектів для економіки загалом.

Так, з огляду на те, що обсяги споживання електроенергії є індикатором економічної активності сектору традиційного виробництва, то аналіз залежності між цими показниками дозволить виявити опосередкований негативний вплив цифровізації.

У цьому контексті варто врахувати втрати в енергетичній інфраструктурі та генерації електроенергії за 2023-2024 роки, а також застосувати сценарного прогнозування на 2025-2026 роки (табл. 3.5) у випадку зростання чи зменшення генерації електроенергії. Очікуване зростання споживання електроенергії до 55 та 80 млрд кВт/год у 2025 та 2026 роках відповідно пов'язано з оптимістичними очікуваннями зростання ВПП, відновлення енергетичної інфраструктури та її захисту від ракетних атак. Сценарій зменшення передбачає скорочення

споживання унаслідок зменшення пропозиції до обмежень генерації електроенергії атомних станцій України, у випадку загострення безпекової ситуації та остаточне знищення залишок енергетичної інфраструктури.

Такий підхід, на нашу думку, є необхідними для побудови прогнозу рівня економічної безпеки на 2025-2026 роки, що дозволить змодельовати опосередкований вплив цифровізації та воєнних дій на загрози одразу для енергетичної, виробничої та інформаційно-цифрової складової економічної безпеки України через діяльність суб'єктів мікрорівня.

Таблиця 3.5

Сценарний прогноз впливу показника споживання електроенергії на розмір середньої частки ІКТ сектору у ВВП на 2025-2026 роки

Показник	2025	2025	2026	2026
Очікування	зростання	зменшення	зростання	зменшення
Споживання електроенергії, млрд кВт/год	55	50	80	45
Ймовірна частка ІКТ сектору у структурі ВВП, %	7,2	7,5	5,6	8,7

Джерело: побудовано автором на основі [142-145]

Здійснений прогноз свідчить про збереження тенденції до поглиблення структурних змін. Так, звертаючись до тенденції виявленої у підрозділі 2.3, зростання частки ІКТ сектору в структурі національного ВВП до 5,6-8,7% у подальшому може призвести до низки загроз економічній безпеці України. Зокрема, варто очікування продовження та посилення вже виявлених тенденцій занепаду сектору традиційного виробництва, відтоку кваліфікованої робочої сили з традиційних секторів та зростання кількості вразливої цифрової інфраструктури, цифрових каналів обігу нелегальних активів.

Тобто, це свідчить про те, що ефективне регулювання негативного впливу цифровізації в системі забезпечення економічної безпеки України потребує не лише стимулювання розвитку цифрових технологій, рішень та послуг, але й

інституційно-правового забезпечення протекціоністських заходів для сектору традиційного виробництва, зокрема з метою запобігання загрозам зменшення наукомістких галузей та збереження виробничого потенціалу.

Продовжуючи, прогнозування розвитку впливу цифровізації на економічну безпеку держави через діяльність суб'єктів мікрорівня може бути розроблено за допомогою трендового аналізу лінійної регресії часових рядів. Для прогнозу на 2025-2026 роки доцільно використати показники, які відображають стан електронної комерції та готовності середовища за 2021-2024 роки (табл. 3.6). Обраний перелік значень слугують вихідними даними для розрахунку рівня інформаційно-цифрової складової економічної безпеки України, сформованому в підрозділі 2.1, і тому відображатимуть майбутній розвиток тенденцій.

Тобто аналіз лінійної регресії (додаток Д) дозволяє передбачити загальні тенденції подальшого розвитку цифровізації економіки. Таких, як збільшення доступу до мережі Інтернет, швидкісного зв'язку, впровадження цифрових технологій, зростання цифрової комерції та участі населення у ній.

Таблиця 3.6

Прогнозування вихідних даних для розрахунку індикаторів інформаційно-цифрової складової економічної безпеки України на 2025-2026 роки

Показник/Рік	2021	2022	2023	2024	2025	2026
Проникнення інтернету в домогосподарствах, %	80	85	94	94	100	100
Онлайн-продажі, млрд грн	129	151	182	239	265,5	301,6
Інтернет-покупці, млн	11	8,5	9,9	11	12,3	13,5
Кількість кібератак	415	684	1536	1999	2560	3120

Джерело: побудовано автором на основі [147-150]

Відображене у таблиці тимчасове падіння кількості інтернет-покупців було викликано об'єктивними обставинами, а прогноз на 2025-2026 роки вже свідчить про відновлення та подальше зростання сектору цифрової комерції. Також можна констатувати повернення до показників обсягу продажів 2021 року. Проте

показники 2020 року у обсязі 2655 млн дол. США будуть досяжні лише у 2025-2026 роках, досягши значення 2655-2677 млн дол. США [130].

Здійснений розрахунок свідчить про загрозу зростання числа кібератак на 203% за період та на 751% від початку спостережень. Це співпадає з існуючою загрозливою тенденцією зростання долі світової кіберзлочинності та загальносвітових втрат від таких інцидентів з 5,99 трлн дол. США у 2021 році до 8,15 трлн дол. США у 2024, та передбаченням зростання до 11,39 трлн дол. США у 2026 році [151]. Така тенденція складає особливу небезпеку для суб'єктів на нанорівні, оскільки збільшує навантаження та вимоги до потенційно найбільш вразливої ланки системи економічної безпеки.

Здійснений розрахунок також свідчить про загрозу зростання числа кібератак на 203% за період та на 751% від початку спостережень. Це співпадає з існуючою загрозливою тенденцією зростання долі світової кіберзлочинності та загальносвітових втрат від таких інцидентів з 5,99 трлн дол. США у 2021 році до 8,15 трлн дол. США у 2024 і аж до 11,39 трлн дол. США у 2026 [151]. Така тенденція складає особливу небезпеку для суб'єктів на нанорівні, оскільки збільшує навантаження та вимоги до потенційно найбільш вразливої ланки системи економічної безпеки.

Підсумовуючи, прогноз свідчить про подальше загострення реальних та реалізацію потенційних загроз, зумовлених поширенням мережі Інтернет, сегменту цифрових послуг і товарів, зростанням числа кібератак, а також фінансової вигоди для бенефіціарів ризикової діяльності. Тому існує об'єктивна потреба протидії загрозам економічної безпеки України через забезпечення захисту суб'єктів мікрорівня.

Так, модель впливу цифровізації на загрози економічній безпеці через діяльність суб'єктів мікрорівня має передбачати, як зростанням ринкових можливостей, так і витрати на захист цифрової інфраструктури, навантаження на кадри малих та середніх підприємств та переліком прогнозованих вище загроз.

Напрям потенційного розвитку залежить від комплексних інституційних, регуляторних та інтеграційних заходів, які полягають у забезпеченні ринку праці фахівцями з ІКТ-кваліфікацією, удосконаленні захисту персональних даних, зменшенні ролі людської помилки.

Тому, варто відзначити, що ці напрями забезпечення економічної безпеки матимуть вплив саме на суб'єктів нанорівня. Так, від рівня фінансової та цифрової грамотності населення залежить захищеність інформації, ефективність протидії фішингу та кібершахрайству, недопущення втручання у корпоративні мережі та витоку інсайдерської інформації. Отже, навички населення одночасно сприяють попиту на цифрові товари та формуванню вимог до забезпечення інформаційно-цифрової складової економічної безпеки до держави.

Зважаючи на те, що цифрова грамотність формує готовність середовища до цифрових інновацій, ресурсний потенціал економіки знань, попит для підприємств цифрової комерції та є джерелом персональних даних, доцільним є дослідження впливу цифровізації на загрози економічній безпеці держави через діяльність суб'єктів нанорівня національної економіки шляхом визначення рівня цифрової грамотності, як фактор цифровізації у моделі впливу цифровізації на загрози економічній безпеці держави.

Для цього доцільно використати опитування для збору соціологічної інформації. Обрана методика дослідження передбачає, що опитування проводилося серед громадян України різних вікових груп, які проживають на території всіх областей України, а також за кордоном. Обсяг вибіркової сукупності становив 325 респондентів. Генеральна сукупність охоплює все населення України і оцінюється приблизно в 32 млн осіб на території та близько 41 млн загалом.

Власне, метод опитування: безособове онлайн-анкетування закритої форми із застосуванням сервісу «Google Forms» та можливістю пропускати питання при

відсутності відповіді (додаток Е). Анкета була поширена шляхом публікації онлайн, у соціальних мережах та розсилкою респондентам.

Наступним етапом є розрахунок помилки репрезентативності дослідження, що відображає достовірність результатів. У соціологічних дослідженнях прийнято виходити з довірчої імовірності 0,95, що можна інтерпретувати як 95% впевненість у результатах та відхилення показника не більше ніж на 5%. Тому, для розрахунку, скористаємося стандартною формулою (3.3).

$$E = z \times SE = z \times \sqrt{\frac{p(1-p)}{n}}, \quad (3.3)$$

де E – похибка вибірки;

SE – стандартна похибка;

n – розмір вибірки;

p – розрахункова частота;

z – статистичний критерій при нульовій гіпотезі.

Оскільки розрахункова частота складає 0,5, а розмір вибірки 325 осіб, то SE складатиме 0,0277, а оскільки вибірка набагато менше за генеральну сукупність, то «корекція популяції» (FPC) не застосовується. Тому, якщо z -критерій при 95% рівні впевненості складає 1,96 [257], тоді похибка вибірки становить 5,43%, що є прийнятним результатом для завдання нашого дослідження.

Що стосується демографічних особливостей вибірки, то в опитуванні взяло участь 184 жінки (56,5%) та 138 чоловіків (42,5%), 3 особи не вказали стать (1%). Відхилення від даних UNCTAD про гендерний розподілення населення України в межах 5%, а саме 54% жінок та 46% чоловіків [132]. У віковій структурі вибірки

респонденти до 16 років складають 7,4%, 16-35 років 52,3%, 36-60 років 28%, а понад 60 років – 12,3%.

Використовуючи методику аналогічного дослідження цифрових навичок «Дія.Сіті» [229], здійснимо розподіл респондентів за шістьма макрорегіонами: центральний 61,8%, північний 11%, східний 7,4%, південний 5,2%, західний 5%, та ті що перебувають не в Україні 9,6%. Відхилення вибірки на користь центрального регіону викликано особливостями опитування, оскільки 198 респондентів зазначили, що вони знаходяться в Полтавській області. А тому результати не в повній мірі відображають саме регіональні особливості.

У відповідях на наступні питання більшість респондентів мали вищу освіту, а саме 245 осіб (75,4%), з них 10,2% зазначили, що мають науковий ступінь. Близько 8% кожної з групи респондентів відзначили професійно-технічну, середню освіту або є школярами. Свій достаток абсолютна більшість респондентів (69,8%) оцінила як середній, 24,3% як низький і лише 5,8% як високий. Самооцінка цифрових навичок відображена на рис. 3.7.

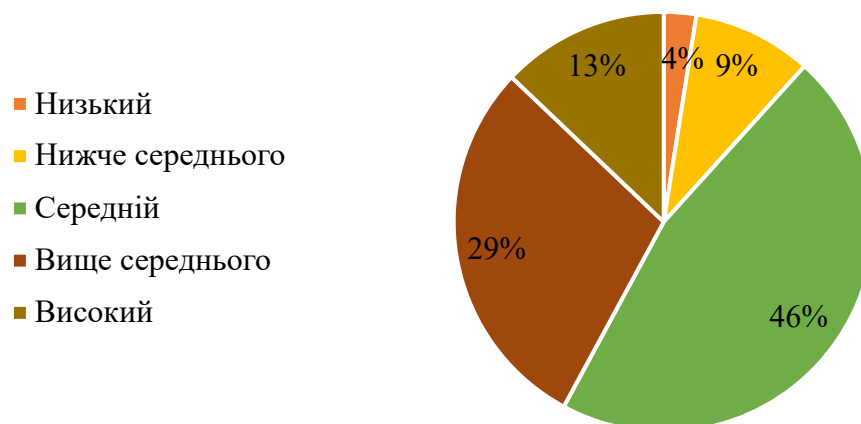


Рис. 3.7. Розподіл самооцінки респондентами своїх цифрових навичок

Джерело: побудовано автором за результатами опитування

Такий розподіл відповідає тенденціям підвищення цифрової грамотності населення: за даними на 2023 рік 59,6% українців мали принаймні базовий рівень

цифрових компетенцій [229]. А значить, можна вважати, що проведене дослідження є репрезентативним, відповідає та доповнює попередні дані.

У нашому дослідженні більшість опитаних зазначили, що активно використовують мережу Інтернет та цифрові технології, рішення та послуги у повсякденному житті. З них понад 80% повідомили, що за останні 3 місяці користувалися миттєвими повідомленнями та здійснювали інтернет-дзвінки, 75-80% – переглядали відео та фільми онлайн, перебували в соціальних мережах та користувались електронною поштою. Рівень онлайн-комунікації та використання цифрових мультимедіа, на наш погляд, свідчить про високу готовність громадян до цифрових технологій, що означає високу сприйнятливність до цифровізації та наявність попиту на цифрові послуги і товари.

У загальному вигляді використання цифрових технологій, рішень та послуг респондентами протягом 3 минулих місяців відображено на рис. 3.8.

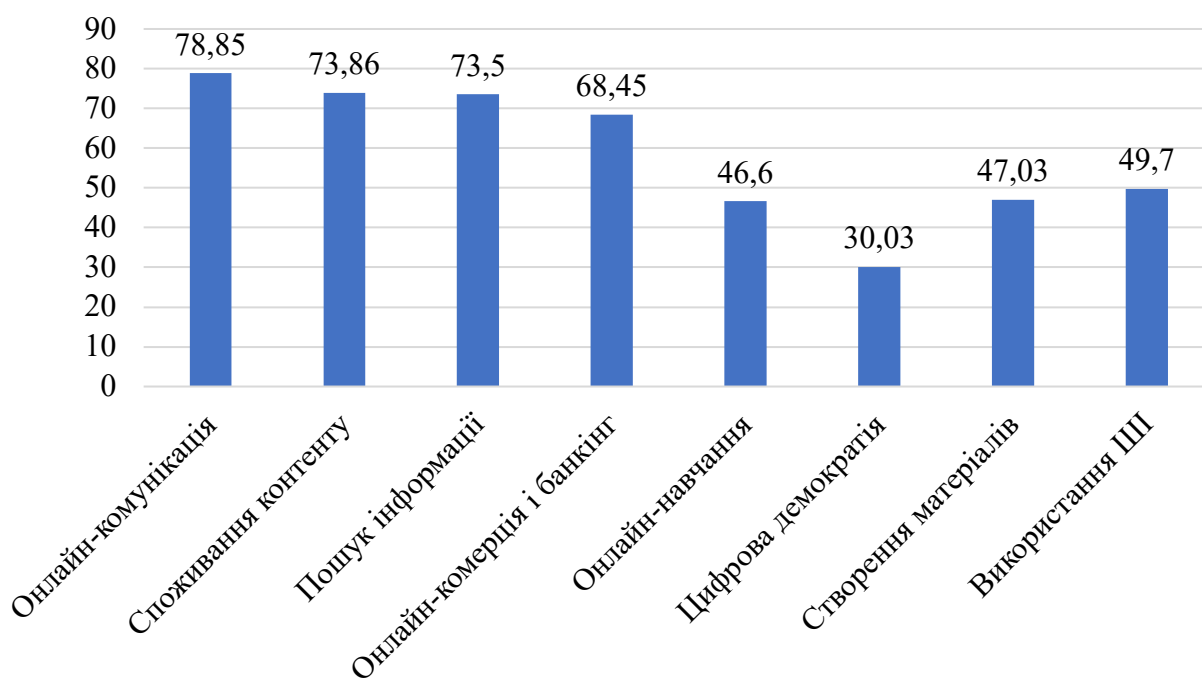


Рис. 3.8. Основні напрями використання цифрових технологій, рішень та послуг респондентами

Джерело: побудовано автором за результатами опитування

Вивчаючи анкети респондентів, у питанні залученості населення до цифрової комерції близько 75% респондентів зазначили, що регулярно здійснювали онлайн-покупки (щотижня або кілька разів на місяць). Це відповідає з прогнозованим вище напрямком зростання комерції у найближчі роки. Виходячи з цього, також підтверджує припущення про готовність середовища до цифрових технологій. А також означає наявність стійкої традиції оплати товарів та послуг через мережу Інтернет. Тому, з погляду безпекології, варто очікувати зростання обсягів вразливої інфраструктури та зростання привабливості для шахрайства, кібератак зі збільшенням потенційної вигоди.

Натомість громадяни проявляють обережність усвідомлюючи про негативний вплив цифровізації та її прямих загроз. Про це також свідчить особистий досвід респондентів у відповіді на питання про загрози, з якими вони стикалися в мережі Інтернет та при використанні цифрових технологій (рис. 3.8).



Рис. 3.9. Основні загрози з якими особисто стикалися респонденти в мережі Інтернет та при використанні цифрових технологій

Джерело: побудовано автором за результатами опитування

До найбільш поширених загроз з якими зустрічалися респонденти належать: неправдиві новини (224 відповіді), фішинг (222), збої чи несправність сайтів (146), інтернет-шахрайство (129), викрадення акаунтів (101), віруси (96). Ці дані демонструють, що більшість респондентів стикалися з прямими інформаційно-цифровими загрозами (фейки, фішинг) і опосередкованими технічними проблемами безпеки. Такі показники підтверджують результати дослідження про загалом незадовільний стан інформаційно-цифрової складової економічної безпеки України.

Найбільшого занепокоєння при використанні цифрових інструментів та мережі Інтернет (рис. 3.10), серед респондентів викликає безпека особистих даних і фінансів.



Рис. 3.10. Частка відповідей респондентів про занепокоєння при використанні цифрових інструментів та мережі Інтернет

Джерело: побудовано автором за результатами опитування

Найбільше респондентів турбує безпека персональних даних (82%) та банківських рахунків (80%), безпека паролів (69%) і безпека особистих файлів (54%). Такі показники відповідають на зростаючу загрозу кібератак, витоку даних, шахрайства та фішингу, і вказують на високу чутливість суб'єктів діяльності на нанорівні національної економіки до динамічних змін середовища.

Досліджуючи анкети, можемо засвідчити, що багато людей занепокоєні поширенням вірусів, шахрайства та шантажу в мережі Інтернет загалом (52%), та у онлайн-магазинах зокрема (44%), неправдивих новин (49%), а також збором персональних даних третіми сторонами (45%). Це свідчить про певний рівень унормування цифрової комерції, цифрової демократії та цифрових медіа у сучасному житті, що тепер викликають менше занепокоєння, а користувачі розуміють потенційні загрози дезінформації, махінацій та маніпуляцій.

Менше опитаних хвилюється щодо кібербулінгу, чутливого контенту або переслідування (11%). Таким чином, на мікрорівні, основним занепокоєнням, за даними самооцінки, є загрози персональним даним, особистим фінансами та дезінформації. Додатково варто звернути увагу і на сприятливу тенденцію, оскільки понад 50% респондентів хоча б раз відмовлялися від замовлення товарів чи використання громадського Wi-Fi з міркувань безпеки.

Переходячи до вікових відмінностей впливу цифрової трансформації варто відмітити, що молодші вікові групи значно частіше повідомляють про досвід цифрових загроз та занепокоєння, ніж старші люди. Наприклад, серед опитаних віком 16–35 років середнє число обраних загроз у 13 питанні перевищує 5 на людину, тоді як для людей 46 років воно менше 3. Середня кількість занепокоєнь у 14 питанні теж знижується з віком від приблизно 12 у респондентів до 35 років аж до 6 у респондентів вікової групи старше 60 років. Рівень академічної освіти слабо корелює з оцінкою цифрових ризиків: усі освітні групи вказують приблизно однакову кількість занепокоєнь (9-10 пунктів), школярі дещо менше фіксують загрози, а особи з вищою освітою зазначають на 1-2 більше.

Натомість самооцінка цифрової грамотності корелює із занепокоєннями, оскільки ті, хто оцінює навички як «високі», зазначають у два рази більше загроз з якими зустрічалися та занепокоєння, порівняно з «низьким» рівнем. Це дозволяє зробити припущення, що просунуті користувачі цифрових технологій краще ідентифікують та розуміють загрози, а значить можуть мінімізувати їх негативний вплив. І тому наряду стимулювання розвитку цифрової грамотності є надзвичайно важливим, як неформальне інституційне забезпечення для запобігання загрозам економічній безпеці.

Підсумовуючи, можна значити, що на рівні діяльності суб'єктів нанорівня національної економіки найбільш актуальними є питання загрози персональним даним та особистим фінансам і це узгоджується з глобальними трендами, що лідирують серед найпоширеніших кіберзагроз для населення [110; 136]. А отже, чутливість середовища до інформації та цифрових технологій формуватиме специфічний попит на мінімізацію негативного впливу цифровізації. І вже на державному рівні цей попит має бути трансформований у пріоритетні напрями запобігання загрозам економічній безпеці держави.

І тому, виходячи з результатів дослідження, можна стверджувати, що при належній увазі до кібербезпеки та освіти громадян цифровізація може бути збалансованою. З одного боку суб'єкти діяльності на нанорівні будуть обізнані щодо ризиків, а з іншого використовуватимуть можливості цифрових технологій, створюватимуть попит і нові ринки, заповнюватимуть потребу в кадрах на ринку.

Так, за результатами проведеного дослідження, можна сформулювати модель впливу цифровізації на економічну безпеку держави із врахуванням показників діяльності суб'єктів на макро-, мікро- та нанорівні національної економіки $R_E = \{M, \mu, n\}$ та визначених критичних точок деструктивних процесів, а саме зростання кількості кібератак, формування структурних дисбалансів між секторами економіки, загострення конкуренції за кваліфіковані кадри (3.4).

$$M_{\text{ВЦБ}} = S_{\text{ВЗ}} \left((A \cap SD \cap C) \leftrightarrow \bigcup_{i=1}^9 P_i \right) \cap f: D_{\text{ц}} \left(\bigcup_{r \in R_E} E_r \right), \quad (3.4)$$

де $M_{\text{ВЦБ}}$ – модель впливу цифровізації на економічну безпеку держави;

$S_{\text{ВЗ}}$ – сфери виникнення загроз економічній безпеці держави

A – кількість кібератак;

SD – структурні дисбаланси між секторами національної економіки;

C – конкуренція за кваліфіковані кадри;

P_i – складові економічної безпеки держави;

$D_{\text{ц}}$ – фактори цифровізації (технології, інституції, цифрова грамотність);

E – національна економіка;

R – рівень національної економіки (макро-, мікро-, нано-).

Таким чином, сформована модель відображає адаптивну динаміку впливу цифровізації на загрози економічній безпеці за рахунок врахування показників діяльності суб'єктів на макро-, мікро- та нанорівні національної економіки та є передумовою мінімізації негативного впливу цифровізації на загрози економічній безпеці України, зважаючи на можливість визначення критичних точок. Відповідно, мінімізація негативного впливу цифровізації на загрози економічній безпеці України потребує розвитку інституційного забезпечення економічної безпеки держави, посилення кадрового потенціалу, розробки та впровадження цифрових технологій, формування цифрової компетентності.

Водночас, виникає потреба в пріоритизації напрямів запобігання загрозам економічній безпеці держави, які передбачають, внесені до моделі впливу цифровізації на економічну безпеку держави, фактори цифровізації та критичні точки її деструктивних процесів, з метою оптимізації взаємодії між компонентами системи економічної безпеки держави.

3.3. Пріоритетні напрями запобігання загрозам економічній безпеці держави

Забезпечення економічної безпеки держави реалізується в умовах дуального впливу цифровізації на неї: з одного боку, цифрові технології сприяють економічному зростанню, технологічному та інституційному прогресу, а з іншого відбувається поширення кіберзлочинності й зростання вразливості цифрової інфраструктури. Це актуалізує потребу в пріоритизації державної економічної політики на засадах безпекорієнтованості.

У цьому контексті виникає об'єктивна необхідність обґрунтування пріоритетних напрямів запобігання загрозам економічній безпеці держави в умовах цифровізації. Для цього доцільно використовувати основні методи пріоритизації, як от експертні, математичні та логічні моделі, методи кількісної оцінки завдань, ресурсів та сфер дій з урахуванням їх важливості, певних обмежень та необхідності протидії загрозам, зумовлених цифровізацією.

Попередньо обґрунтовано, що для України цінною є максимальна адаптація міжнародного досвіду, врахування регіональних пріоритетів, а також імплементація принципів транснаціональної економічної безпеки в умовах цифровізації, сформованих та оформлених регуляторними актами ЄС (табл. Ж.1, Додаток Ж). Необхідно також враховувати, що в умовах ринкової економіки надмірно жорстке державне регулювання процесів цифровізації може викликати побічні ефекти: відтік капіталу, зниження інноваційного потенціалу, обмеження свободи підприємництва, зниження конкурентоспроможності національної економіки тощо. Тому, на нашу думку, одним із основних стратегічних орієнтирів державної політики в умовах сьогодення є створення збалансованої системи регулювання процесів цифровізації, що ґрунтується на стимулюванні цифрового розвитку національної економіки з одночасним забезпеченням економічної безпеки держави.

Зважаючи на європейський досвід керівні аспекти запобігання загрозам економічній безпеці України мають базуватися на забезпеченні конкурентоспроможності національної економіки, зменшенні зовнішніх негативних впливів та міжнародній співпраці (табл. 3.7).

Таблиця 3.7

Пріоритетні напрями запобігання загрозам економічній безпеці України в умовах євроінтеграції

Пріоритет 1	Механізм досягнення 2	Результат 3
Конкурентоспроможність національної економіки	Використання інвестицій, прогресивного зеленого переходу, досягнень передових наукоємних галузей та диверсифікація ланцюгів постачань, що дозволяє одночасно підвищувати технологічну незалежність і економічну стійкість ЄС.	Запобігання загрозам переривання ланцюгів постачання стратегічних ресурсів, залежності від технологій та ресурсів третіх держав, відсталості та вразливості у виробництві ключових технологій. Забезпечення зростання якості життя, зменшення соціальної нерівності.
Зменшення негативного зовнішнього впливу	Моніторинг та перевірка іноземних інвестицій, боротьба з економічним примусом, контроль над критичними технологіями. Захист всіх ланок кіберінфраструктури: від енергетичної сфери до фізичних точок доступу в мережу. Реалізація інструментів для оцінки та мінімізації вразливостей, що сприяє інтеграції безпеки у торгівлю та виробничі ланцюги.	Запобігання впливу цифровізації на загрози економічній безпеці держави, а саме: економічному примусу, технологічному шпигунству, витоку технологій, кібератакам на критичну інформаційну, цифрову та енергетичну інфраструктуру.
Сприяння міжнародній співпраці	Взаємодія з країнами-однодумцями для створення стійких ланцюгів постачання, укладення угод про вільну торгівлю тощо. Реалізація спільних дій проти втручання третіх сторін, розбудова геополітичних союзів, модернізація та розбудова цифрової інфраструктури, ліквідація «сірих зон».	Запобігання загрозам фрагментації торгової системи, деструктивного протекціонізму, виключення та занепаду окремих секторів економіки, що покладають на вільну торгівлю, технологічній ізоляції, поширенню транскордонної злочинності та недобросовісних практик, виведенню доходів, поширенню нелегального контенту, сповільненню економічного розвитку.

Джерело: систематизовано автором на основі [162-167; 176-177]

Слід зауважити, що довоєнні пріоритети забезпечення економічної безпеки України (табл. Ж.2, додаток Ж) мають бути переглянуті з урахуванням сучасних тенденцій цифровізації та відповідності європейським стандартам економічної й інформаційної безпеки.

На жаль, досвід України у нормативно-правовому забезпеченні запобігання загрозам економічній безпеці держави стосується здебільшого концептуальних засад, характеризується обмеженим фінансуванням, нестачею кваліфікованих кадрів та неефективністю механізмів забезпечення економічної безпеки.

Отже, основними пріоритетами забезпечення економічної безпеки України в умовах зростаючого впливу цифрових ризиків і загроз мають стати: формування стійкості національної економіки до загроз, зменшення залежності від зовнішніх ресурсів, диверсифікація поставок та розвиток внутрішнього ринку; фінансовий моніторинг як інструмент запобігання ризикам та боротьби з легалізацією відмивання коштів; розвиток інститутів та агенцій, які виконують координаційні, аналітичні та регуляторні функції; захист критичних технологій і підтримка інноваційного середовища; орієнтація на стратегічних міжнародних партнерів, що закріплюється в політиці європейської інтеграції. Ці пріоритетні напрями мають підкріплюватися розгалуженою нормативно-правовою базою, яка охоплює не лише національні стратегії, а й міжнародні зобов'язання, зокрема в сфері енергетики, інновацій, кібербезпеки, фінансів, боротьби з тінізацією економіки.

Звертаючись до попередніх наукових та аналітичних досліджень (табл. Ж.3, додаток Ж), що були направлені на досягнення макроекономічної стабільності, економічного зростання, розвитку інновацій, погоджуємося з думкою О. Володимир [178], С. Веретюка та В. Пілінського [179] щодо визначення загальних пріоритетних напрямів запобігання загрозам економічній безпеки України. Серед них варто виділити структурну перебудову економіки,

розвиток інноваційної діяльності, забезпечення макроекономічної стабільності та посилення міжнародної інтеграції.

Що стосується питання пріоритетних напрямів використання цифровізації задля запобігання загрозам економічної безпеки України, слід відмітити думку К. Шиманської та В. Бондарчук [180], які виокремлюють ряд заходів, направлених на мінімізацію негативного впливу загроз цифровізації шляхом створення та підготовки сприятливого середовища для цифрових технологій, рішень та послуг. Утім, на наш погляд, сприяння розвитку інформаційного середовища не є достатньою передумовою для забезпечення економічної безпеки України в умовах цифровізації, адже воно може бути використане бенефіціарами ризикової поведінки. Зокрема, актуальним прикладом є воєнні дії, що виступають зовнішньою та внутрішньою детермінантою негативного впливу та породжують цілу низку деструктивних явищ. До них належить, як фізичне знищення виробничих потужностей, цифрової та енергетичної інфраструктури, так і втрата людських ресурсів, територій, руйнування ланцюгів постачання. Подібний рівень екзистенційних загроз економічній безпеці держави формує нові пріоритети й висуває на перший план потреби виживання.

У цьому контексті варто звернути увагу на звіт Міністерства фінансів України та Міністерства економіки України про пріоритети економічної політики, спрямованої на забезпечення економічного зростання [182]. Так, у звіті, спираючись на матрицю реформ, умови позики МВФ та Світового Банку, плани фінансової підтримки від ЄС та програми кредитування України, визначено ряд пріоритетних напрямів запобігання загрозам, а саме забезпечення макроекономічної стабільності, усунення першочергових бар'єрів для зростання, посилення потенціалу економічного зростання. Сукупність цих напрямів має сприяти підвищенню стійкості економіки України, її адаптації до детермінант дальнього зовнішнього середовища та розширенню можливостей економічного розвитку в умовах цифровізації.

Згідно з висновками, викладеними у звіті «Економічні пріоритети повоєнної України» [181] аналітичних центрів CASE та CASE Україна можна визначити низку довгострокових пріоритетів забезпечення економічної безпеки України. Вони включають: реформу інституцій, верховенство права, боротьбу з корупцією, децентралізацію, гармонізацію ролі держави, кадрову конкуренцію в управлінні, макроекономічну стабільність, лібералізацію та приватизацію ринків, завершення земельної реформи, скорочення бюджетних витрат, розвиток людського капіталу та інтеграцію освіти, науки й виробництва. Такий комплексний підхід має сформувавши основу для макроекономічного розвитку, зростання конкурентоспроможності та зміцнення економічної безпеки в довгостроковій перспективі.

Потрібно відмітити, що спираючись на аналіз наукового доробку та нормативно-правового забезпечення, очевидною стає необхідність формування системи пріоритетів, яка одночасно враховуватиме як особливості економічного розвитку України, так і вплив цифровізації. Варто підкреслити, що пріоритети забезпечення економічної безпеки України, які визначені на національному рівні у відповідних стратегічних документах, недостатньо повно висвітлюють вплив цифровізації, що суттєво звужує можливості реагування на сучасні загрози. А отже існує потреба у використанні методів пріоритизації, що дозволить визначити першочергові напрями запобігання загрозам економічній безпеці України в умовах цифровізації для оптимального розподілу ресурсів та зусиль.

Одним з базових підходів пріоритизації є метод RICE [259], за допомогою якого можна оцінювати зони докладання зусиль, фокусуватися на ключових напрямках і ефективно використовувати ресурси (формула 3.5).

$$RICE = \frac{(Reach \times Impact \times Confidence)}{Effort} Effort, \quad (3.5)$$

де RICE – оцінка пріоритетності;

Reach – охоплення змінами цільової аудиторії;

Impact – рівень впливу від рішення, від 0,25 до 2;

Confidence – рівень довіри припущенням, від 0,25 до 1;

Effort – час на впровадження змін, відповідно до процесів, від 0,25 до 2.

Загалом, метод RICE був розроблений у межах управління продуктовими стратегіями та впровадження цифрових інновацій у приватному секторі. Утім, його структурна універсальність та логічна прозорість забезпечують можливість ефективної адаптації до задач дослідження, зокрема у сфері формування та реалізації державної політики економічної безпеки в умовах цифровізації.

Обрання методу RICE як аналітичного інструменту пріоритизації напрямів запобігання та мінімізації загроз економічній безпеці держави є доцільним як з методичної, так і з практичної точки зору. Для цього варто скористатися пріоритетами та завданнями, виокремленими в нормативно-правових актах ЄС та України з питання цифровізації

Доцільність застосування методу RICE у процесі пріоритизації напрямів запобігання загрозам економічній безпеці держави обумовлюється рядом системних чинників. По-перше комплексністю економічної безпеки держави, що вимагає пошуку інструменту, здатного забезпечити можливість порівняння різних типів заходів, а по-друге – обмеженістю ресурсів національної економіки. Тому виникає потреба в оцінюванні потенційної ефективності напрямів запобігання загрозам, зважаючи на співвідношення очікуваного ефекту та витрат від різних заходів. Включення до моделі параметра «Confidence» дає змогу враховувати рівень достовірності аналітичних прогнозів, що є критичним за умов високої невизначеності середовища та динамічного впливу цифровізації. Нарешті, відтворюваність розрахунків у межах RICE забезпечує прозорість ухвалення рішень та дає можливість уточнення результатів.

Показник «Reach» розраховується на основі чисельності населення України, яке станом на 2025 рік складає 32 млн осіб [184]. Враховуючи 94% покриття домогосподарств мережею Інтернет [134] напрями що мають системний вплив на економічну безпеку держави в її цифрових аспектах, варто оцінювати у 30 млн осіб. Для інших напрямів, показник «Reach» визначається пропорційно частці населення, безпосередньо охопленого їх впливом.

Для визначення показників «Impact», «Confidence» та «Effort» було проведено експертне оцінювання, на основі розробленої карти оцінки напрямів запобігання загрозам економічної безпеки України в умовах цифровізації (додаток И), на базі Навчально-наукового інституту фінансів, економіки, управління та права Національного університету «Полтавська політехніка імені Юрія Кондратюка». В опитуванні взяли участь десять експертів, які є кандидатами та докторами економічних наук.

Результати опитування (додаток К) відображені у табличній формі для розрахунку оцінки RICE (табл. 3.8). Перевірка узгодженості оцінок експертів за кожною групою показників методом розрахунку коефіцієнта варіації надала задовільні результати: значення коефіцієнтів варіації коливаються від 0,03 до 0,28 при граничному значенні 0,3.

Таблиця 3.8

Пріоритизація напрямів запобігання загрозам економічної безпеки України в умовах цифровізації методом «RICE»

Напря́м	R, млн ос.	I	C	E	RICE
1	2	3	4	5	6
Гармонізація та уніфікація нормативно-правового забезпечення					
Модернізація економічного законодавства цифровими аспектами	32	1,3	0,8	1,7	19,6
Удосконалення інструментів регулювання впливу цифровізації	30	0,8	0,8	1,5	12,8
Формування єдиної цифрової стратегії	28	0,5	0,6	1	8,5
Оновлення методологічного апарату оцінки загроз в умовах цифровізації	27	0,5	0,8	0,5	21,3

Продовження табл. 3.8

1	2	3	4	5	6
Розвиток інформаційно-технологічних безпекових інструментів					
Сприяння зростанню цифрової грамотності населення	22	1,7	0,8	2	15,2
Навчання цифрових компетенцій, фахівців ІКТ сектору та допомога перекваліфікації працівників галузі ІТ	14	1,3	0,6	1	11,2
Удосконалення механізмів захисту зв'язку та мережі Інтернет	30	1	0,7	1	21,0
Розвиток цифрової демократії	32	0,7	0,9	1,5	13,4
Інтеграція в фінансовий та інституційний безпековий регіональний простір					
Участь у європейських проєктах розвитку і захисту цифрової інфраструктури	32	1	0,9	0,8	36
Залучення інвестиційних коштів для розвитку цифрових технологій	14	1	0,9	1	13,0
Спільні правила цифрового простору	22	0,9	0,8	0,8	19,6
Інтеграція інституцій та агенцій у безпекову архітектуру ЄС	32	1,8	0,8	2	23,0

Джерело: складено автором на основі [259; 134, 184]

Так, за результатами розрахунку найбільший потенціал з середнім значенням у 22,9 балів має напрям інтеграції в регіональний безпековий простір, дозволяючи охопити якнайбільшу кількість учасників і гарантуючи розвиток національних інституцій у відповідності до європейських практик, перейняття та адаптацію досвіду і технологій з мінімальними витратами. Утім, незначна різниця у 0,2 бали між середніми оцінками другого та третього напрямів, зумовлена їх спільним недоліком, а саме повільність процесів системного розвитку, оскільки він не може бути забезпечений імплементацією існуючого досвіду чи євроінтеграцією. Тому ці напрями вимагають значних інвестицій, мають накопичувальний та відкладений ефект.

Інший метод пріоритизації на основі матриці «Value vs. Effort» (пер. з англ. – цінність проти зусилля) [260] є дещо іншим інструментом пріоритизації. Він здебільшого використовується для ранжування ініціатив, проєктів або заходів за критеріями їх очікуваної результативності та ресурсної складності реалізації.

Потрібно відмітити, що цей метод, на відміну від більш деталізованих підходів на кшталт RICE, акцентує увагу саме на стратегічному співвідношенні витрат до користі у наглядному форматі. Тобто дозволяє швидко пріоритизувати напрями з високим потенціалом ефективності при низькій ресурсній вартості. В основі цього підходу лежить візуалізація об'єктів аналізу у двовимірному просторі. Так, вісь Y відображає цінність, а вісь X – зусилля, необхідні для реалізації. Це дозволяє класифікувати напрями запобігання загрозам економічної безпеки України в умовах цифровізації у чотири сектори: незначні цілі, легкі здобутки, великі цілі та не варті зусиль.

Адаптація матриці «Value vs. Effort» до потреб дослідження є доцільною з огляду на її аналітичну гнучкість, операційну простоту та здатність швидко структурувати великий масив альтернатив. Так, цей метод дозволяє швидко ідентифікувати, так звані, «швидкі перемоги» – заходи, що мають високу ефективність, і водночас не потребують значного фінансування чи тривалого впровадження. По-друге, цей метод забезпечує чітке позиціонування довгострокових, але ресурсномістких стратегій, оскільки вони потребують поетапного планування, залучення зовнішніх джерел фінансування та політичного консенсусу. І як третій фактор, у поєднанні з результатами попередньої оцінки за методом RICE, матриця «Value vs. Effort» дозволяє здійснити повторну перевірку вже визначених пріоритетних напрямів (рис. 3.11).

За результатами аналізу відповідної матриці можна виділити, що ключовими напрямками забезпечення економічної безпеки держави в умовах цифровізації є загальні реформи економіки та євроінтеграційні процеси. Проте забезпечувати економічні реформи, залучати іноземний капітал, брати участь у спільних безпекових проєктах одночасно є надскладною задачею, тому ці напрями мають реалізовуватися послідовно.

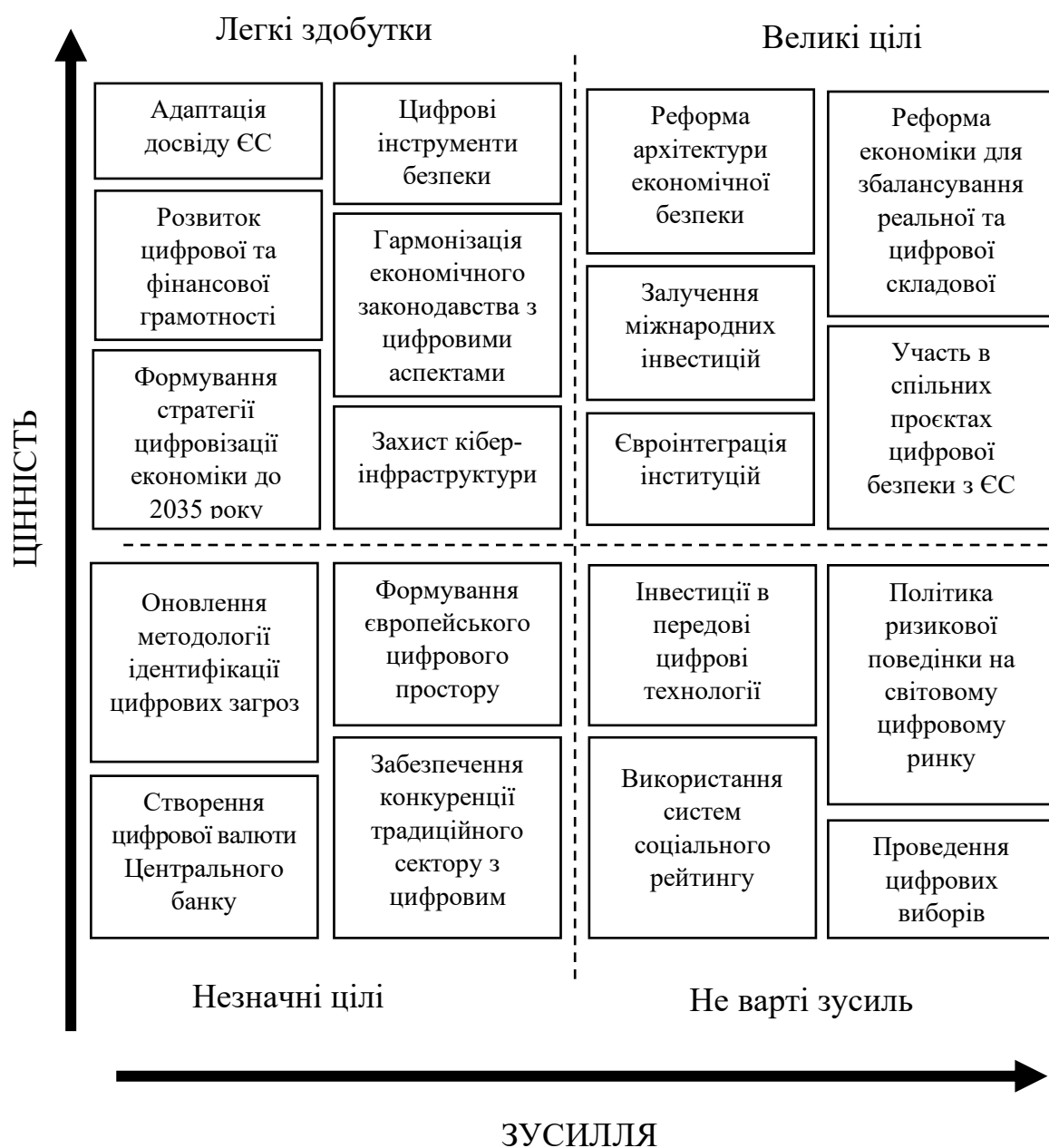


Рис. 3.11. Матриця «Value vs. Effort» пріоритизації напрямів запобігання загрозам економічної безпеки України в умовах цифровізації

Джерело: авторська розробка

Такі напрями запобігання загрозам економічної безпеки України, як імплементація європейського досвіду, розвиток нормативно-правового та інституційного забезпечення дозволяють отримати легкі переваги, проте не

створюють системних змін. Цьому також має сприяти загальний розвиток цифровізації, подальші ринкові реформи, наукове вивчення та осмислення нових економічних явищ, утім без значимих заходів на макро-, мікро- і нанорівнях це не матиме вагомого значення.

Третім підходом до пріоритизації, який доцільно використати для вирішення завдань дослідження, є метод Капо [261], що базується на концептуальній моделі аналізу потреб та очікувань зацікавлених сторін відповідно до впливу конкретних характеристик або ініціатив на рівень задоволеності кінцевих бенефіціарів. У контексті пріоритизації напрямів запобігання загрозам економічної безпеки України в умовах цифровізації метод Капо набуває нового значення, оскільки дозволяє класифікувати напрями забезпечення економічної безпеки держави не лише за показниками ефективності чи вартості реалізації, як це здійснюється в рамках RICE або «Value vs. Effort», але й з урахуванням очікувань бенефіціарів забезпечення безпеки: населення, бізнесу, інвесторів, міжнародних партнерів.

Так, застосування моделі Капо до задач дослідження, дозволить визначити першочергові потреби, реалізація яких є критично необхідною для підтримання мінімального рівня економічної безпеки держави в умовах цифровізації. Визначені «потреби» мають бути реалізовані незалежно від інших чинників, оскільки їх відсутність призводить до значного посилення впливу загроз. Натомість ідентифікація «вимог з лінійним впливом» дозволяє виявити напрями, які забезпечують пропорційне зростання економічної стійкості відповідно до обсягу вкладених ресурсів, а категорія «бажань» є важливою для формування сприятливого бізнес-середовища.

Отже, поєднання моделі Капо з попередніми аналітичними підходами формує повноцінну базу для визначення пріоритетних заходів запобігання загрозам економічній безпеці держави. Тому, з урахуванням попереднього застосування методів та «Value vs. Effort», використаємо модель Капо для пріоритизації напрямів запобігання загрозам економічної безпеки України в умовах цифровізації (рис. 3.12).



Рис. 3.12. Пріоритизація напрямів запобігання загрозам економічної безпеки України в умовах цифровізації методом «Капо»

Джерело: авторська розробка

Цей підхід дозволить ввести суб'єктивний, але важливий чинник – сприйняття та очікування бенефіціарів безпекозабезпечувальної діяльності. Що, в свою чергу, надає пріоритизації напрямів запобігання загрозам економічній безпеці України системного та багаторівневого виміру, забезпечуючи комплексне врахування внутрішніх обмежень та впливу детермінант зовнішнього середовища.

За методом Капо ядро пріоритетів вимог з лінійним впливом підкреслює значимість комплексних взаємопов'язаних заходів, що мають сприяти запобіганню загрозам економічної безпеки України в умовах цифровізації. Зважаючи на обмежені фінансові ресурси саме достатній вимір нормативно-правового забезпечення, адаптації агенцій та інституцій, сприяння проникненню технологій до підготовленого споживача утворює сприятливе середовище, що зменшує силу негативного впливу цифровізації на загрози економічній безпеці України. Також критичним є захист інфраструктури, особливо в умовах повномасштабної війни, враховуючи залежність усіх суб'єктів економіки від стійкості мережі Інтернет та зв'язку.

Застосовані моделі пріоритизації дозволяють зробити припущення про існування трьох груп пріоритетних напрямів запобігання загрозам економічної безпеки держави у відповідності до стратегічних цілей та орієнтирів. Стратегічні підходи першої групи орієнтовані на максимальне охоплення заходами забезпечення економічної безпеки держави суб'єктів її економічної діяльності. Насамперед вони передбачають комплексні структурні реформи економіки та інтеграція всіх суб'єктів економічної діяльності у європейську архітектуру безпеки. Друга група спирається на формуванні середовища стійкого до загроз цифровізації шляхом зміцнення стійкості цифрової та енергетичної інфраструктури та насичення і оновлення регуляторного забезпечення до вимог часу. І третя група, зосереджена на підвищенні ефективності виробництва в умовах цифровізації, що передбачає розвиток інституційного забезпечення та цифрових технологій, які сприятимуть зростанню продуктивності праці, конкурентоспроможності національної економіки та розвитку наукомістких галузей.

Отже, пріоритетні напрями запобігання загрозам економічної безпеки України в умовах цифровізації сформувані у модель (рис. 3.13).

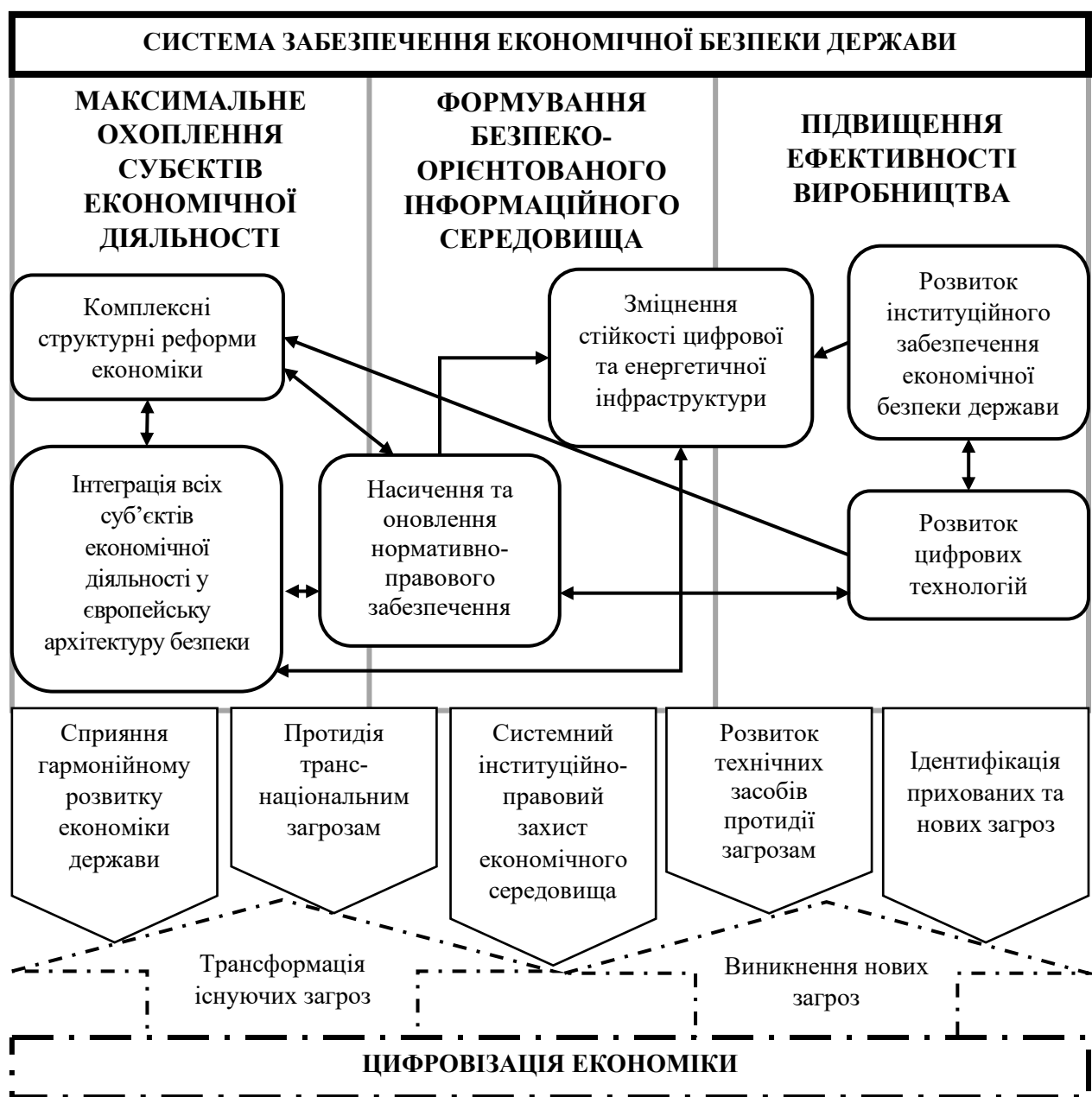


Рис. 3.13. Модель пріоритетних напрямів запобігання загрозам економічній безпеці України в умовах цифровізації

Джерело: авторська розробка

Так, на графіку видно, що коло пріоритетів достатньої мірою корелює з питаннями макроекономічного розвитку та загрозами економічній безпеці держави. А оскільки цифровізація лише посилює переваги і недоліки системи, то ключовим пріоритетом забезпечення безпеки на національному рівні залишається мінімізація впливу комплексних структурних загроз.

Спираючись на аналіз наукових досліджень, нормативно-правових актів та проведену пріоритизацію, постає нагальна потреба оптимізації взаємодії між окремими інституційними, нормативно-правовими та техніко-технологічними компонентами системи економічної безпеки держави, з виокремленням п'яти їх кластерів. Перший, насамперед, передбачає заходи щодо досягнення макроекономічної стабільності, захисту енергетичної інфраструктури та військової безпеки. Другий пов'язаний розвитком інституційного забезпечення економічної безпеки держави. Третій – оновлення нормативно-правового забезпечення економічної безпеки в умовах цифровізації та дотримання верховенства права. Четвертий передбачає залучення інвестицій в науку та сприяння розвитку цифрових технологій. П'ятий кластер побудований довкола безпекової євроінтеграції та спільних дій із забезпечення економічної безпеки.

Так, модель взаємозв'язку напрямів запобігання загрозам економічній безпеці України в умовах цифровізації (рис. 3.14) відображає специфіку взаємодії між детермінантами внутрішнього, ближнього та дальнього зовнішнього середовища. Розвиток інституційного забезпечення економічної безпеки виступає регулятором впливу цифровізації на економіку, нормативно-правове забезпечення – обмеженнями та орієнтиром для державної політики, а макроекономічна стабільність є джерелом ресурсного забезпечення економічної безпеки держави. Гармонійна взаємодія цих компонентів формує систему, здатну запобігати впливу традиційних, новоутворених та трансформованих загроз економічній безпеці держави в умовах цифровізації.

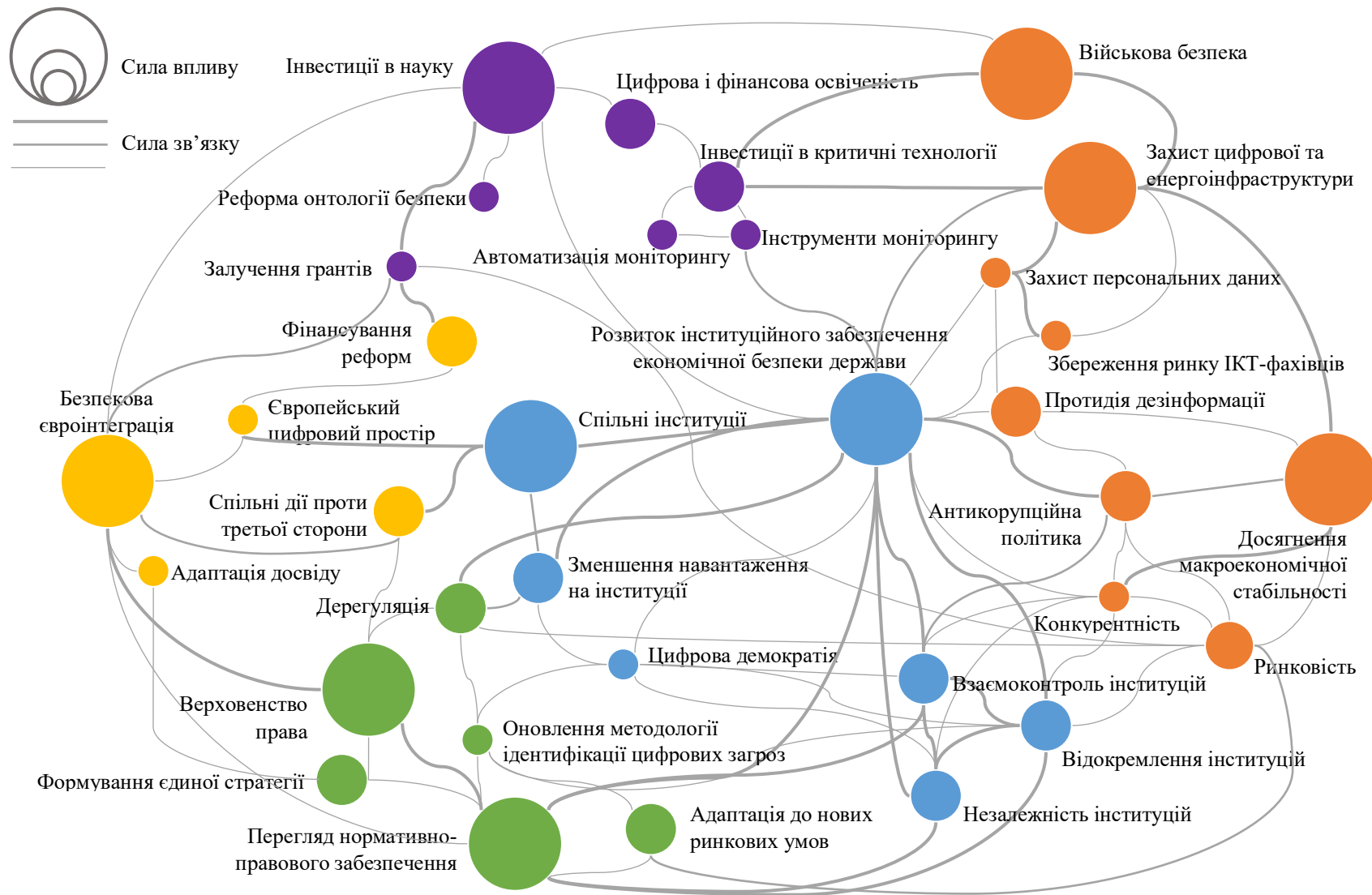


Рис. 3.14. Модель взаємозв'язку напрямів запобігання загрозам економічної безпеки України в умовах цифровізації

Джерело: систематизовано та доповнено автором на основі [101; 121; 172; 178-182]

Саме тому, на нашу думку, пріоритетним завданням запобігання загрозам економічній безпеці України в умовах цифровізації є удосконалення інституційно-правового забезпечення, що передбачає наділення відповідних інституцій автономією та достатніми повноваженнями.

Проте варто зазначити два бар'єри, що ускладнюють процес удосконалення інституційно-правового забезпечення економічної безпеки України. По-перше, це опір з боку внутрішніх бенефіціарів ризикової поведінки – тіньового бізнесу, надмірно бюрократизованих структур, суб'єктів корупційної та кримінальної діяльності. А другий, це нестача фінансових ресурсів, які важко залучити за рахунок внутрішнього запозичення, тоді як суб'єкти зовнішнього середовища зосереджені на власних цілях.

Саме тому зусилля, спрямовані на протидію окремим загрозам, є неефективними через розпорошення залучених ресурсів, докладених зусиль та слабкої політичної волі. Це зумовлює потребу у формуванні інтегрованого підходу, що дозволяє враховувати комплекс взаємозв'язків між усіма аспектами запобігання загрозам економічній безпеці України.

Так, розглядаючи напрями запобігання загрозам економічній безпеці України в умовах цифровізації (рис. 3.15), доцільно розподіляти їх за визначеними кластерами, конкретизуючи їх вплив на загрози та взаємозв'язок із складовими економічної безпеки держави. Так, зважаючи на визначені пріоритетні напрями на засадах максимального охоплення суб'єктів економічної діяльності, формування середовища стійкого до загроз цифровізації та підвищення ефективності виробництва, це дозволить узагальнити процес мінімізації загроз економічній безпеці України в умовах цифровізації.

Формування такого взаємозв'язку є необхідною передумовою для систематизації стратегічних пріоритетів та підвищення узгодженості інституційного забезпечення економічної безпеки в умовах цифровізації.

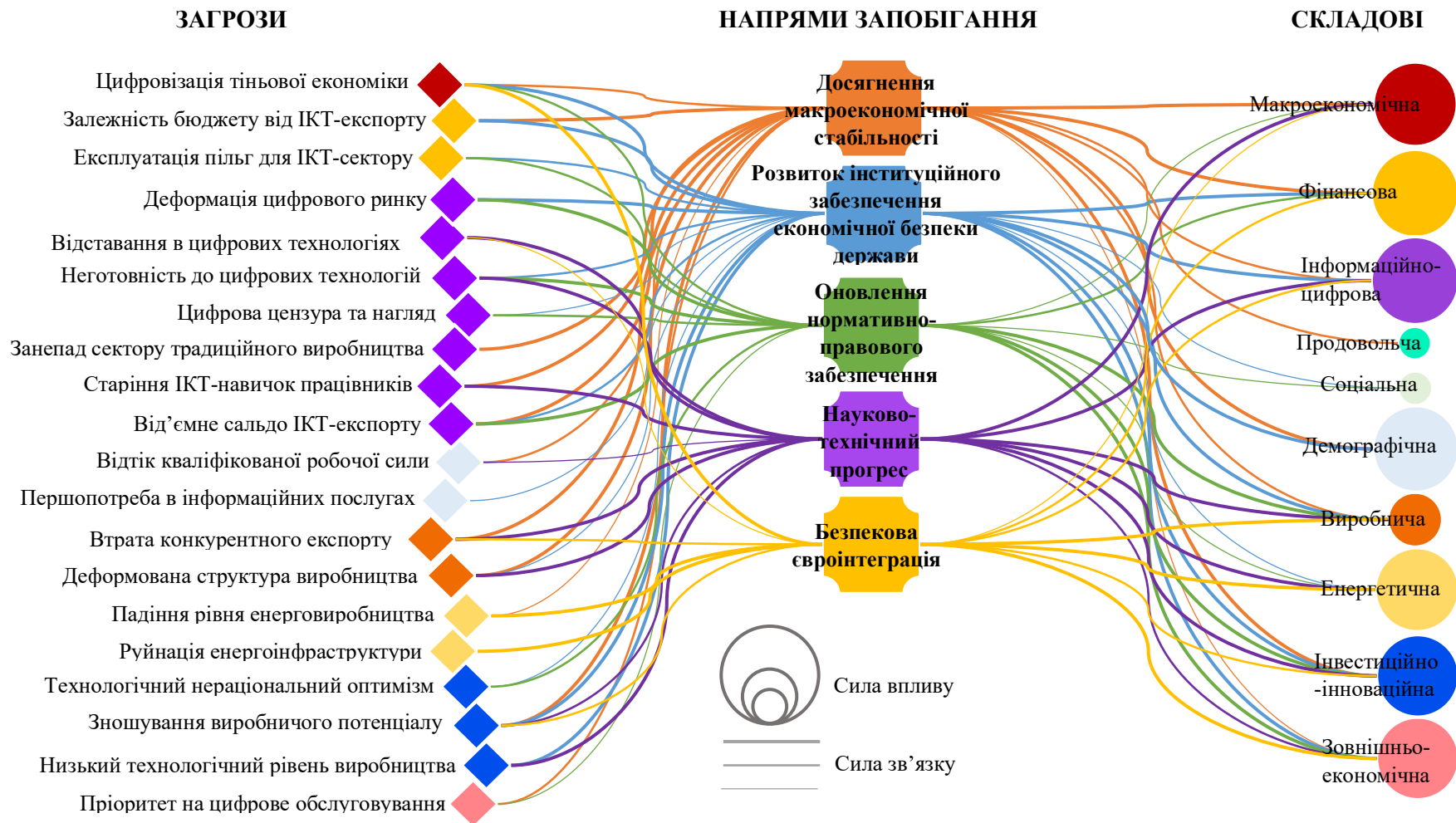


Рис. 3.15. Напрями запобігання загрозам економічній безпеці України в умовах цифровізації

Джерело: авторська розробка

Отже, оскільки моделювання впливу цифровізації на економічну безпеку держави через діяльність суб'єктів на макро-, мікро- та нанорівні національної економіки дозволило визначити критичні точки деструктивних процесів, зокрема, зростання кількості кібератак, формування структурних дисбалансів між секторами економіки, загострення конкуренції за кваліфіковані кадри в умовах ресурсного виснаження економіки та воєнних дій, існує об'єктивна потреба у мінімізації негативного впливу цифровізації на загрози економічній безпеці України.

Так, в умовах цифровізації актуальними пріоритетними напрямками запобігання загрозам економічній безпеці держави є приведення національного законодавства до європейських стандартів, активне використання міжнародного досвіду, розвиток науково-технічного потенціалу та участь у глобальних безпекових ініціативах. Утім, в умовах обмежених ресурсів та динамічних змін, спираючись на застосовані методи пріоритизації: RICE, «Value vs. Effort» та Kano, можна здійснити узагальнення стратегічних рішень на засадах максимального охоплення суб'єктів економічної діяльності, формування середовища стійкого до загроз цифровізації та підвищення ефективності виробництва, що дозволяє зменшити негативний вплив загроз на економічну безпеку держави.

Тому ефективне запобігання загрозам економічній безпеці України в умовах цифровізації потребує системного та багаторівневого стратегічного підходу, який має поєднувати ідентифікацію загроз інформаційно-цифровій складовій економічної безпеки держави, моделювання впливу цифровізації на неї та пріоритизацію напрямів за визначеними принципами. На наш погляд, такий підхід відображає адаптивну та дуальну динаміку впливу цифровізації на загрози економічній безпеці, визначає її критичні точки та виступає безальтернативним шляхом розвитку економічної безпеки України в умовах цифровізації та адаптації до нових глобальних викликів.

Висновки до розділу 3

1. На основі порівняльного аналізу архітектури інституційного забезпечення економічної безпеки України та Європейського Союзу обґрунтовано необхідність удосконалення нормативно-правових засад, механізмів взаємодії та інструментів забезпечення економічної безпеки України із урахуванням її прискореної інтеграції в європейський безпековий простір. Імплементация європейського досвіду є доцільною, зважаючи на узгодженість стратегічних цілей і пріоритетів економічного розвитку та необхідність гармонізації національної системи забезпечення економічної безпеки України із принципами та стандартами Європейського Союзу.

2. Визначено передумови інтеграції України в європейський цифровий простір та концептуальні засади розвитку інституційного забезпечення економічної безпеки держави в умовах цифровізації шляхом регуляторного удосконалення, що передбачає гармонізацію нормативно-правової бази, посилення інституційної спроможності та компетенцій, а також стимулювання техніко-технологічного розвитку.

3. За результатами ретроспективного аналізу та прогнозування інтегральних показників складових економічної безпеки України виявлено негативні тренди падіння її інтегрального показника у середньостроковій перспективі, що послугувало підґрунтям для подальшого моделювання впливу цифровізації на формування та трансформацію загроз економічній безпеці держави, зважаючи на динамічний характеру сучасних загроз.

4. Здійснено соціологічне дослідження цифрової грамотності населення, як чинника вразливості до загроз цифровізації на нанорівні національної економіки. Виявлено низький рівень готовності громадян до цифрових ризиків, нерівномірність цифрових компетенцій та високий суспільний запит на захист персональних даних. Обґрунтовано, що підвищення цифрової грамотності населення є необхідною передумовою

забезпечення стійкості національної економіки до негативного впливу цифровізації.

5. Розроблено науково-практичний підхід до моделювання впливу цифровізації на економічну безпеку держави, який, за авторською методикою, інтегрує кількісні та якісні методи аналізу, зокрема, соціологічного дослідження рівня цифрової грамотності. Запропонована модель відображає адаптивну динаміку впливу цифровізації на загрози економічній безпеці через діяльність суб'єктів на макро-, мікро- та нанорівні національної економіки. Використання даного підходу дозволило ідентифікувати та врахувати критичні точки деструктивних процесів, зумовлених цифровізацією, серед яких зростання кількості кібератак, формування структурних дисбалансів між секторами економіки, загострення конкуренції за кваліфіковані кадри для мінімізації загроз економічній безпеці України в умовах цифровізації.

6. Визначено пріоритетні напрями запобігання загрозам економічній безпеці держави в умовах цифровізації за допомогою комплексного застосування методів RICE, «Kano» та «Value vs. Effort» на засадах максимального охоплення суб'єктів економічної діяльності та формування безпекоорієнтованого інформаційного середовища, що мають забезпечити системність державної економічної політики в умовах цифровізації і зменшити негативний вплив загроз на економічну безпеку держави.

Основні результати дослідження відображені у наукових працях автора [203; 205; 219; 220; 222; 258].

ВИСНОВКИ

Проведене дослідження, спрямоване на вивчення впливу цифровізації на загрози економічній безпеці держави, дозволило поглибити теоретичні положення, удосконалити методичні підходи та розробити практичні рекомендації щодо виявлення та оцінювання впливу цифровізації на загрози економічній безпеці держави. Отримані теоретико-методичні та прикладні результати дозволяють сформулювати наступні висновки.

1. Теоретичне узагальнення основоположних елементів поняття цифровізація дозволило сформулювати інтегрований підхід до трактування її сутності через поєднання техніко-форматної, комерційно-оптимізаційної і технологічно-інформаційної концепцій. Обґрунтовано структурно-логічні взаємозв'язки між такими категоріями як цифрова трансформація, цифрова революція, цифрова економіка, цифрова інфраструктура, цифрова грамотність, цифрові технології, рішення і послуги. Встановлено властивості цифровізації, а саме адаптивність, мультиплікативність, циклічність розвитку, анонімність, віртуальність, масштабність, мобільність, персоналізація, транспарентність, що формує основу для розуміння багатовекторного впливу цифровізації на економічну безпеку держави.

2. Удосконалено підходи до класифікації загроз економічній безпеці в умовах цифровізації шляхом їх структуризації за рівнем походження (національний, наднаціональний) та за впливом цифрового компонента (активний, пасивний, відсутній). Запропонована класифікація сприяє розвитку методологічної бази виявлення загроз економічній безпеці держави. Здійснено кластеризацію нових загроз та обґрунтовано трирівневу модель детермінант впливу цифровізації на загрози економічній безпеці держави, що охоплює внутрішнє, ближнє та дальнє зовнішнє середовище.

3. Встановлено дуальний характер впливу цифровізації на економічну безпеку, що, з одного боку, проявляється у підвищенні стійкості економіки, а з іншого – призводить до виникнення нових та трансформації

існуючих загроз економічній безпеці держави. Визначено три сфери детермінації дуального впливу цифровізації на загрози економічній безпеці (соціально-економічну, кібернетично-технологічну, інституційно-регуляторну), що є підґрунтям для формування стратегічних орієнтирів держави за умов обмежених ресурсів та інтеграції до європейського цифрового простору.

4. Здійснено критичний аналіз чинного методичного інструментарію оцінки економічної безпеки України, що дозволило виявити низку його концептуальних недоліків: застарілість, суперечливість нормативного забезпечення, перевантаження індикаторами, фіксованість порогових значень. Поглиблено науково-методичних засади оцінювання впливу цифровізації на економічну безпеку доповненням існуючої методики індикаторами діагностики інформаційно-цифрової складової економічної безпеки України. Визначено загальний негативний стан економічної безпеки України. Ідентифіковано реальні загрози економічній безпеці держави в умовах цифровізації: вразливість до кібератак, залежність від імпорту технологій, структурні деформації та асиметрія розвитку національної економіки, що обмежують стійкість та адаптивність держави до нових викликів.

5. Визначено домінуючі тенденції цифровізації, які мають найбільший вплив на економічну безпеку України, а саме: зміна підходів до ведення воєнних дій, гібридне протистояння в кіберпросторі, внутрішні диспропорції впровадження цифровізації, прискорення процесів цифровізації. Виявлено, що цифровізація національної економіки, в умовах воєнного стану, зумовлює появу нових форм загроз та трансформацію вже існуючих.

6. Проведено компаративний аналіз інституційного забезпечення економічної безпеки України та ЄС, з урахуванням процесів інтеграції у європейський цифровий простір, що дозволив обґрунтувати концептуальні засади інституційного розвитку за трьома напрямками: удосконалення цифрових інструментів, гармонізацію регуляторного забезпечення та сприяння євроінтеграції.

7. Обґрунтовано науково-практичний підхід до моделювання впливу цифровізації на економічну безпеку держави, що базується на інтеграції кількісних і якісних методах аналізу та проведеного соціологічного дослідження рівня цифрової грамотності. Запропонована модель відображає адаптивну динаміку впливу цифровізації на загрози економічній безпеці через діяльність суб'єктів на макро-, мікро- та нанорівні національної економіки. Застосування моделі дозволило визначити критичні точки деструктивних явищ, а саме зростання кількості кібератак, формування структурних дисбалансів між секторами економіки, загострення конкуренції за кваліфіковані кадри, що створює передумови для мінімізації загроз економічній безпеці України в умовах цифровізації.

8. Запропоновано системний підхід до пріоритизації напрямів запобігання загрозам економічній безпеці держави в умовах цифровізації шляхом комплексного застосування методів RICE, «Kano» та «Value vs. Effort» на засадах максимального охоплення суб'єктів економічної діяльності та формування безпекоорієнтованого інформаційного середовища. Обґрунтовано напрями системної координації інституційного, нормативно-правового та техніко-технологічного забезпечення економічної безпеки держави, що дозволяє зменшити негативний вплив цифровізації на загрози економічній безпеці держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Berman S., Bell R. Digital transformation: Creating new business models where digital meets physical. NY : IBM Global Services, 2011. 20 p. URL: <https://www.ibm.com/downloads/documents/us-en/10a99803fc2fdcfa>.
2. Brennen S., Kreiss D. Digitalization and Digitization. *Culture Digitally*. URL: <https://culturedigitally.org/2014/09/digitalization-and-digitization/>.
3. Sharma A. K., Shanmugaboopathi D. P. S. Digital Revolution and Its Nature and Extent in the Contemporary World. *Technoarete Transactions on Advances in Social Sciences and Humanities*. 2022. Vol. 2, № 4. URL: <https://doi.org/10.36647/ttassh/02.04.a005>.
4. Абакуменко О., Деркач А., Корнеєва М. Діджиталізація банківського сектору України. *Фінансові дослідження*. 2016. № 1 (1). С.69–75. URL: <https://fr.stu.cn.ua/tmppdf/20.pdf>.
5. Ionan V. Digital Transformation in Ukraine: Before, During, and After the War. *ALI Social Impact Review*. URL: <https://www.sir.advancedleadership.harvard.edu/articles/digital-transformation-in-ukraine-before-during-after-war>
6. Новицька М. В. Порівняльний аналіз визначень терміну «цифрова економіка». *Економіка і організація управління*. 2022. № 2. С. 183–189. URL: <https://doi.org/10.31558/2307-2318.2022.2.18>.
7. Личковська М. Р., Меджидова В. О. Цифровізація економіки: Нові можливості та проблеми підвищення інноваційної спрямованості праці і професійної мобільності. *Міжнародні економічні відносини та світове господарство*. 2019. №27. С. 93-98.
8. Піжук О.І. Ключові драйвери цифрової трансформації економіки. *Вісник Київського національного університету технологій та дизайну. Серія Економічні науки*. 2019. № 3 (135). С. 38–47.
9. Цифровізація економіки України: трансформаційний потенціал: монографія / Вишневський В.П. (Ред.), Гаркушенко О.М., Князєв С.І. (Ред.),

Липницький Д.В., Чекіна В.Д. НАН України : Інститут економіки промисловості. Київ : Академперіодика, 2020. 188 с.

10. Економічна стратегія України 2030. *Український інститут майбутнього*. URL: <https://strategy.uifuture.org/>.

11. Strutynska I. Definitions of digital transformation. *Black Sea Economic Studies*. 2019. № 48. URL: <https://doi.org/10.32843/bses.48-47>.

12. Лігоненко Л., Хріпко А., Доманський А. Зміст та механізм формування стратегії діджиталізації в бізнес-організаціях. *Міжнародний науковий журнал «Інтернаука». Економічні науки*. 2018. № 22 (62) Т. 2. С. 21–24.

13. Семилітко Д. Діджиталізація в дії: як цифрова трансформація бізнесу впливає на успіх компанії. *Аудитор України*. 2019. № 5. С. 76–79.

14. Digitization, digitalization, digital and transformation: the differences. *i-SCOOP*. URL: <https://www.i-scoop.eu/digital-transformation/digitization-digitalization-digital-transformation-disruption/>.

15. Куйбіда В. С., Карпенко О. В., Наместнік В. В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України. Державне управління*. 2018. № 1. С. 5–11. URL: <http://academy.gov.ua/infpol/pages/dop/2/files/974f8478-cfe8-4d31-971b-d5116efff458.pdf>

16. Onore T. Digitalisation is not a fashion, but a way of business development. *Columbus*. URL: <https://www.linkedin.com/pulse/digitization-intangible-business-development-thomas-honore>.

17. Лукін С. Сучасні аспекти цифровізації публічних просторів. *Аспекти публічного управління*. 2020. Спецвипуск № 1. Т. 8 С. 91–93.

18. Наместнік В. В., Павлов М. М. Електронне, цифрове та smart-управління: сутність та співвідношення термінів. *Вісник Національної академії державного управління при Президентові України. Державне управління*. 2020. №1(96). С. 115–121.

19. Gudz O., Fediunin S., Shcherbyna V. Digitalization as competitive advantage of companies. *Economy. Management. Business*. 2019. P. 18–24. URL: <https://doi.org/10.31673/2415-8089.2019.031824>.
20. Грибіненко О. Діджиталізація економіки в новій парадигмі цифрової трансформації *Міжнародні відносини. Серія «Економічні науки»*. 2018. № 16. С. 35–37. URL: http://journals.iir.kiev.ua/index.php/ec_n/article/view/3523.
21. Gurenko A. V., Gaschutina O. E. The directions of the management systems development in the conditions of the digitalization of business in Ukraine. *Economy and Society*. 2018. № 19. URL: <https://doi.org/10.32782/2524-0072/2018-19-113>.
22. Korol S., Polovyk Y. Digitization of the Economy as Professional Development Factor. *Modern Economics*. 2019. Vol. 18, № 1. P. 67–73. URL: [https://doi.org/10.31521/modecon.v18\(2019\)-11](https://doi.org/10.31521/modecon.v18(2019)-11).
23. Digitalisation. *Oxford English Dictionary*. URL: <https://www.oed.com/information/about-the-oed?tl=true>.
24. Міхровська М. Діджитизація, діджиталізація, цифрова трансформація: зміст та особливості. *Грааль науки*. 2021. № 1. URL: <https://doi.org/10.36074/grail-of-science.19.02.2021.023>.
25. Greenstein S., Goldfarb A., Tucker C. The Economics of Digitization. Cheltenham, U.K. : Edward Elgar Publishing, 2013. 672 p.
26. Digitization of Economic Systems and Human Capital: Enterprise, Region, National Economy / L. H. Melnyk et al. *Mechanism of an Economic Regulation*. 2020. № 2. P. 9–28. URL: <https://doi.org/10.21272/mer.2020.88.01>.
27. French A. M., Shim J. P. The Digital Revolution: Internet of Things, 5G and Beyond. *Communications of the Association for Information Systems*. 2016. Vol. 38. P. 840–850. URL: <https://doi.org/10.17705/1cais.03840>.
28. Knell M. The digital revolution and digitalized network society. *Review of Evolutionary Political Economy*. 2021. Vol. 2, № 1. P. 9–25. URL: <https://doi.org/10.1007/s43253-021-00037-4>.

29. Єрмолаєва М. В. Теоретичні та практичні аспекти обліку грошових коштів. *Наукові та прикладні аспекти удосконалення бухгалтерського обліку, економічного контролю та системи оподаткування* : колективна монографія / за заг. ред. Плаксієнка В. Я. Полтава, 2018. С. 58 – 68

30. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України : Наказ Міністерства економічного розвитку і торгівлі України від 29.10.2013 № 1277. URL: <https://zakon.rada.gov.ua/rada/show/v1277731-13#Text>.

31. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : від 09.08.2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

32. Помулева В. М. Електронні гроші: сутність, облік та оподаткування. *Трансформація обліково-інформаційної політики та гармонізація фінансової звітності, аналізу і аудиту в умовах євроінтеграції* : монографія / за ред. Н. М. Левченко, Ж. К. Нестеренко. 2015. URL: http://eir.zntu.edu.ua/bitstream/123456789/1898/1/Pomulieva_Ecashs.pdf.

33. Ганущак Т. Інформаційна безпека підприємства та умови її забезпечення. *Вісник Одеського національного університету*. 2014. № 2(3), Т. 19. С. 59–63. URL: [http://nbuv.gov.ua/UJRN/Vonu_econ_2014_19_2\(3\)_15](http://nbuv.gov.ua/UJRN/Vonu_econ_2014_19_2(3)_15).

34. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>.

35. Погорелов Ю.С. Природа, рушійні сили та способи розвитку підприємства. Харків: АДА, 2010. 352 с.

36. Шемаєва Л., Лященко О. Визначення властивостей ресурсного забезпечення економічної безпеки підприємства. *Фінанси України*. 2012. Т. 1, № 10. С. 76–83. URL: https://finukr.org.ua/?page_id=723&aid=540.

37. Козловський С. В., Жураківський Є. С. Теоретико-методологічні підходи до визначення категорії економічна безпека та складових економічної безпеки України. *Економіка та держава*. 2015. Т. 6. С. 37–42.
38. Stolterman E., Fors A. Information Technology and the Good Life. *Information Systems Research*. 2003. Vol. 143. P. 687–692. URL: https://doi.org/10.1007/1-4020-8095-6_45.
39. Пекін А. Економічна безпека підприємств як економіко-правова категорія. *Економіст*. 2007. Т. 8. С. 23–25.
40. Franchuk V. I., Korchynskyi I. O. Economic security of the state: historical aspects and characteristic of the essence. *Efektivna ekonomika*. 2019. № 8. URL: <https://doi.org/10.32702/2307-2105-2019.8.7>.
41. Neustroiev Y. Modern approaches to the concept of «economic security of the country». *Efektivna ekonomika*. 2021. № 1. URL: <https://doi.org/10.32702/2307-2105-2021.1.98>.
42. Акімова Л. М. Становлення системи економічної безпеки держави в Україні: сутність, рівні, складники. *Публічне адміністрування: теорія та практика*. 2018. №1(19). С. 2–11.
43. Варналій З.С., Буркальцева Д.Д., Саєнко О.С. Економічна безпека України: проблеми та пріоритети зміцнення : монографія. Київ: Знання України, 2011. – 299 с.
44. Заросило В. Міжрегіональна Академія управління персоналом. *Наукові праці МАУП*. 2017. Т. 52 (1). С. 17–22.
45. Пугач О. Класифікація та систематизація загроз економічній безпеці держави в системі національної безпеки. *Економіка і організація управління*. 2014. Т. 1(17)–2(18), № 1-2. С. 209–217.
46. Porter M. E. Competitive Strategy: Techniques for Analyzing Industries and Competitors. New York, U.S. : Free Press, 1980. 186 p.
47. Johnson G., Scholes K., Whittington R. Exploring Strategy: Text & Cases (9th Edition). Hoboken, New Jersey, U.S. : Prentice Hall, 2011. 808 p.

48. Mardner O. The Relationship Between External Threats and Internal Weaknesses- The Basis for Security Reforms. *Security System Reforms as a Precondition for Euro-Atlantic Integration* : 9th International Scientific Conference, Skopje, 1 August 2018. URL: https://www.researchgate.net/publication/327317992_The_Relationship_Between_External_Threats_and_Internal_Weaknesses-_The_Basis_for_Security_Reforms.

49. Tendency of national security in the Baltic sea region : monograph / ed. by H. A. Makðtutis. Lithuania, Vilnius: The General Jonas Zemaitis Military Academy of Lithuania, 2006. 332 p. URL: <https://biblioteka.lka.lt/data/PDF-leidiniai/2006-2010/2006-Makstutis-Tendency%20of%20National%20security.pdf>

50. Гальцова О. Л. Цифровізація економіки як фактор економічного зростання : колективна монографія / за ред. О. Л. Гальцова. Херсон : Вид. дім «Гельветика», 2021. 260 с.

51. Кудінова (Чайкіна) А.О., Маслій О.А., Буряк А.А. Формалізація ризиків і загроз економічній безпеці України в умовах цифровізації. *Управління змінами та інновації*. 2024. № 12. С. 25–31. URL: <https://doi.org/10.32782/СМІ/2024-12-4>

52. Маркевич К. Не позитивами єдиними. Які небезпеки криються за цифровізацією. *Центр Разумкова*. URL: <https://razumkov.org.ua/statti/ne-pozytyvamy-iedynumu-yaki-nebezpeky-kryiutsia-za-tsyfrovizatsiiei>.

53. Кузнецова І. О., Кюне О. О. Класифікація загроз економічній безпеці підприємства. *Вісник соціально-економічних досліджень*. 2015. Т. 3, № 58. С. 120–128. URL: <http://dspace.oneu.edu.ua/jspui/bitstream/123456789/5248/1/Класифікація%20загроз%20економічній%20безпеці%20підприємства.pdf>.

54. Кириченко О. Класифікація загроз економічній безпеці української промисловості. *Вчені записки Університету «КРОК»*. 2017. № 48. С. 38–47. URL: <https://dspace.krok.edu.ua/server/api/core/bitstreams/0c596254-6ec2-4835-995f-6f00592d69a5/content>.

55. Fitzgerald P., Chien E. The Hackers Behind Stuxnet. *Broadcom Community*. URL: <https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=4f9aa8d9-2eb5-40f8-8997-10a258055c61&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.
56. Акулюшина М., Ісламова А., Біюк В. Перспективи розвитку цифрової економіки в Україні. *Економіка та суспільство*. 2024. № 61. URL: <https://doi.org/10.32782/2524-0072/2024-61-11>.
57. Maslii O., Maksymenko A. Risks and threats to Ukraine's economic security in the digital sphere in times of war. *Market economy: modern management theory and practice*. 2023. Vol. 21, № 3(52). P. 176–196. URL: [https://doi.org/10.18524/2413-9998.2022.3\(52\).275802](https://doi.org/10.18524/2413-9998.2022.3(52).275802).
58. China's digital dictatorship. *The Economist*. URL: <https://www.economist.com/leaders/2016/12/17/chinas-digital-dictatorship>.
59. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках : Розпорядження Кабінету Міністрів України від 31.12.2024 № 1351-р. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-p#Text>.
60. Гіг-економіка як середовище трансформації міжнародного ринку праці / В. Г. Панченко та ін. *Журнал «Інвестиції: практика та досвід»*. 2024. № 4. С. 12–18. URL: <https://doi.org/10.32702/2306-6814.2024.4.12>.
61. Ashford S. J., Caza B. B., Reid E. M. From surviving to thriving in the gig economy: A research agenda for individuals in the new world of work. *Research in Organizational Behavior*. 2018. Vol. 38. P. 23–41. URL: <https://doi.org/10.1016/j.riob.2018.11.001>.
62. Рубанов П. М. Розмежування сутності понять «електронні гроші», «віртуальні гроші» та «криптовалюти». *Ефективна економіка*. 2015. № 4. URL: <http://www.economy.nayka.com.ua/?op=1&z=6026>.

63. Грицай С. Цифрові гроші в Україні – CBDC? *Юридичний науковий електронний журнал*. 2022. № 4. С. 247–249. URL: <https://doi.org/10.32782/2524-0374/2022-4/57>.
64. Bloom D. E., McKenna M., Prettnner K. Demography, unemployment, automation, and digitalization: implications for the creation of (decent) jobs, 2010–2030. Cambridge, MA : National Bureau Of Economic Research, 2018. 34 p. URL: https://www.nber.org/system/files/working_papers/w24835/w24835.pdf.
65. Гавриленко Н. Г., Тарасенко І. О. Сучасні тенденції цифровізації економіки: проблеми та перспективи розвитку. *Міжнародний науковий журнал «Інтернаука»*. Серія : Економічні науки. 2021. Т. 1, № 3 (47). С. 36–46.
66. Abeliasky A., Prettnner K. Automation and demographic change. *University of Göttingen, Center for European, Governance and Economic Development Research (cege), Göttingen*. 2017. Cege Discussion Papers, № 310. URL: <https://www.econstor.eu/handle/10419/157381>.
67. Acemoglu D., Restrepo P. Robots and Jobs: Evidence from US Labor Markets. *Journal of Political Economy*. 2020. Vol. 128(6). P. 2188–2244. URL: <https://doi.org/10.3386/w23285>.
68. Acemoglu D., Restrepo P. Demographics and Automation. *Review of Economic Studies*. 2021. P. 1–44. URL: <https://doi.org/10.1093/restud/rdab031>.
69. Shevchuk I., Deputat B., Tarasenko O. Digitalization and its impact on Ukraine's economy: advantages, challenges, threats and risks. *Black Sea Economic Studies*. 2019. № 47. URL: <https://doi.org/10.32843/bses.47-66>.
70. Вінник О. Переваги та ризики цифровізації економіки: проблеми правового регулювання. *Entrepreneurship, Economy and Law*. 2020. № 3. С. 56–62. URL: <https://doi.org/10.32849/2663-5313/2020.3.10>.
71. Advantages and challenges of digitalization of the Ukrainian economy / O. Cherep et al. *Ukrainian Journal of Applied Economics and Technology*. 2024. Vol. 9, № 1. P. 131–135. URL: <https://doi.org/10.36887/2415-8453-2024-1-21>.
72. 2030 Digital Compass: the European way for the Digital Decade : Communication From The Commission to The European Parliament, The Council,

The European Economic And Social Committee And The Committee Of The Regions of 09.03.2021 № COM(2021) 118 final. URL: <https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf>.

73. Wang P., D'Cruze H., Wood D. Economic Costs and Impacts of Business Data Breaches. *Issues in Information Systems*. 2019. Vol. 20, № 2. P. 162–171. URL: <https://pdfs.semanticscholar.org/c104/5c170e6f7cbd31423354dbf93eef4eb1dd1a.pdf>.

74. Cost of a data breach 2024. *International Business Machines Corporation*. URL: https://www.ibm.com/reports/data-breach?_ga=2.3019568.1436252282.1637663307-1392706600.1635762999.

75. FBI: Internet crime report. *Internet Crime Complaint Center (IC3)*. URL: <https://www.ic3.gov/Home/Index>.

76. Setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing regulation : Regulation (EC) № 765/2008 : as of 13 August 2008. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0765&locale=en>.

77. The Netherlands moves toward an outright loot box ban. *PCgamer*. URL: <https://www.pcgamer.com/the-netherlands-moves-toward-an-outright-loot-box-ban>.

78. Diablo Immortal skips Dutch and Belgian launches and loot boxes might be to blame. *The Verge*. URL: <https://www.theverge.com/2022/6/1/23149771/diablo-immortal-loot-boxes-belgium-the-netherlands-gambling>.

79. Tofan M., Bostan I. Some Implications of the Development of E-Commerce on EU Tax Regulations. *Laws*. 2022. Vol. 11, № 1. P. 13. URL: <https://doi.org/10.3390/laws11010013>.

80. Farrugia S., Ellul J., Azzopardi G. Detection of illicit accounts over the Ethereum blockchain. *Expert Systems with Applications*. 2020. Vol. 150. P. 113318. URL: <https://doi.org/10.1016/j.eswa.2020.113318>.

81. Hornuf L., Kück T., Schwienbacher A. Initial coin offerings, information disclosure, and fraud. *Small Business Economics*. 2021. URL: <https://doi.org/10.1007/s11187-021-00471-y>.
82. Navarro Cardoso F. Criptomonedas (en especial, bitcóin) y blanqueo de dinero. *Revista Electrónica de Ciencia Penal y Criminología*. Vol. 21-14. P. 1–45. URL: <https://dialnet.unirioja.es/servlet/articulo?codigo=7042336>.
83. The Chainalysis 2024 Geography of Cryptocurrency Report. *The Blockchain Data Platform*. URL: <https://www.chainalysis.com/blog/2024-global-crypto-adoption-index>.
84. Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain / D. Sanz-Bas et al. *Laws*. 2021. Vol. 10, № 3. P. 57. URL: <https://doi.org/10.3390/laws10030057>.
85. Цифрова економіка: тренди, ризики та соціальні детермінанти. Київ : «Заповіт», 2020. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf.
86. Digitization of Economic Systems and Human Capital: Enterprise, Region, National Economy / L. H. Melnyk et al. *Mechanism of an Economic Regulation*. 2020. № 2. P. 9–28. URL: <https://doi.org/10.21272/mer.2020.88.01>.
87. Explore academic papers in a visual graph / A. Tarnavs.ky et al. *Connected Papers*. URL: <https://www.connectedpapers.com/>.
88. Schaefer D. L. Economic Scarcity and Political Philosophy: Ancient and Modern Views. *International Political Science Review*. 1983. Vol. 4, № 3. P. 279–94. URL: <http://www.jstor.org/stable/1601096>.
89. Economic Security: Meaning, History in the US, FAQs. *Investopedia*. URL: <https://www.investopedia.com/economic-security-5213404>.
90. Коптева Г. Класифікація підходів до оцінки економічної безпеки підприємства. *Східна Європа: економіка, бізнес та управління*. 2020. № 2(25). URL: <https://doi.org/10.32782/easterneurope.25-32>.

91. The Elephant Curve of Global Inequality and Growth / F. Alvaredo et al. *AEA Papers and Proceedings*. 2018. Vol. 108. P. 103–108. URL: <https://doi.org/10.1257/pandp.20181073>.
92. Vărzaru A. A., Bocean C. G. Digital Transformation and Innovation: The Influence of Digital Technologies on Turnover from Innovation Activities and Types of Innovation. *Systems*. 2024. Vol. 12, № 9. P. 359. URL: <https://doi.org/10.3390/systems12090359>.
93. Пищуліна О. Дві сторони цифрових технологій: цифрова диктатура або збереження стійкості. *Центр Разумкова*. URL: https://razumkov.org.ua/statti/dvi-storony-tsyfrovykh-tekhnologii-tsyfrova-dyktatura-abo-zberezhennia-stiikosti#_ftn9.
94. Вареник В.М. Аналіз методик розрахунку економічної безпеки України. *Академічний Огляд*. 2016. Т. 1, № 44. С. 70–79. URL: <https://acadrev.duan.edu.ua/images/PDF/2016/1/9.pdf>.
95. Маринич Т. Компаративний аналіз індикаторів фінансової стабільності України. *Механізм регулювання економіки*. 2010. Т. 1, № 3. С. 218–226. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/3582/1/5_2.pdf.
96. Субботович Ю., Антропова О. Індикатори фінансової безпеки України. *Фінансовий сектор*. 2013. № 2. С. 1444–151. URL: <http://dspace.wunu.edu.ua/bitstream/316497/10024/1/Субботович%20Ю..pdf>.
97. Єрмошенко М. М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення : монографія. Київ : КНТЕУ, 2001. 309 с.
98. Міністерство економіки України. Офіційна відповідь на запит № ЗІ-647-24 від 27.05.2024 щодо надання публічної інформації про показники фінансової складової економічної безпеки України за період 2019-2022 років. 2024. URL: https://dostup.org.ua/request/pokazniki_finansovoyi_skladovoyi?nocache=incoming-407827#incoming-407827.

99. Міністерство економіки України. Офіційна відповідь на запит № ЗІ-952-23 від 04.10.2023 щодо надання публічної інформації про економічну безпеку України за період 2010-2022 років. 2023. URL: https://dostup.org.ua/request/pokazniki_iekonomichnoyi_bezpie_5?utm_campaign=alaveteli-experiments-87&utm_content=sidebar_similar_requests&utm_medium=link&utm_source=доступ+до+правди.

100. Національний банк України. *Національний банк України*. URL: <https://bank.gov.ua/>.

101. Гбур З. Інституційне забезпечення економічної безпеки України. *Інвестиції: практика та досвід*. 2018. № 3. С. 98–102. URL: http://www.investplan.com.ua/pdf/3_2018/22.pdf.

102. Moldowan O. Economic security of the state as a basic concept of ecoestate: in searching of a universal definition. *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Economy and Management*. 2021. Vol. 71, № 4. URL: <https://doi.org/10.32838/2523-4803/71-4-2>.

103. Schoenmaker D., Van Dijk M., Jan Reinders H. The COVID-19 threat to financial stability in Europe. *CEPR*. URL: <https://cepr.org/voxeu/columns/covid-19-threat-financial-stability-europe>.

104. Cybersecurity threat trends: phishing, crypto top the list. *Cisco Umbrella*. URL: <https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list>.

105. Internet Security Threat Report. *Symantec*. 2019. 61 p.

106. Про боротьбу з корупцією : Закон України від 05.10.1995 № 356/95-ВР : станом на 1 січ. 2011 р. URL: <https://zakon.rada.gov.ua/laws/show/356/95-vp#Text>.

107. Основи платіжного картознавства : посіб.-довід. для прокурорів та суддів / за ред. О. Карпов. Київ : Укр. міжбанк. Асоц. членів платіж. систем «ЕМА», 2018. 86 с.

108. 2024 Cybersecurity Statistics: The Ultimate List of Stats, Data & Trends. *PurpleSec*. URL: <https://purplesec.us/resources/cybersecurity-statistics/>.
109. Назаренко І. Л., Ткаченко Ю. В. Стан і перспективи розвитку IT сфери в Україні в період війни. *Вісник економіки транспорту і промисловості*. 2023. № 81-82. С. 59–67. URL: <https://doi.org/10.18664/btie.81-82.287170>.
110. Global Risks Report 2024. Geneva, Switzerland : World Economic Forum. 2024. 124 p. URL: <https://www.weforum.org/publications/global-risks-report-2024/>.
111. Cyber security breaches survey 2024. London, UK : Department for Science, Innovation & Technology UK. 2024. 85 p. URL: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#chapter-6-cyber-crime>.
112. Allianz Risk Barometer 2023 - Rank 1: Cyber incidents. *Allianz Commercial*. URL: <https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2023-cyber-incidents.html>.
113. Global cybercrime estimated cost 2029. *Statista*. URL: <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>.
114. Complaints on internet crime annual 2023. *Statista*. URL: <https://www.statista.com/statistics/267546/number-of-complaints-about-us-internet-crime/>.
115. Number of internet users worldwide 2024. *Statista*. URL: <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/>.
116. COVID-19: the impact on SMEs with forecasting model. *Modelfinance*. URL: <https://www.modelfinance.com/en/blog/2020-03-12-covid-19-the-forecasting-model-to-predict-the-impact-on-smes>.
117. The impact of Covid-19 on businesses' expectations: evidence from the Decision Maker Panel. *Bank of England*. URL: <https://www.bankofengland.co.uk/quarterly-bulletin/2020/2020-q3/the-impact-of-covid-19-on-businesses-expectations-evidence-from-the-decision-maker-panel>.

118. Navigating disruptive crises through service-led growth: The impact of COVID-19 on Italian manufacturing firms / M. Rapaccini et al. *Industrial Marketing Management*. 2020. Vol. 88. P. 225–237. URL: <https://doi.org/10.1016/j.indmarman.2020.05.017>.

119. Casaló L. V., Flavián C., Ibáñez-Sánchez S. Influencers on Instagram: Antecedents and consequences of opinion leadership. *Journal of Business Research*. 2020. Vol. 117. P. 510–519. URL: <https://doi.org/10.1016/j.jbusres.2018.07.005>.

120. The impact of COVID-19 on small business outcomes and expectations / A. W. Bartik et al. *Proceedings of the National Academy of Sciences*. 2020. Vol. 117, № 30. P. 17656–17666. URL: <https://doi.org/10.1073/pnas.2006991117>.

121. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>.

122. The COVID-19 pandemic is contracting in some countries while expanding in others, shaping the attitudes and behaviors of financial decision makers / J. Euart et al. *McKinsey & Company*. URL: <https://www.mckinsey.com/industries/financial-services/our-insights/a-global-view-of-financial-life-during-covid-19>.

123. Barrafreem K., Västfjäll D., Tinghög G. Financial well-being, COVID-19, and the financial better-than-average-effect. *Journal of Behavioral and Experimental Finance*. 2020. Vol. 28. P. 100410. URL: <https://doi.org/10.1016/j.jbef.2020.100410>.

124. The effects of coronavirus on household finances and financial distress / P. Bourquin et al. London, U.K. : The Institute for Fiscal Studies, 2020. 33 p. URL: <https://doi.org/10.1920/bn.ifs.2020.bn0298>.

125. Human Development Report 2021-22. New York, U.S. : UNDP. 2022. 320 p. URL: <https://hdr.undp.org/content/human-development-report-2021-22>.

126. The World Press Freedom Index. *Reporters Without Borders*. URL: <https://rsf.org/en/index>.
127. Шевчук І.Б, Шевчук А. В, Стасенко З.В. ІТ-сфера в умовах війни: основні тенденції та вплив на розвиток економіки регіону. *Scientific Bulletin of PUET: Economic Sciences*. 2023. № 4(110). URL: <https://doi.org/10.37734/2409-6873-2023-4-9>.
128. The Economist Intelligence Unit's quality-of-life index. *The Economist*. URL: https://www.economist.com/media/pdf/QUALITY_OF_LIFE.pdf.
129. Corruption Perceptions Index. *Corruption Perceptions Index Transparency International Ukraine*. URL: <https://cpi.ti-ukraine.org/2023>.
130. Market Insights. eCommerce – Ukraine. *Statista*. URL: <https://www.statista.com/outlook/emo/e-commerce/ukraine?currency=usd#revenue>.
131. Results and plans: e-commerce of Ukraine 2018/2019. *EVO.Business*. URL: <https://evo.business/itogi-plany-e-commerce-ukrainy-20182019/>.
132. UN Trade and Development Statistic Informations. *UN Trade and Development (UNCTAD)*. URL: <https://unctad.org/>.
133. Лісік О., Моряк Т. Аналіз стану ІТ-сектору України в умовах повномасштабної війни. *Економіка та суспільство*. 2023. № 55. URL: <https://doi.org/10.32782/2524-0072/2023-55-67>.
134. Дослідження цифрової грамотності в Україні. Київ : Міністерство цифрової трансформації України. 2023. 70 с. URL: <https://assets.kpmg.com/content/dam/kpmg/ca/pdf/2017/04/the-truth-about-online-consumers-canadian-addendum.pdf>.
135. Ukraine Retail Sales YoY. *Trading Economics*. URL: <https://tradingeconomics.com/ukraine/retail-sales-yoy>.
136. Global Risks Report 2025. Geneva, Switzerland : World Economic Forum. 2025. 104 p. URL: <https://www.weforum.org/publications/global-risks-report-2025/>.

137. Junior A. S. C., Arima C. H. Threat modeling: a study on its application in digital transformation from the perspective of risk. *Revista de Gestão e Secretariado*. 2023. Vol. 14, № 1. P. 1158–1169. URL: <https://doi.org/10.7769/gesec.v14i1.1581>.

138. Ostrovskiy I., Stadnyk G. Sustainable development in the digital economy: strategies, challenges and indicators of the development of smart cities. *Economic scope*. 2024. URL: <https://doi.org/10.32782/2224-6282/189-29>.

139. Aliyev A., Shahverdiyeva R. O. Scientific and Methodological bases of Complex Assessment of Threats and Damage to Information Systems of the Digital Economy. *International Journal of Information Engineering and Electronic Business*. 2022. Vol. 14, № 2. P. 23–38. URL: <https://doi.org/10.5815/ijieeb.2022.02.02>.

140. Aliyev A. Issues of complex assessment of damage to the security of information systems. *I Republican Scientific-Practical Conference «Problems of Information Security»* : Baku, 2013. P. 71–74.

141. Threat Modeling. *DEKRA*. URL: <https://www.dekra.com/en/threat-modeling/>

142. Як Україна виробляла електроенергію до повномасштабної війни. *Слово і Діло*. URL: <https://www.slovoidilo.ua/2024/06/04/infografika/ekonomika/yak-ukrayina-vyroblyala-elektroenerhiyu-povnomasshtabnoyi-vijny>.

143. Розвиток генерувальних потужностей та інвестиції в альтернативну енергетику. *Forbes*. URL: <https://forbes.ua/money/rozvitok-generuyuchikh-potuzhnostey-ta-investitsii-v-alternativnu-energetiku-pro-trendi-energetichnoi-galuzi-ta-prognoz-na-2025-rik-rozpovidae-energoekspert-ivan-bondarchuk-15012025-26321>.

144. Інфляційний звіт Квітень. Київ : Національний банк України. 2024. 54 с. URL: https://bank.gov.ua/admin_uploads/article/IR_2024-Q2.pdf?v=7.

145. Про схвалення основних прогнозних макропоказників економічного і соціального розвитку України на 2024-2026 роки : Постанова

Каб. Міністрів України від 15.12.2023 № 1315. URL: <https://zakon.rada.gov.ua/laws/show/1315-2023-п#Text>.

146. A decision support model for evaluating risks in the digital economy transformation of the manufacturing industry / C. Shang et al. *Journal of Innovation & Knowledge*. 2023. Vol. 8, № 3. URL: <https://doi.org/10.1016/j.jik.2023.100393>.

147. Як український еcommerce пережив 2023 річні показники + прогноз 2024. Аналітична агенція Promodo. URL: <https://www.promodo.ua/yak-ukrayinskiy-ecommerce-pereziv-2023>.

148. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Київ: Державна служба спеціального зв'язку та захисту інформації України. 2022. 10 с. URL: <https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanih-kiberincidentiv-viros-la-maizhe-vtrichi-zvit>.

149. Російські кібероперації. Київ: Державна служба спеціального зв'язку та захисту інформації України. 2023. 23 с. URL: <https://cip.gov.ua/ua/news/kilkist-zareyestrovanih-kiberincidentiv-u-pershomu-pivrichchi-2023-roku-zros-la-bilshe-nizh-udvichi>.

150. Digitalization of the Ukrainian economy during a state of war is a necessity of the time / L. Verbivska et al. *Revista Amazonia Investiga*. 2023. Vol. 12, № 68. P. 184–194. URL: <https://doi.org/10.34069/ai/2023.68.08.17>.

151. Global Innovation Index 2024: Unlocking the Promise of Social Entrepreneurship. Geneva, Switzerland: WIPO, 2024. 325 p. URL: <https://doi.org/10.34667/tind.50062>.

152. Колеснікова Г. Інституційне забезпечення розвитку фінансово-інвестиційної інфраструктури промислового регіону. *Управління економікою: теорія та практика*. 2013. С. 149–170. URL: http://nbuv.gov.ua/UJRN/Ue_2013_2013_13.

153. Пустоваров А. Інституційне забезпечення процесу цифрової трансформації управління розвитком національної економіки. *Науковий вісник Ужгородського національного університету*. 2019. Т. 1, № 24. С. 164–169. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/24_1_2019ua/32.pdf.

154. World Development Report «Digital dividends». Washington DC, U.S. : The World Bank Group, 2016. 359 p. URL: <https://www.worldbank.org/en/publication/wdr2016>.
155. Інфляційний звіт Липень. Київ : Національний банк України. 2024. 46 с. URL: https://bank.gov.ua/admin_uploads/article/IR_2024-Q3.pdf?v=9.
156. Horn S., Reinhart C. M., Trebesch C. China's overseas lending. *Journal of International Economics*. 2021. Vol. 133. P. 103539. URL: <https://doi.org/10.1016/j.jinteco.2021.103539>.
157. Setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) : Regulation (EU) 2021/821 of 11.06.2021 № PE/54/2020/REV/2 : as of 8 November 2024. URL: <http://data.europa.eu/eli/reg/2021/821/oj>.
158. Regards the list of dual-use items : Regulation (EU) 2021/821 of 15.12.2023 № 2023/2616. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302616&qid=1702635582620.
159. The Netherlands and EU policy areas. *Information from the Government of the Netherlands*. URL: <https://www.government.nl/topics/european-union/the-netherlands-and-the-eu-policy-areas>.
160. The Netherlands as a champion of EU enlargement? Wassenaar, The Netherlands : Clingendael 2020. 10 p. URL: https://www.clingendael.org/sites/default/files/2020-11/Policy_brief_The_Netherlands_as_a_champion_of_EU_enlargement_November_2020.pdf.
161. Illuminating the Role of Third-Country Jurisdictions in Sanctions Evasion and Avoidance (SEA) / L. O'Shea et al. Birmingham, UK : University of Birmingham., 2023. 46 p. URL: <https://static1.squarespace.com/static/63e4aef3ae07ad445eed03b5/t/653638a6d036b43de26ab4ab/1731067227329/SOCACE-RP21-ThirdCountries-20Oct23.pdf>.
162. Evroux C. Enhancing research security. European Parliamentary Research Service, 2024. 8 p. URL:

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760387/EPRS_BRI\(2024\)760387_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760387/EPRS_BRI(2024)760387_EN.pdf).

163. European economic security Strategy : Joint Communication to the European Parliament of 20.06.2023 № JOIN(2023) 20 final. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020>.

164. A Set Of Robust And Comprehensive Measures For An Eu Coordinated Approach To Secure 5g Networks : The EU toolbox for 5G security of 17.04.2024. URL: <https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security>.

165. Establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (Chips Act) : Regulation (EU) of 18.09.2023 № PE/28/2023/INIT. URL: <http://data.europa.eu/eli/reg/2023/1781/oj>.

166. Regulation (EU) : The protection of the Union and its Member States from economic coercion by third countries of 07.12.2023 № PE/34/2023/REV/1. URL: <http://data.europa.eu/eli/reg/2023/2675/oj>.

167. Regulation (EU) : The establishment of a European instrument for temporary support to mitigate unemployment risks in an emergency (SURE) following the COVID-19 outbreak : Council Regulation (EU) of 20.05.2020 № ST/7917/2020/INIT. URL: <http://data.europa.eu/eli/reg/2020/672/oj>.

168. Bureau van Dijk. Orbis. Modys. URL: <https://www.moody's.com/web/en/us/capabilities/company-reference-data/orbis.html>.

169. About us - The Wassenaar Arrangement. *The Wassenaar Arrangement*. URL: <https://www.wassenaar.org/about-us>.

170. Відомості про діяльність Міністерства економіки та енергетики Німеччини. *Офіційний сайт Федерального Міністерства економіки та енергетики Німеччини*. URL: <https://www.bmwi.de/Redaktion/DE/Home/home.html>.

171. Federal Statistical Office. Short-term indicators. *Destatis*. URL: https://www.destatis.de/EN/Themes/Economy/Short-Term-Indicators/_node.html.

172. Глушко А., Таранець Б. Інституційне забезпечення економічної безпеки суб'єктів господарювання: досвід ЄС для України. *Економіка відновлення міст : зб. матеріалів Міжнар. урбаністич. форуму*, Київ : КНЕУ, 2023. С. 39–42. URL: <https://reposit.nupp.edu.ua/bitstream/PolNTU/12650/1/International%20Urban%20Forum%20KNEU%20-%20abstracts-39-42.pdf>.
173. Законодавство Франції. *Légifrance*. URL: <https://www.legifrance.gouv.fr/>.
174. Відомості Міністерства підприємництва і торгівлі Польщі. *Офіційний сайт Міністерства підприємництва та технологій Польщі*. URL: <https://www.gov.pl/web/entrepreneurship-and-technology-ministry>.
175. Офіційні відомості Банку Англії. *Bank of England*. URL: <https://www.bankofengland.co.uk/>.
176. Regulation (EU) : The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Consolidated text: Regulation (EU) of 04.05.2016 № 02016R0679-20160504. URL: <http://data.europa.eu/eli/reg/2016/679/2016-05-04>.
177. Consolidated text: Directive (EU) : On measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive and repealing (NIS 2 Directive) of 27.12.2022 № 02022L2555-20221227. URL: <http://data.europa.eu/eli/dir/2022/2555/2022-12-27>.
178. Vladymyr O. Strategic areas of Ukraine's national economy development under modern globalization transformation conditions. *Herald of Ternopil National Economic University*. 2019. № 3(93). P. 7–21. URL: <https://doi.org/10.35774/visnyk2019.03.007>.
179. Веретюк С., Пілінський В. Визначення пріоритетних напрямків розвитку цифрової економіки в Україні. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2016. № 2(42). С. 51–58. URL: <https://journals.dut.edu.ua/index.php/sciencenotes/article/view/591/545>.

180. Шиманська К. В., Бондарчук В. В. Пріоритетні напрями та механізми розвитку цифрової економіки в Україні. *Економіка, управління та адміністрування*. 2021. № 1(95). С. 17–22. URL: [https://doi.org/10.26642/ema-2021-1\(95\)-17-22](https://doi.org/10.26642/ema-2021-1(95)-17-22).
181. Боярчук Д., CASE Україна. Економічні пріоритети повоєнної України. 2023. 88 с. URL: https://case-ukraine.com.ua/content/uploads/2023/02/Economic_priorities_in-post-war_Ukraine_UKR_01.pdf.
182. Міцніший фундамент, вищий потенціал і швидше відновлення. Київ: М-во фінансів та М-во економіки України. 2024. 12 с. URL: <https://reformmatrix.mof.gov.ua/wp-content/uploads/2024/06/bila-kniga-ukr-fin.pdf>.
183. Maslii O., Maksymenko A. Digitalization as an object of economic security science. *Scientific opinion: Economics and Management*. 2024. № 2(86). URL: <https://doi.org/10.32782/2521-666x/2024-86-3>.
184. Статистична інформація. *Державна служба статистики України*. URL: <https://www.ukrstat.gov.ua/>.
185. Динаміка і структура споживання електроенергії в Україні. *Всеукраїнська Енергетична Асамблея*. URL: <https://uaea.com.ua/dysp/ee-cons.html>.
186. Maksymenko A. Real and potential threats to the digital economy in war. *Economic scope*. 2023. URL: <https://doi.org/10.32782/2224-6282/188-7>.
187. Бусел В. Великий тлумачний словник сучасної Української мови. Ірпінь : ВТФ «Перун», 2003. 1087 с.
188. The Economist. Cyberwarfare is becoming scarier. *The Economist*. URL: https://web.archive.org/web/20081209081836/http://www.economist.com/world/international/displaystory.cfm?story_id=E1_JNNRSVS.

189. IT 2023: що насправді відбувається з вітчизняним ринком. *Укрінформ*. URL: <https://www.ukrinform.ua/rubric-technology/3692904-it2023-so-naspravdi-vidbuvaetsa-z-vitciznanim-rinkom.html>.

190. Желюк Т. Економічна безпека в системі інституційного вектора збалансованого розвитку. *Вісник Тернопільського національного економічного університету*. 2013. № 1. С. 19–32.

191. Georgian economy continues rapid growth in Q2 2008. Tbilisi, Georgia : Department of Statistics of Georgia. 2008. 4 p. URL: https://www.gov.ge/files/34_272_580195_q2_08_real_gdp_growth_7.9_080924.pdf.

192. Keizer G. Cyberattacks knock out Georgia's Internet presence. *Computerworld*. URL: <https://www.computerworld.com/article/1564999/cyberattacks-knock-out-georgia-s-internet-presence.html>.

193. Georgia real GDP by industry U.S. 2023. *Statista*. URL: <https://www.statista.com/statistics/304946/georgia-real-gdp-by-industry/>.

194. Economic Indicators & Forecasts. *S&P Global*. URL: <https://www.spglobal.com/marketintelligence/en/mi/industry/economics-country-risk.html>.

195. 2023 Country Report – Estonia. Brussel, Belgium : European Commission. 2023. 74 p. URL: https://economy-finance.ec.europa.eu/system/files/2023-05/ET_SWD_2023_606_en.pdf.

196. Republic of Estonia: 2008 Article IV Consultation–Staff Report; Staff Statement; Public Information Notice on the Executive Board Discussion; and Statement by the Executive Director for the Republic of Estonia. Washington DC, U.S. : International Monetary Fund. 2009. 52 p. URL: <https://www.imf.org/external/pubs/ft/scr/2009/cr0986.pdf>.

197. Tucker M. China accused of hacking Ukraine days before Russian invasion. *The Times & The Sunday Times*. URL:

<https://www.thetimes.com/world/russia-ukraine-war/article/china-cyberattack-ukraine-z9gfkbmfgf>.

198. Russia: ICT services export value by type 2022. *Statista*. URL: <https://www.statista.com/statistics/1024850/russia-information-services-exports-value-by-type/>.

199. Onyshchenko S., Maslii O., Maksymenko A. The Threats of Ukraine Financial Security: Identification and Systemization. *Економіка і регіон*. 2019. № 2 (73). P. 73–80. URL: [https://doi.org/10.26906/EIP.2019.2\(73\).1629](https://doi.org/10.26906/EIP.2019.2(73).1629).

200. Systematization of Threats to Financial Security of Individual, Society, Business and the State in Terms of the Pandemic / V. Onyshchenko et al. *Proceedings of the 4th International Conference on Building Innovations : Lecture Notes in Civil Engineerin*. Cham, 2023. URL: https://doi.org/10.1007/978-3-031-17385-1_63.

201. Ptashchenko L., Berezhetska T., Maksymenko A. Small Business Simplification under Digitalization and Globalization Challenges: Teal Organizations Development. *Економіка і регіон*. 2019. № 4(75). P. 107–112. URL: [https://doi.org/10.26906/eir.2019.4\(75\).1858](https://doi.org/10.26906/eir.2019.4(75).1858).

202. Maslii O., Maksymenko A., Onyshchenko S. The Threats of Ukraine Financial Security: Identification and Systemization. *Економіка і регіон*. 2019. № 2(73). P. 73–80. URL: [https://doi.org/10.26906/eir.2019.2\(73\).1629](https://doi.org/10.26906/eir.2019.2(73).1629).

203. Жукова Л. М., Максименко А. П., Дерюга А. В. Сучасні тенденції цифрової трансформації національного господарства як чинник забезпечення економічної безпеки. *Investytsiyyi: praktyka ta dosvid*. 2024. № 8. С. 71–76. URL: <https://doi.org/10.32702/2306-6814.2024.8.71>.

204. Маслій О. А. Оцінювання впливу загроз на рівень економічної безпеки національної економіки : дисертація кандидата економічних наук / Полтав. нац. техн. ун-т ім. Юрія Кондратюка, Полтава, 2016.

205. Маслій О., Максименко А. Оцінка ризиків фінансовій безпеці бізнесу в умовах пандемії з використанням міжнародного досвіду.

Підприємництво і торгівля: тенденції розвитку : матеріали IV Міжнар. наук.-практ. конф. Одеса, 2021. С. 297–300.

206. Максименко А. П. Цифровізація економіки під час пандемії COVID-19: загрози та переваги гіг-праці. *матеріали III міжнародна науково-практична конференція Розвиток фінансового ринку в Україні: загрози, проблеми та перспективи*. Полтава, 2021. С. 65–67.

207. Маслій О., Максименко А. Неокейнсіанська модель виходу з кризи в умовах пандемії COVID-19. *Трансформація національної моделі фінансово-кредитних відносин: виклики глобалізації та регіональні аспекти* : матеріали VI Всеукр. наук.-практ. Конф. Ужгород, 2021. С. 27–28.

208. Максименко А. Вплив діджиталізації на подолання мовних та комунікативних бар'єрів. *Інформація та документ у сучасному науковому дискурсі* : Матеріали VII Всеукр. дистанц. науково-практ. Конф. Івано-Франківськ, 2022. С. 159–164.

209. Максименко А. Цифровізація України: переваги та загрози для розвитку молодіжного бізнесу. *Підприємництво і торгівля: тенденції розвитку* : матеріали V міжнар. науково-практ. конф. Одеса, 2022. С. 178.

210. Маслій О., Максименко А. Мінімізація загроз економічній безпеці України в умовах воєнного стану з використанням резервів цифровізації. *Сталий розвиток: виклики та загрози в умовах воєнного стану* : Зб. міжнар. науково-практ. інтернет-конф. Полтава, 2022. С. 153–155.

211. Маслій О. А., Максименко А. П. Загрози критичній цифровій інфраструктурі в умовах війни. *Економічна безпека: держава, регіон, підприємство* : матеріали Міжнар. науково-практ. Інтернет-конф Полтава, 2022. С. 144–148.

212. Максименко А. Загрози цифровій економіки спричинені криптовалютами. *Розвиток фінансового ринку в Україні: загрози, проблеми та перспективи* : Матеріали IV Міжнар. науково-практ. конф., Полтава, 2022. С. 45–48.

213. Максименко А., Маслій О. Chatgpt як інструмент діджиталізації економіки: переваги та загрози. *Розвиток фінансів, аудиту, бухгалтерського обліку та оподаткування: реалії часу* : II Міжнар. науково-практ. інтернет-конф. студентів, аспірантів та молодих вчен. пам'яті видат. укр. вченого-економ. Сергія Ілл. Юрія, Кам'янець-Подільський, 2023. С. 427–430.

214. Максименко А. П. Цифрова адаптивність небанківської фінансової складової економічної безпеки України. *Економіка, фінанси, банківська справа та освіта: актуальні питання розвитку, досягнення та інновації* : матеріали VIII Міжнар. науково-практ. Інтернет-конф. Одеса-Острів, 2023. С. 216–229.

215. Максименко А. Вплив цифровізації на формування та трансформацію загроз економічній безпеці держави. *Економічна безпека: держава, регіон, підприємство* : Матеріали IX Міжнар. науково-практ. Конф. Полтава, 2025. С. 204–207.

216. Maksymenko A. The role of technological optimism in digitalisation of the Ukrainian economy. *Modern Scientific Views on the Development of the World Economy and International Cooperation*. 2023. P. 95–99. URL: <https://doi.org/10.30525/978-9934-26-356-9-27>.

217. Pavlova O., Maksymenko A. Directions of modern development of the it sphere in Ukraine. *Impact of Artificial Intelligence and Other Technologies on Sustainable Development* : Proceedings of the 1st International Scientific and Practical Internet Conference. Dnipro, 2023. P. 26–29.

218. Максименко А. Transnational instruments to ensure the security of the EU digital economy. *«Реформування економіки в контексті міжнародного співробітництва: механізми та стратегії»* : матеріали доп. Міжнар. науково-практ. Конф. Львів-Торунь, 2024. С. 37–41.

219. Максименко А. Специфіка безпекових ризиків України в загальносвітових обставинах. *Наукові стратегії в контексті глобальних викликів* : матеріали I-ої Міжнар. науково-практ. конф. Київ, 2024. С. 74–76.

220. Максименко А. Діджиталізація медіа та дезінформація як загрози економічній безпеці держави. *Економічна безпека: держава, регіон, підприємство* : Матеріали VIII Міжнар. науково-практ. конф. Полтава, 2024. С. 146–150.
221. Clark B.B., Robert C., Hampton S. A. The technology effect: how perceptionsof technology drive excessive optimism. *Journal of business and psychology*. 2015.Vol. 31, no. 1. P. 87–102. URL: <https://doi.org/10.1007/s10869-015-9399-4>.
222. Digitalization of the Ukrainian economy during a state of war is a necessity of the time / L. Verbivska et al. *Revista Amazonia Investiga*. 2023. Vol. 12, № 68. P. 184–194. URL: <https://doi.org/10.34069/ai/2023.68.08.17>.
223. DESA, DPADM. The United Nations E-Government Knowledgebase. *EGOVKB | United Nations*. URL: <https://publicadministration.un.org/egovkb/en-us/Data-Center>.
224. World Bank Open Data. *World Bank*. URL: <https://data.worldbank.org/>.
225. Freedom On The Net 2024 The Struggle for Trust Online. Washington DC, U.S.: Freedom House, 2024. 45 p. URL: <https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf>.
226. Maslii O., Maksymenko A. Digital Transformation and Economic Deindustrialisation: Impact on State Financial Security. *Financial and credit activity problems of theory and practice*. 2025. Vol. 1, № 60. P. 401–414. URL: <https://doi.org/10.55643/fcaptp.1.60.2025.4599>.
227. IMD's World Competitiveness Center. World Digital Competitiveness Ranking. Lausanne : Institute Management Development, 2024. 214 p. URL: <https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/>.
228. Офіційні відомості та соціальні дослідження групи «Рейтинг». *Соціологічна група «Рейтинг»*. URL: <https://ratinggroup.ua/>.

229. Дослідження цифрових навичок українців. Київ: М-во цифрової трансформації України.. URL: <https://osvita.diia.gov.ua/research>.
230. Рівень безробіття в Україні становить 30% - Мінекономіки. *Укрінформ*. URL: <https://www.ukrinform.ua/rubric-economy/3654271-riven-bezrobitta-v-ukraini-stanovit-30-minekonomiki.html>.
231. IMF ranks Ukraine as Europe's poorest country. *IMF. Business news*. URL: <https://www.intellinews.com/imf-ranks-ukraine-as-europe-s-poorest-country-150301/>.
232. Standard & Poor's. Кредитні рейтинги державних цінних паперів - 2024. *Міністерство Фінансів України*. URL: https://mof.gov.ua/uk/credit_ratings_2019-345.
233. Eurostat. Usage of AI technologies increasing in EU enterprises. *European Commission*. URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250123-3?utm_source=chatgpt.com.
234. Геєць В. М., Семиноженко В. П. Інноваційні перспективи України : монографія. Харків : Константа, 2006. 272 с.
235. Жаліло Я. До формування категоріального апарату науки про економічну безпеку. *Стратегічна панорама*. 2004. № 3. С. 97–104.
236. Пастернак-Таранущенко Г. Економічна безпека держави: проблеми та механізми їх розв'язання. *Вісник НАН України*. 1998. № 11-12. С. 67–71.
237. Шлемко В., Бінько І. Економічна безпека України: сутність і напрямки забезпечення : монографія. К. : Видво НІСД, 1997. 144 с.
238. Мунтіян В. Економічна безпека України. Київ : КВШ, 1998. 462 с.
239. Бондарук Т. Г., Бондарук І. С. Соціальні аспекти економічної безпеки держави. *Економічні горизонти*. 2018. № 2. С. 76–86.
240. Губський Б. Економічна безпека: методологія виміру, стан і стратегія забезпечення. К. : Укрархбудінформ, 2001. 122 с.
241. Єрмошенко М. Фінансова безпека держави: національні інтереси, реальні загрози, стратегія забезпечення. Київ : КНТЕУ, 2001.

242. Давиденко С. Економіка та економічна безпека держави. Теорія та практика : монографічний навчальний посібник. Ужгород, 2017. 390 с.
243. Рожков В. Підходи до визначення сутності поняття економічної безпеки. *Вісник Миколаївського національного університету імені В.О. Сухомлинського*. 2016. Т. 10. С. 478–480.
244. Чубукова О., Воронкова Т. Система економічної безпеки (екосистейт): сутність, структура. *Ефективна економіка*. 2014. № 2. URL: http://nbuv.gov.ua/UJRN/efek_2014_2_82.
245. Уманців Ю. М., Міняйло О. І. Економічна політика держави за умов глобальних трансформацій. *Економіка України*. 2018. № 9. С. 37–49. URL: http://nbuv.gov.ua/UJRN/EkUk_2018_9_5.
246. Романчик Т. В. Небезпека, загроза, ризик: аналіз термінологічного апарату теорії економічної безпеки. *Економічний вісник НТУУ «КПІ»*. 2020. № 17. С. 257–267.
247. Предборський В. Економічна безпека держави : монографія. Київ : Кондор, 2005. 391 с.
248. Дідович І., Фабін І. Формування економічної безпеки держави та регіону. *Науковий вісник НЛТУ України*. 2009. № 19. С. 152–158.
249. Мігус І. П., Лаптева С. М. Необхідність розмежування понять «загроза» та «ризик» при діагностиці економічної безпеки суб'єктів господарювання. *Ефективна економіка*. 2011. № 12. URL: http://nbuv.gov.ua/UJRN/efek_2011_12_5.
250. Цікановська Н. Інтерпретація понять «виклик», «небезпека», «загроза» та «ризик» у теорії фінансової безпеки. *Фінансовий простір*. 2013. № 3(11). С. 110–114.
251. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект. К. : Атіка, 2005. 432 с.
252. Плетнікова І. Л. Визначення рівня і забезпечення економічної безпеки залізниці: автореф. дис. на здобуття наук ступня канд. екон. наук: спец. 08.07.04 «Економіка транспорту і зв'язку». Х. : Харків. держ. акад. залізн. трансп., 2001.

253. Дмитрова О. Класифікація загроз та ризиків економічної безпеки банку. *Ефективна економіка. Серія «Економічні науки»*. 2015. № 11. URL: <http://www.economy.nayka.com.ua/?op=1&z=2544..>
254. Білько С. С. Формування інформаційної безпеки національної економіки : дисертація доктора філософії / Полтава : НУПП, 2023. 211 с.
255. Черв'як А. В. Економічна безпека фінансово-кредитних установ : дисертація доктора філософії/. Полтава : НУПП, 2022. 255 с.
256. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union : of 07.06.2016 № 12016ME. *Official Journal of the European Union*. 2016. 7 June. P. 1–388. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12016ME/TXT>.
257. Паніотто В. І., Максименко В. С., Харченко Н. М. Статистичний аналіз соціологічних даних. К: Вид. дім «КМ Акад.», 2004. 270 с.
258. Максименко А.П. Пріоритетні напрями запобігання загрозам економічної безпеки України в умовах цифровізації. *Цифрова економіка та економічна безпека*. 2025. Випуск 2(17).URL: <https://doi.org/10.32782/dees.17-21>
259. RICE: Simple prioritization for product managers. *The Intercom Blog*. URL: <https://www.intercom.com/blog/rice-simple-prioritization-for-product-managers/>.
260. Gonzalez D. L. E. How to Become an Extraordinary Manager. Bloomington, Indiana, U.S. : Author House, 2011. 192 p.
261. Attractive quality and must-be quality / N. Kano et al. *Journal of the Japanese Society for Quality Control*. 1984. Vol. 14, no. 2. P. 39–48.
262. . Digital Transformation Index. 2021. *European Business Association* URL: <https://eba.com.ua/en/zaregulovanist-brak-koshtiv-ta-nyzka-tsyfrova-gramotnist-strymuyut-tsyfrovu-transformatsiyu-v-ukrayini-doslidzhennya-eva/>.
263. Індекс цифрової трансформації регіонів України. Київ : М-во цифр. Трансформації, 2022. 99 с. URL: <https://backend.hromada.gov.ua/storage/uploads/files/research/indeks->

cifrovoyi-transformaciyi-regioniv-ukrayini-

2022/Індекс%20ЦТ_v2.pdf?time=1745222202288.

264. Індекс цифрової трансформації регіонів України. Київ : М-во цифр. Трансформації, 2023. 26 с.

265. Індекс цифрової трансформації регіонів України. Київ : М-во цифр. Трансформації, 2024. 28 с.
URL: <https://thedigital.gov.ua/storage/uploads/files/page/community/reports/%D0%86%D0%9D%D0%94%D0%95%D0%9A%D0%A1%202024%202%201.pdf>

266. Digital Economy and Society Index (DESI) 2021. Shaping Europe's digital future. URL: <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021>

267. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV : станом на 1 січ. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>

268. 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*. 2022. №181. P. 749–759. URL: https://doi.org/10.1007/978-3-030-85043-2_69

269. Yehorycheva S., Hlushko A., Khudolii Y. Issue of Ukrainian financial sector information security. *Управління розвитком*. 2023. Вип. 21. № 4. С. 45-52. URL: <https://doi.org/10.57111/devt/4.2023.45>

270. Кулик В. Управління економічною безпекою бізнесу: концептуальні засади. *Економіка і регіон*. 2025. № 1 (96). С. 255–260. URL: [https://doi.org/10.26906/EiR.2025.1\(96\).3772](https://doi.org/10.26906/EiR.2025.1(96).3772)

271. Кулик В., Похідня Б., Інформаційний менеджмент на підприємстві. *Економічний простір*. 2025. №201. С. 96–99. URL: <https://doi.org/10.30838/ep.201.96-99>

272. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

273. Impact of digitalization of the economy on transformation of the labor market: opportunities and threats / G. Nazarova et al. *Financial and credit activity problems of theory and practice*. 2024. Vol. 3, no. 56. P. 459–473. URL: <https://doi.org/10.55643/fcaptp.3.56.2024.4391>

274. Про Бюро економічної безпеки України : Закон України від 28.01.2021 № 1150-IX : станом на 30 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/1150-20#Text>

275. Digital technologies in hr management / Y. Sotnikova et al. *Management theory and studies for rural business and infrastructure development*. 2021. Vol. 42, no. 4. P. 527–535. URL: <https://doi.org/10.15544/mts.2020.54>

276. Пахненко О. М., Чжан К. Підвищення ефективності міжнародного бізнесу за допомогою цифрових технологій. *Economic synergy*. 2024. № 3. С. 49–62. URL: <https://doi.org/10.53920/es-2024-3-3>

277. Пахненко О. М., Мордань Є. Ю., Божко М. О. Оцінювання перспективних напрямків цифрової трансформації економіки країни. *Цифрова економіка та економічна безпека*. 2024. № 5 (14). С. 259–264. URL: <https://doi.org/10.32782/dees.14-43>

278. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода Україна від 27.06.2014 : станом на 30 листоп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

279. Світлана Б. Є., Кучер А. В. Наукові підходи до ідентифікації загроз економічній безпеці галузі промисловості. *Zenodo*. 2025. URL: <https://doi.org/10.5281/zenodo.15088141>

280. Khudolii Y., Hlushko A. The impact of innovation and fintech on the banking business. *ScienceRise*. 2023. No. 3. P. 41–50. URL: <https://doi.org/10.21303/2313-8416.2023.003218>

ДОДАТКИ

Додаток А

Таблиця А.1

Підходи до трактування категорії «цифровізації»

Автори	Визначення
1	2
Техніко-форматний підхід	
О.В. Абакуменко [4]	Процес переведення певного інформаційного поля з аналогового у цифровий формат для більш легкого подальшого використання на сучасних електронних девайсах.
Л. Лігоненко [12]	Процес перенесення інформації у цифрову форму, тобто перетворення паперових книжок у електронні, фотографії у зображення на екрані тощо.
Комерційно-оптимізаційний підхід	
О.Є. Гудзь, С.А. Федюнін [19]	Заснований на можливостях сучасної ІТ-індустрії процес застосування бізнесом сучасних інформаційно-комунікаційних технологій для досягнення своєї мети, зорієнтований на трансформацію існуючих бізнес-процесів шляхом їх діджиталізації.
О.М. Грибіненко [20]	Трансформація, проникнення цифрових технологій щодо оптимізації та автоматизації бізнес-процесів, підвищення продуктивності та покращення комунікації зі споживачами.
А.В. Гуренко [21]	Процес використання цифрових технологій з одночасним поліпшенням системи обслуговування клієнтів.
Ж.-П. де Клерк [14]	Використанні цифрових технологій та даних з метою одержання прибутку, поліпшення бізнесу, зміни/трансформації бізнес-процесів та створення належного середовища для їх реалізації, в основі якого – використання цифрової інформації.
Т. Оноре [16]	Протилежна «цифровій революції», адже вона спрямована «всього лише» на автоматизацію тих робочих процесів, які раніше виконувалися вручну.
І.В. Струтинська [11]	Це перехід бізнесу на нові технології орієнтований на користувача, що прискорюють та спрощують взаємодію, підвищують якість наданих послуг та дають змогу моделювати поведінку клієнтів і все більше підвищувати якість обслуговування. Збільшує ефективність компаній та змінюють усталені бізнес-моделі.
А. Семилітко [13]	Перехід організації до нових способів мислення й роботи на базі використання соціальних, мобільних та інших цифрових технологій; зміну стилю управління, систем заохочення і прийняття нових бізнес-моделей на протигагу діджитал-трансформації, яку вважає масштабною трансформацією бізнесу, що передбачає використання цифрових технологій для оптимізації бізнес-процесів, підвищення продуктивності компанії й поліпшення досвіду взаємодії з клієнтами»
М.С. Міхровська [24]	Автоматизація більшості процесів у сфері публічного управління для більш зручного та швидкого спілкування між державою та громадянином.

Продовження табл. А.1

Технологічно-інформаційний підхід	
1	2
Український інститут майбутнього [10]	Це впровадження цифрових технологій в усі сфери життя: від взаємодії між людьми до промислових виробництв, від предметів побуту до дитячих іграшок, одягу тощо. Це перехід біологічних та фізичних систем у кібербіологічні та кіберфізичні, тобто об'єднання фізичних та обчислювальних компонентів. Перехід діяльності з реального матеріально-виробничого світу у світ віртуальних сервісів та онлайн-технологій
С.Я. Король [22]	Передбачає створення системи збору, зберігання і аналізу даних, оптимізацію пошуку інформації з використанням Інтернету, обробку великих масивів даних, застосування штучного інтелекту, Інтернет речей у виробництві та інші складові.
Оксфордський словник англійської мови [23]	Запровадження або збільшення використання організаціями, в певній галузі, країні тощо цифрових і комп'ютерних технологій.
В.С. Куйбіда, О.В. Карпенко, В.В. Наместнік [15]	Процес впровадження цифрових технологій для вдосконалення життєдіяльності людини, суспільства і держави.
С. Лукін [17]	Характеризується волею сучасного суспільства до віртуальної комунікації, зміни форм і стилю суспільновладних взаємовідносин, що обумовлює включення державно-управлінських структур у віртуальне середовище та зміну форм управління, зокрема впровадження онлайн платформ життєдіяльності громад.
В. В. Наместнік, М. М. Павлов [18]	Процес створення та використання нових, цифрових за замовчуванням, інтероперабельних, стандартизованих інформаційних систем у публічному управлінні, які дають змогу не лише оцифрувати й автоматизувати наявні управлінські процеси за допомогою електронних інструментів, а й визначати певні «критичні точки» управлінського процесу, співвідношення між ними та приймати рішення з їх урахуванням.

Джерело: систематизовано автором на основі [4, 10-24]

Таблиця А.2

Підходи до трактування категорії «економічна безпека»

Автори	Визначення
1	2
Л. Акімова [42]	Стан захищеності підсистем: фінансової, соціально-економічної, техніко-технологічної і тощо. Це динамічна складова частина економіки, яка адаптується до вимог часу. Нині під цим поняттям розуміють стан, у якому такі складники, як: фінансова, інформаційна, соціально-економічна, інституційно-правова, техніко-технологічна, інтелектуально-кадрова, силова та екологічна діяльність – перебувають у стані захищеності, збереження, надійності, стабільності, спокою, незалежності. Це комплекс дієвих заходів офіційних державних органів, які забезпечують стійкість до зовнішніх та внутрішніх загроз.

Продовження табл. А.2

1	2
В. Гесць [234]	Стан економіки, суспільства та інститутів державної влади, при якому забезпечується реалізація та гарантований захист національних економічних інтересів, прогресивний соціально-економічний розвиток країни
Я. Жаліло [235]	Складна багатофакторна категорія, що характеризує здатність національної економіки до розширеного самовідтворення з метою задоволення на визначеному рівні потреб власного населення і держави, протистояння дестабілізуючій дії чинників, що створюють загрозу нормальному розвитку країни, забезпечення конкурентоспроможності національної економіки у світовій системі господарювання.
З. Варналій, Д. Буркальцева, О. Саєнко [43]	Сукупність форм і методів узгодження різних інтересів суб'єктів економіки, що дозволяє вирішувати конфлікти з найменшими витратами та з використанням найменш руйнівного для економіки способу.
Г.Пастернак- Таранущенко [236]	Стан держави, за якого вона забезпечена можливістю створення і розвитку розуму для плідного життя її населення, перспективного розвитку її економіки в майбутньому, та зростання добробуту її мешканців.
В. Шлемко [237]	Стан економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз і здатний задовольнити потреби особи, сім'ї, суспільства, держави.
В. Мунтіян [238]	Загальнонаціональний комплекс заходів, спрямованих на постійний та стабільний розвиток економіки держави, що містить механізм протидії внутрішнім і зовнішнім загрозам.
Методика Міністерства економіки [30]	Стан національної економіки, який дає змогу зберігати стійкість до внутрішніх і зовнішніх загроз, і здатний задовольняти потреби особи, сім'ї, суспільства та держави.
Т. Бондарук [239]	Це складна багатофакторна категорія, яка дозволяє зберігати стійкість до зовнішніх та внутрішніх загроз, характеризує здатність національної економіки до розширеного самовідтворення для задоволення потреб громадян, суспільства і держави на якомусь визначеному рівні.
Б. Губський [240]	Це можливість і готовність економіки забезпечити достатні умови життя і розвитку особи, соціально-економічну і військово-політичну стабільність суспільства і держави, протидіяти впливу внутрішніх і зовнішніх загроз
М. Єрмошенко [241]	Характеризується збалансованістю і стійкістю до негативного впливу внутрішніх і зовнішніх загроз, здатністю забезпечувати на основі реалізації національних економічних інтересів сталий і ефективний розвиток вітчизняної економіки і соціальної сфери.
С. Давиденко та ін. [242]	Специфічна «випереджувальна похідна» від економічного та політичного курсу держави, де різні її види реалізуються за допомогою відмінних, а у деяких випадках – протилежних заходів.

Продовження табл. А.2

1	2
В. Рожков [243]	Має трактуватися різнобічно: по-перше, через характеристику стану системи, а саме: стійкість, стабільність тощо; по-друге, через здатність протидіяти внутрішнім та зовнішнім загрозам; по-третє, через можливість повноцінної реалізації всіх функцій суб'єкта господарювання; по-четверте, через повноцінне забезпечення усіма необхідними ресурсами та їх використання у виробничо-господарській діяльності.
О. Чубукова Т. Воронкова [244]	Інтегральна категорія, у предметну сферу якої входять поняття різних рівнів ієрархії, а також функціональних сфер економіки, які за взаємодії і взаємозумовленості виражають економічні відносини між суб'єктами міжнародних утворень, державою, регіонами, підприємствами, організаціями, установами, господарствами та окремими особистостями та всередині цих підсистем і елементів із приводу досягнення такого рівня розвитку економіки, за якого здійснюється задоволення потреб і гарантований захист інтересів усіх суб'єктів економіки.

Джерело: систематизовано автором на основі [30; 42-44; 234-244]

Таблиця А.3

Підходи до трактування категорії «загроза»

Автор	Визначення
Т. Ганущак [33]	Дія дестабілізуючих природних факторів і/або суб'єктивних, пов'язаних з недобросовісною конкуренцією та порушенням.
Закон України про національну безпеку [31]	Явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.
З. Варналій, Д. Буркальцева, О. Сасенко [43]	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 унеможливають реалізацію стратегічних національних економічних інтересів і породжують небезпеку для політичної та соціально-економічної системи, життєзабезпечення нації, національних цінностей та кожного громадянина.
О. Міняйло Ю. Уманців [245]	Наявні чи потенційні дії, що ускладнюють або унеможливають реалізацію національних економічних інтересів і створюють небезпеку для соціально-економічної та політичної систем, національних цінностей, життєзабезпечення нації та окремої особи.
Л. Шемаєва [36]	Сукупність наявних і потенційно можливих явищ та чинників, що призводять до порушення процесу формування й розподілу централізованих фондів держави та, як наслідок, дестабілізації банківської системи, знецінення національної валюти й дефолту за суверенними боргами.

Продовження табл. А.3

1	2
Е. Олейніков, Н. Матвеев, А. Пекін [39]	Найбільш конкретна і безпосередня форма небезпеки або сукупність умов і чинників, що створюють небезпеку інтересам різних суб'єктів.
В. Мунтіян [238]	Здатність заподіяти шкоду, вчинити фізичні, майнові чи моральні (духовних) збитки державі, особистості або суспільству.
Т. Романчик [246]	Дія, що підвищує ймовірність небезпеки, наближуючи її до конкретних негативних результатів.
В. Предборський [247]	Це намір будь-якого характеру, можливість здійснити фізичну, моральну, матеріальну чи будь-яку іншу шкоду інтересам суспільства чи особистим.
І. Дідович [247]	Це спектр певних чинників та умов, котрі продукують небезпеку особистості та її інтересам, державі, суспільству, значно ускладнюють або взагалі унеможливають виконання національних економічних інтересів.
І. Мігус, С. Лаптева [249]	Являє собою певну подію, що впливає на діяльність суб'єктів господарювання, тоді як «ризик» виступає результатом впливу загроз на господарську діяльність суб'єктів господарювання.
О. Пугач [45, 2]	Сукупність викликів, ризиків, чинників та умов, що унеможливають та / або перешкоджають стабільному функціонуванню економічної системи держави, створюють небезпеку національним економічним інтересам, цінностям та основним соціально-економічним пріоритетам та «упередження загроз економічній безпеці національної економіки» як процесу реалізації уповноваженими органами державної влади та іншими суб'єктами економічної безпеки держави системи заходів, спрямованої на протидію поширенню загроз з метою запобігання їхнього негативного впливу на національну економіку:
Н. Цікановська [250]	Сукупність деструктивних та дестабілізуючих чинників зовнішнього середовища.
М. Камлик [251]	Це потенційні або реальні умови, чинники чи дії фізичних та юридичних осіб, що порушують нормальний фінансово-економічний стан підприємницької діяльності і здатні заподіяти великої шкоди аж до припинення його діяльності.
І. Плетнікова [252]	Найбільш конкретна і безпосередня форма небезпеки, коли для суб'єкта економічних відносин обов'язково настануть несприятливі наслідки, якщо не застосовувати ніяких заходів для їх запобігання.

Джерело: систематизовано автором на основі [31; 33; 36; 39; 45; 204; 238; 244-252]

Додаток Б

Таблиця Б.1

Центральні дослідження для формування кластерів методом графів

Тип загрози	Дослідження	Скорочення
Adverse outcomes of AI technologies (Загрози ШІ)	Ugwudike P. AI audits for assessing design logics and building ethical systems: the case of predictive policing algorithms. <i>AI and Ethics</i> . 2021. Vol. 2, № 1. P. 199–208. URL: https://doi.org/10.1007/s43681-021-00117-5 .	AI
Adverse outcomes of frontier technologies (Загрози передових технологій)	Clark B. B., Robert C., Hampton S. A. The Technology Effect: How Perceptions of Technology Drive Excessive Optimism. <i>Journal of Business and Psychology</i> . 2015. Vol. 31, № 1. P. 87–102. URL: https://doi.org/10.1007/s10869-015-9399-4 .	AOFT
Censorship and surveillance (Цензура та обмеження)	Tanczer L. M., McConville R., Maynard P. Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics. <i>Journal of Global Security Studies</i> . 2016. Vol. 1, № 4. P. 346–355. URL: https://doi.org/10.1093/jogss/ogw016 .	CS
Cyber espionage and warfare (Цифровий шпівонаж та ківбервійни)	Rosli W. R. W. Waging warfare against states: the deployment of artificial intelligence in cyber espionage. <i>AI and Ethics</i> . 2025. URL: https://doi.org/10.1007/s43681-024-00628-x .	CEW1
	Devanny J., Martin C., Stevens T. On the strategic consequences of digital espionage. <i>Journal of Cyber Policy</i> . 2021. Vol. 6, № 3. P. 429–450. URL: https://doi.org/10.1080/23738871.2021.2000628 .	CEW2
Misinformation and disinformation (Дезінформація та введення в оману)	Yan C., Pu K., Luo X. Knowledge mapping of information cocoons: A bibliometric study using visual analysis. <i>Journal of Librarianship and Information Science</i> . 2024. URL: https://doi.org/10.1177/09610006231222628 .	MD
Online harms (Онлайн-насильство)	Bright J. et al. Understanding engagement with platform safety technology for reducing exposure to online harms //arXiv preprint arXiv:2401.01796. – 2024. URL: https://doi.org/10.48550/arXiv.2401.01796 .	OH

Джерело: систематизовано автором на основі [87]

Таблиця Б.2

Посилання на сформовані кластери інструментом Connected Papers [228]

Скорочення загрози	URL кластера Connected Papers
AI	AI audits for assessing design logics and building ethical systems: the case of predictive policing algorithms. Connected Papers. URL: https://www.connectedpapers.com/main/e90b71fa55769fe3e94ad214b35b319d3968f9d2/AI-audits-for-assessing-design-logics-and-building-ethical-systems:-the-case-of-predictive-policing-algorithms/graph .
AOFT	The Technology Effect: How Perceptions of Technology Drive Excessive Optimism. Connected Papers. URL: https://www.connectedpapers.com/main/42245bf0847ac88206d7389a3e87d8b8b31bcc5e/The-Technology-Effect%3A-How-Perceptions-of-Technology-Drive-Excessive-Optimism/graph .
CS	Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics. Connected Papers. URL: https://www.connectedpapers.com/main/d661549d8e9486dc6aa215441de808f1c7de7c17/Censorship-and-Surveillance-in-the-Digital-Age%3A-The-Technological-Challenges-for-Academics/graph .
CEW1	Waging warfare against states: the deployment of artificial intelligence in cyber espionage. Connected Papers. URL: https://www.connectedpapers.com/main/586f6cd3f41eb04fc3bbf412f5eca2eea05f77c0/Waging-warfare-against-states%3A-the-deployment-of-artificial-intelligence-in-cyber-espionage/graph .
CEW2	On the strategic consequences of digital espionage. Connected Papers. URL: https://www.connectedpapers.com/main/848ba4d1b6c5c52a349992d951c6290cad219f66/On-the-strategic-consequences-of-digital-espionage/graph .
MD	Knowledge mapping of information cocoons: A bibliometric study using visual analysis. Connected Papers. URL: https://www.connectedpapers.com/main/e374436d455492cc40242b98f9b27082b013aab6/Knowledge-mapping-of-information-cocoons%3A-A-bibliometric-study-using-visual-analysis/graph .
OH	Understanding engagement with platform safety technology for reducing exposure to online harms. Connected Papers. URL: https://www.connectedpapers.com/main/8842309561eccc6175dc00c06aee50f86376f2a1/Understanding-engagement-with-platform-safety-technology-for-reducing-exposure-to-online-harms/graph .

Джерело: систематизовано автором на основі [87]

Додаток В

Таблиця В.1

Ранжування відхилення від критичного значення показника складової інтегральної оцінки рівня безпеки національній економіці України станом на 2021-2022 роки

Загроза	Значення	Загроза	Значення
1	2	3	4
Енергоємність ВВП, кг умовного палива/грн.	0	Частка населення із середньодушовими еквівалентними загальними доходами у місяць, нижчими 75 відсотків медіанного рівня загальних доходів, %	0,8133333
Індекс ЕМВІ+Україна	0	Різниця між процентними ставками за кредитами, наданими депозитними корпораціями у звітному періоді резидентам України, та процентними ставками за депозитами, залученими депозитними установами, в.п.	0,8181818
Рівень волатильності індексу ПФТС, кількість критичних відхилень (-10%)	0	Рівень доларизації грошової маси, %	0,84
Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу, %	0	Добова калорійність харчування людини, тис. ккал	0,8404931
Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу: Олія, %	0,075436	Відкритість економіки (відношення обсягу експорту та імпорту товарів та послуг до ВВП), %	0,877
Ступінь зносу основних засобів промисловості, %	0,082645	Частка споживчих кредитів, наданих домогосподарствам, у загальній структурі кредитів, наданих резидентам	0,8904762
Відношення експорту роялті, ліцензійних послуг, комп'ютерних та інформаційних послуг, наукових та конструкторських розробок, послуг в архітектурних, інженерних та інших технічних галузях % до ВВП	0,083333	Частка продажу імпортованих продовольчих товарів через торговельну мережу підприємств, відсотки	0,896

Продовження табл. В.1

1	2	3	4
Ступінь зносу основних засобів на підприємствах транспорту та зв'язку, %	0,10989	Рівень зайнятості населення у віці 15-70 років, у відсотках до населення відповідної вікової групи	0,8976661
Сальдо купівлі-продажу населенням іноземної валюти, млрд. доларів США	0,125	Частка витрат на продовольчі товари у споживчих грошових витратах домогосподарств, %	0,91
Частка імпорту палива з однієї країни (компанії) у загальному обсязі його імпорту, %	0,148333	Індекс зміни офіційного курсу національної грошової одиниці до долара США, середній за період	0,9115385
Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу: Картопля, %	0,205128	Відношення офіційних міжнародних резервів до валового зовнішнього боргу, %	0,9174312
Рівень середньозваженої процентної ставки за кредитами, наданими депозитними корпораціями (крім Національного банку) в національній валюті, відносно індексу споживчих цін, в. п.	0,242857	Очікувана тривалість життя при народженні, років	0,9428571
Сума заборгованості з виплати заробітної плати у відсотках до фонду оплати праці	0,25	Частка активів 5-ти найбільших банків у сукупних активах банківської системи, %	0,9683333
Частка осіб, які повідомили, що за останні 12 місяців користувалися послугами Інтернету (обстеження домогосподарств)	0,25	Знос основних виробничих фондів підприємств паливно- енергетичного комплексу, %	0,9714286
Відношення середньомісячної номінальної зарплати до прожиткового мінімуму на одну працездатну особу, разів	0,267857	Частка населення похилого віку у загальній кількості населення (станом на 1.01. наступного року), % (коефіцієнт старіння)	0,992
Виробництво зерна на одну особу на рік, тонн	0,285714	Відношення середньої вартості 1 м ² житла до середньомісячної заробітної плати, рази	1
Рентабельність активів, %	0,285714	Деіндустріалізація реального сектору внаслідок діяльності підприємств ІКТ	1

Продовження табл. В.1

1	2	3	4
Частка імпорту у внутрішньому споживанні країни, %	0,289017	Пастка середніх доходів, в тому числі для спеціалістів з ІКТ	1
Сутнісна зміна предметів ринкової діяльності створює ринкову турбулентність	0,3	Відношення вартості нововведених основних засобів до обсягу капітальних інвестицій, %	1,0242086
Відношення середньомісячної заробітної плати, нарахованої в середньому за оплачену годину, у країнах ЄС-27 та в Україні, рази	0,30303	Відношення наявного доходу населення до ВВП, %	1,0507692
Частка відновлювальних джерел у первинному постачанні енергії	0,30303	Рівень "тінізації" економіки, % до ВВП	1,0666667
Урожайність основних зернових та зернобобових культур, ц з 1 га площі збирання	0,327511	Чисельність наявного населення, % до рівня 1990 року	1,070529
Питома вага підприємств, що впроваджували інновації, у загальній кількості промислових підприємств, %	0,33557	Рівень безробіття (за МОП), %	1,1
Рентабельність операційної діяльності підприємств транспорту та зв'язку, %	0,350649	Рівень перерозподілу ВВП через зведений бюджет, %	1,1324324
Запаси природного газу, місяці споживання	0,357143	Внутрішні витрати на виконання НДР за рахунок коштів державного бюджету, % від ВВП	1,1428571
Різниця індексу ВДВ промисловості України та Китаю, в.п.	0,364078	Середньозважена дохідність облігацій внутрішньої державної позики (ОВДП) на первинному ринку, %	1,1545455
Валові міжнародні резерви України, у місяцях імпорту	0,384615	Відношення обсягу валового зовнішнього боргу до ВВП, %	1,1657143
Рентабельність операційної діяльності підприємств будівництва, %	0,416667	Індекс світової торгівлі (умов торгівлі) ціновий	1,1988717
Різниця між темпами росту середньомісячної заробітної плати та продуктивності праці в Україні, в. п.	0,416667	Утворення цифрового тіньового сектору економіки; поширення транскордонної злочинності	1,2
Частка високотехнологічної продукції в загальному обсязі реалізованої промислової продукції, %	0,434783	Питома вага обсягу виконаних наукових і науково-технічних робіт у ВВП, %	1,2195122

Продовження табл. В.1

1	2	3	4
Відношення середнього розміру пенсії за віком до прожиткового мінімуму осіб, які втратили працездатність, разів	0,454545	Співвідношення банківських кредитів та депозитів в іноземній валюті	1,2224939
Рівень імпортої залежності за домінуючим ресурсом у загальному постачанні первинної енергії, %	0,456667	Коефіцієнт покриття експортом імпорту (відношення між обсягами експорту та імпорту товарів та послуг), разів	1,2318841
Питома вага провідного товару (товарної групи) за виключенням енергетичного імпорту у загальному обсязі імпорту товарів, %	0,475	Співвідношення довгострокових (понад 1 рік) кредитів та депозитів, разів	1,2333333
Трудомісткість промислового виробництва, %	0,481928	Рентабельність операційної діяльності промислових підприємств, %	1,25
Надмірний технологічний оптимізм	0,5	Рівень проникнення страхування (страхові премії до ВВП), %	1,25
Сальдо поточного рахунку платіжного балансу України, % до ВВП	0,5	Відношення обсягу державного та гарантованого державою боргу до ВВП, %	1,2966667
Тривале безробіття (безробітні понад 12 міс. до заг. кількості безробітних)	0,502	Індекс інвестиційної сприятливості бізнес-середовища	1,305483
Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу: Овочі та продовольчі баштанні, %	0,52597	Кількість спеціалістів, які виконують науково-технічні роботи, до кількості зайнятого населення (на 1000 осіб)	1,3586957
Обсяг видатків зведеного бюджету на освіту, відсотки до ВВП	0,535714	Чисельність віл інфікованих, з діагнозом, що встановлений вперше в житті, осіб на 100 тис. населення	1,4066667
Ступінь зносу основних засобів у сільському господарстві, мисливстві, лісовому господарстві, %	0,548	Питома вага сировинного та низького ступеня переробки експорту (промисловості) у загальному обсязі експорту товарів, %	1,4583333
Частка кредитів в іноземній валюті у загальному обсязі наданих кредитів, %	0,554	Валове нагромадження основного капіталу, % ВВП	1,5517241

Продовження табл. В.1

1	2	3	4
Чисельність хворих на активний туберкульоз, з діагнозом, що встановлений вперше в житті, осіб на 100 тис. населення	0,571667	Питома вага реалізованої інноваційної продукції в обсязі промисловості, %	1,5789474
Середній річний удій молока від однієї корови, кг	0,581959	Рівень запасів зернових культур на кінець періоду, відсотки від споживання	1,581
Співвідношення ліквідних активів до короткострокових зобов'язань, %	0,582072	Співвідношення імпоротної ціни на газ в Україні та Європі, разів	1,5833333
Питома вага провідної країни - партнера в загальному обсязі експорту товарів, %	0,604	Рівень злочинності (кількість злочинів на 100 тис. населення), тис.	1,6166282
Обсяг легального відпливу фінансових ресурсів за межі країни, млрд. дол. США	0,613333	Загальний коефіцієнт міграційного приросту, скорочення (–) (на 10000 осіб)	1,7
Коефіцієнт дитячої смертності (померло дітей віком до одного року), на 1000 народжених живими	0,618182	Різниця індексу промислового виробництва України та росії, %.	1,7241379
Частка власних джерел у балансі паливно-енергетичних ресурсів держави, %	0,621118	Питома вага довгострокових кредитів у загальному обсязі наданих кредитів (скорегований на курсову різницю), %	1,8382353
Ступінь зносу основних засобів у будівництві, %	0,622407	Дефіцит/профіцит бюджетних та позабюджетних фондів сектору загальнодержавного управління, у % до ВВП	1,84
Питома вага провідної країни - партнера в загальному обсязі імпорту товарів, %	0,628	Питома вага провідного товару (товарної групи) в загальному обсязі експорту товарів, %	2,06
Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу: Яйця, %	0,64	Частка втрат при транспортуванні та розподіленні у споживанні енергії, %	2,1
Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу: Цукор, %	0,667	Відношення обсягу сукупних платежів з обслуговування та погашення державного боргу до доходів державного бюджету, %	2,125

Продовження табл. В.1

1	2	3	4
Загальна кількість учнів денних загальноосвітніх навчальних закладів у % до загальної чисельності постійного населення 6-17 років	0,690955	Завантаженість транзитних потужностей нафтотранспортної системи, %	2,2026432
Частка іноземного капіталу у статутному капіталі банків, %	0,699301	Індекс споживчих цін	2,2166667
Частка надходжень страхових премій 3-х найбільших страхових компаній у загальному обсязі надходжень страхових премій (окрім страхування життя), %	0,7	Обсяг виконаних будівельних робіт до 1990 року, %	2,5
Співвідношення загальних доходів 10 відсотків найбільш та найменш забезпеченого населення (децильний коефіцієнт фондів), разів	0,7	Відношення дефіциту, профіциту державного бюджету до ВВП, %	2,9166667
Відношення інвестицій в підприємства паливно-енергетичного комплексу до ВВП, %	0,714286	Завантаженість транзитних потужностей газотранспортної системи, %	4,3859649
Розмір економіки України, % до світового ВВП	0,714286	Середнє співвідношення обсягів валової доданої вартості промисловості України та ВДВ промисловості окремих країн Європи, %	4,5454545
Співвідношення обсягів заробітної плати та соціальних допомог та інших одержаних поточних трансфертів у загальній структурі доходів населення, рази	0,714286	Запаси кам'яного вугілля, місяці споживання	5
Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу: М'ясо, %	0,719424	Частка простроченої заборгованості за кредитами у загальному обсязі кредитів, наданих банками резидентам України, %	5,4428571
Обсяг видатків зведеного бюджету на охорону здоров'я, відсотки до ВВП	0,722892	Коефіцієнт природного приросту, на 1000 наявного населення	5,6
Демографічне навантаження непрацездатного населення на працездатне, %	0,724638	Відношення кредитів, наданих нефінансовим корпораціям та домашнім господарствам на придбання, будівництво та реконструкцію нерухомості (кумулятивно), у % ВВП	14,285714

Продовження табл. В.1

1	2	3	4
Питома вага готівки поза банками в загальному обсязі грошової маси (M0/M3), %	0,76	Схильність до заощадження населення, %	15
Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу: Молоко, %	0,76555	Різниця темпів росту ВВП України та темпів росту економік країн, що розвиваються, в.п.	16,75
Зайнятість населення у неформальному секторі економіки, у % до загальної кількості зайнятих	0,78	Відношення чистого приросту прямих іноземних інвестицій до ВВП, %	20
Відношення обсягу ВВП на одну особу в Україні до середнього значення у країнах ЄС, %	0,793651	Впровадження ІІІ в бізнес	2,3

Джерело: розраховано та доповнено автором на основі [98-99]

Таблиця В.2

Групування індикаторів для визначення загроз економічній безпеці України в умовах цифровізації

Загроза	Індикатори	Середнє відхилення
1	2	3
Технічна відсталість економіки	Середнє співвідношення обсягів валової доданої вартості промисловості України та ВДВ промисловості окремих країн Європи, %	1,584
	Відношення експорту роялті, ліцензійних послуг, комп'ютерних та інформаційних послуг, наукових та конструкторських розробок, послуг в архітектурних, інженерних та інших технічних галузях % до ВВП	
	Частка високотехнологічної продукції в загальному обсязі реалізованої промислової продукції, %	
	Питома вага обсягу виконаних наукових і науково-технічних робіт у ВВП, %	
	Внутрішні витрати на виконання НДР за рахунок коштів державного бюджету, % від ВВП	
	Кількість спеціалістів, які виконують науково-технічні роботи, до 1,476кількості зайнятого населення (на 1000 осіб)	
	Питома вага сировинного та низького ступеня переробки експорту (промисловості) у загальному обсязі експорту товарів, %	
	Завантаженість транзитних потужностей нафтотранспортної системи, %	
	Завантаженість транзитних потужностей газотранспортної системи, %	
	Питома вага реалізованої інноваційної продукції в обсязі промисловості, %	

Продовження табл. В.2

1	2	3
Структурні деформації економіки	Рівень безробіття (за МОП), %	1,494
	Відношення вартості нововведених основних засобів до обсягу капітальних інвестицій, %	
	Індекс інвестиційної сприятливості бізнес-середовища	
	Рівень запасів зернових культур на кінець періоду, відсотки від споживання	
	Співвідношення банківських кредитів та депозитів в іноземній валюті	
	Питома вага довгострокових кредитів у загальному обсязі наданих кредитів (скорегований на курсову різницю), %	
	Питома вага провідного товару (товарної групи) в загальному обсязі експорту товарів, %	
Енергетична залежність	Частка імпорту палива з однієї країни (компанії) у загальному обсязі його імпорту, %	0,148
Нерентабельність банків	Рентабельність активів банків, %	0,285
Дисбаланс торгових відношень	Розмір економіки України, % до світового ВВП	0,502
	Частка імпорту у внутрішньому споживанні країни, %	
Дефіцит товарів ПН	Співвідношення обсягів виробництва та споживання продовольчих товарів на 1 особу, %	0,485
Платіжний дисбаланс	Сальдо поточного рахунку платіжного балансу України, % до ВВП	0,5
Неконкуренто-спроможність ринку праці	Різниця між темпами росту середньомісячної заробітної плати та продуктивності праці в Україні, %	0,699
	Обсяг видатків зведеного бюджету на освіту, відсотки до ВВП	
	Загальна кількість учнів денних загальноосвітніх навчальних закладів у % до загальної чисельності постійного населення 6-17 років	
	Чисельність наявного населення, % до рівня 1990 року	
Соціальна нерівність	Частка населення із середньодушовими еквівалентними загальними доходами у місяць, нижчими 75 відсотків медіанного рівня загальних доходів, %	0,558
	Відношення середньомісячної номінальної зарплати до прожиткового мінімуму на одну працездатну особу, разів	
	Відношення середнього розміру пенсії за віком до прожиткового мінімуму осіб, які втратили працездатність, разів	
	Співвідношення загальних доходів 10 відсотків найбільш та найменш забезпеченого населення (децильний коефіцієнт фондів), разів	
Вимивання капіталів	Обсяг легального відпливу фінансових ресурсів за межі країни, млрд. дол. США	0,613

Продовження табл. В.2

1	2	3
Тінізація економіки	Рівень «тінізації» економіки, % до ВВП	1,341
	Рівень злочинності (кількість злочинів на 100 тис. населення), тис.	
Енергетична деструкція	Частка втрат при транспортуванні та розподіленні у споживанні енергії, %	1,791
	Співвідношення імпортової ціни на газ в Україні та Європі, разів	
Дефолт	Відношення офіційних міжнародних резервів до валового зовнішнього боргу, %	1,461
	Відношення дефіциту, профіциту державного бюджету до ВВП, %	
	Дефіцит/профіцит бюджетних та позабюджетних фондів сектору загальнодержавного управління, у % до ВВП	
	Рівень перерозподілу ВВП через зведений бюджет, %	
	Відношення обсягу сукупних платежів з обслуговування та погашення державного боргу до доходів державного бюджету, %	
	Індекс зміни офіційного курсу національної грошової одиниці до долара США, середній за період	
	Валові міжнародні резерви України, у місяцях імпорту	
	Відношення офіційних міжнародних резервів до валового зовнішнього боргу, %	
Інфляційні загрози (стагфляція)	Рівень безробіття (за МОП), %	1,934
	Індекс споживчих цін	
Геополітична економічна слабкість	Різниця індексу промислового виробництва України та росії, %	1,724
Бюджетний дефіцит	Відношення дефіциту, профіциту державного бюджету до ВВП, %	2,91
Деградація цифрової держави	Рівень розвитку цифрових послуг	0,975
	Рівень розвитку цифрової держави	
Обмеження мережі	Частка населення з доступом до мережі Інтернет	1,305
	Частка населення з доступом до фіксованого широкосмугового зв'язку	

Джерело: розраховано та доповнено автором на основі[98-99]

Додаток Г

Таблиця Г.1

Пріоритети інформаційно-цифрової складової економічної безпеки в Європі
та шляхи їх забезпечення

Пріоритет	Спосіб забезпечення
1	2
Безпека інвестицій	Подальше посилення захисту безпеки та громадського порядку ЄС, пропонуючи покращений скринінг іноземних інвестицій в ЄС, оскільки Китай та росія використовують реструктуризацію боргу в економічно менш розвинених країнах і експлуатують сучасну економічну модель аби втручатися в діяльність стратегічних підприємств, отримувати доступ до технологій, інфраструктурних проєктів, провокувати структурні стратегічні загрози.
Формування експортної координації	Існує нагальна потреба в стимулюванні дискусій та кооперативних дій для більшої європейської координації у сфері експортного контролю. Геополітичний контекст вимагає дій на рівні ЄС для поліпшення координації експортного контролю за цивільними та військовими товарами. Новий єдиний контроль, відносно товарів, де не діють інші міжнародні угоди, з направленими проти росії та експорту військових технологій має забезпечити більший ефект від санкцій і економічного впливу проти третіх країн.
	Особливого занепокоєння викликає цифровізація тіньових ринків: фінансові послуги, реєстрація компаній, товари подвійного призначення та військові товари, експорт підсанкційних російських товарів і контрабанда нафти. Усі вони діють переважно в приватному секторі та покладаються на слабе застосування санкцій третіми країнами або навмисну відмову впроваджувати їх.
Безпека технологій подвійного використання	Критичним для забезпечення технологічної переваги є дотримання усіма країнами-учасниками обмежень, які стосуються передових технологій, інновацій та окремих елементів для їх відтворення. Так, існує реальна перевага Євросоюзу, зокрема Нідерландів, у технології літографії чипів, проте окремі елементи цієї технології знаходяться в експортному контролі Німеччини та Австрії і вони також мають докладати зусиль до охорони регіональної переваги. Це стосується також технологій штучного інтелекту, квантових технологій та біотехнологій, які можуть бути використані для розробки зброї.
Безпека технологічної переваги	Запропонована рекомендація Ради Європи передбачає визначення безпеки досліджень на основі управління трьома групами ризиків: передача інформації, передові інновації і технології, які можуть вплинути на безпеку ЄС; будь-яке втручання третіх сторін у безпеку досліджень, інформації, передових інновацій або технологій, які можуть вплинути на безпеку ЄС та будь-яке втручання з боку третіх країн, які намагаються використати дослідження для підбурювання

Продовження табл. Г.1

1	2
	дослідників або студентів до самоцензури, порушення дослідницької доброчесності або академічної свободи; будь-яке зловживання знаннями і технологіями для підриву або скасування фундаментальних цінностей у всьому світі, в тому числі через порушення етики або доброчесності.
Загальна наукова безпека	Безпекові заходи у науковому середовищі викликані загрозою того, що вищі навчальні та науково-дослідні установи можуть стати жертвою недобросовісного впливу авторитарних держав, ключові спеціалісти можуть бути скомпрометовані, програми відкритості та співпраця без кордонів у науково-дослідному та інноваційному секторі можуть бути використані для технологічного шпигунства та просування пропаганди. Тому існує потреба захисту одночасно безпечного і вільного наукового розвитку, обміну знаннями та притоку спеціалістів в ЄС.
Сприяння конкурентоспроможності	Підтримка інновацій та промислового потенціалу, зберігаючи при цьому соціальну ринкову економіку. Це потребує поглиблення єдиного ринку, інвестування в економіку майбутнього та в людський капітал. Спільне Комюніке Ради та Парламенту ЄС відзначає, що інші країни мають вживати заходів, диверсифікуючи свої економічні зв'язки для зменшення залежності та збільшення місцевого виробництва.
Розгортання архітектури безпеки	Передбачає захист від негативного впливу цифровізації на загрози економічній безпеці ЄС шляхом розгортання інструментів протекціонізму національного виробника, залучення іноземних субсидій, забезпечення безпеки інфраструктури 5G/6G, фінансовий моніторинг та експортного контролю, спільній протидії економічному примусу з боку третіх держав.
Формування партнерства	Розвиток інституційного забезпечення економічної безпеки шляхом спільної роботи з якомога ширшим колом партнерів, зокрема в аспектах сприяння стійкості ланцюгів поставок та зміцненню міжнародного економічного порядку, заснованого на правилах та інститутах. Це також означає партнерство з країнами, що розділяють спільні безпекові цінності, просування та доопрацювання угод про вільну торгівлю, а також інвестування в сталий розвиток та безпечні зв'язки.

Джерело: систематизовано то доповнено автором на основі [156-164]

Таблиця Г.2

Нормативно-правові інструменти, регуляторне забезпечення економічної безпеки ЄС та їх складові в умовах цифровізації

Назва інструменту 1	Опис 2	Складові 3
Network and Information Security Directive 2 [177] (Директива про мережеву та інформаційну безпеку)	Має забезпечувати безпеку мережевих та інформаційних систем у всьому ЄС, не лише в секторі ІКТ, а в усіх інших галузях.	Розширення сфери застосування на енергетику, транспорт, фінансові послуги та інші галузі; уніфікація вимог безпеки, що передбачає встановлення єдиних стандартів кібербезпеки для всіх держав-членів ЄС; підвищення відповідальності із запровадженням більш суворих вимог до управління та звітності про інциденти кібербезпеки; а також збільшення штрафних санкцій, як мотиваційний стимул до зобов'язань суб'єктів щодо кібербезпеки.
The European Chips Act [165] (Європейський Акт про напівпровідники)	Має на меті підвищити технологічний суверенітет, конкурентоспроможність, стійкість ЄС, а також сприяти зеленим трансформаціям та цифровізації.	Комунікація, що передбачає обґрунтування та загальну напівпровідникову стратегію; створення спільної науково-технічної потужності; фінансові інвестиції та залучення коштів на ризикове внутрішнє виробництво; розвиток систем моніторингу глобальних ланцюжків поставок напівпровідників.
The Anti-Coercion Instrument [166] (Інструмент протидії економічному тиску)	Дозволяє вжити заходів у випадках економічного тиску проти ЄС або держав-учасниць з боку третіх країн. Метою є стримування примусу і необхідна реакція на нього задля захисту власних інтересів силою кооперації та концентрації спільних зусиль.	Комісійний розгляд та відповідальність перед партнерами, а також дипломатичне вирішення. Проте у ситуації де третя сторона ігнорує межі – існує перелік заходів, що включають обмеження доступу до ринку ЄС та інші економічні санкції для третьої країни. Союз також може вимагати відшкодування шкоди, заподіяної економічним примусом, відповідно до міжнародного публічного права та залучати треті країни зі спільними цінностями в протидії недобросовісним суб'єктам.

1	2	3
The EU toolbox for 5G security [164] (Європейський набір інструментів безпеки мереж 5G)	Зважає, що цифровізація економіки стосується мільярдів підключених об'єктів і систем, які використовуються в критично важливих секторах: енергетиці, транспорті, банківській справі, силових відомствах, національній безпеці, охороні здоров'я тощо. У той же час, завдяки менш централізованій архітектурі, розміщенні обчислювальної потужності на периферії, потребі в більшій кількості антен і підвищенні залежності від програмного забезпечення – мережі 5G пропонують більше потенційних точок входу для зловмисників.	Моніторинг інвестицій, експортний контроль, протекціонізм, використання внутрішніх механізмів фінансування. Окремо потребують обмеження та стандартизації мобільні оператори та провайдери з ризиковою поведінкою; диверсифікація та конкуренція постачальників має також обмежити залежність та збільшити гнучкість систем. Також, правовим інструментом, надаються роз'яснення до різних рівнів контролю і доступу до чутливих мереж. Оскільки системи стають пов'язаними та доступними для всіх учасників, то всі вони мають однаково піклуватися про захист спільних даних.
Dual-use export controls [157, 158] (Експортний контроль за товарами подвійного призначення)	Встановлює режим ЄС для контролю експорту, посередництва, технічної допомоги, транзиту та передачі товарів подвійного призначення. В умовах значних підсанкційних обмежень на росію, Іран, Сирію, КНДР та протидії нарощуванню китайських військових сил, а також забезпечення технологічної переваги – існує пряма необхідність в посиленому експортному режимі, який не охоплюється ширшими інструментами. Наприклад, Вассенаарською угодою [169], яка є режимом добровільного експортного контролю шляхом обміну анонімною та відкритою інформацією про передачу зброї та товарів і технологій подвійного призначення.	Цей інструмент передбачає п'ять типів експортних обмежень, якими можуть скористатися держави-учасниці, що діють на всій митній зоні ЄС, та регулюють стосунки з різними третіми країнами відповідно до переліку технологій подвійного призначення. Держави-члени можуть самостійно заборонити або вимагати дозвіл на експорт товарів з міркувань громадської безпеки, для передачі предметів подвійного використання зі своєї території до іншої держави-члена, а також обмежувати інші держави в сприянні експорту критичних технологій, шляхом інформування, співпраці та моніторингу за переліком ключових товарів.

Продовження табл. Г.2

1	2	3
The European instrument for temporary Support to mitigate Unemployment Risks in an Emergency [167] (SURE) (Європейський тимчасовий інструменти боротьби з безробіттям)	Мобілізував значні фінансові кошти для боротьби з негативними економічними та соціальними наслідками спалаху коронавірусу на території ЄС. Він створювався, щоб допомогти державам-членам захистити робочі місця, а отже, працівників та самозайнятих від ризику безробіття та втрати доходу під час COVID-19.	Цей інструмент складався з елементів фінансової підтримки, перерозподілу та розсіюванню ризиків по системі, поєднанню соціальної підтримки та економічних переваг, а також консультацій та комісій. Перевагою такого інструменту зазначається поширення позитивного впливу від учасників-реципієнтів, до всієї системи загалом, шляхом похідного розпорошення інвестицій та економічної стабілізації. І хоча він був тимчасовим – це створило прецедент застосування тимчасових рішень з метою вирішення конкретних загроз економічній безпеці держав-учасниць.
ORBIS [168]	Є порівняльним ресурсом даних про приватні компанії, їх власників та історію власності, контрагентів, потенційні фінансові ризики.	В умовах цифровізації існує можливість, виражена в цифровому інструменті ретельно фіксувати широкий спектр індикаторів, обробляти, насичувати та стандартизувати їх. Це дозволяє учасникам ринку вести фінансову розвідку і знижувати власні ризики, зменшувати транзакційні витрати, а також слугує силовим відомствам в заходах протидії фінансової злочинності.

Джерело: систематизовано автором на основі [157-158; 164-168; 177]

Додаток Д

Таблиця Д.1

Вихідні дані для розрахунку лінійної регресії проникнення інтернету в домогосподарствах в Україні за 2010-2024 рр.

Роки	2010	2011	2012	2013	2014	2015	2016	2017
Проникнення інтернету в домогосподарствах, % (права вісь)	22	28,7	35,3	33	46	49	53	59
	2018	2019	2020	2021	2022	2023	2024	
	63	70	76	80	85	94	94	

Джерело: побудовано автором на основі [147]

Таблиця Д.2

Показники лінійної регресії проникнення інтернету в домогосподарствах в Україні

b	5,265357	-10561	a
SE b	0,127813	257,8001	SE a
r2	0,992398	2,138727	SE y
F	1697,083	13	df
SS regresion	7762,716	59,46396	SS residual

Джерело: розраховано автором

Таблиця Д.3

Вихідні дані для розрахунку лінійної регресії онлайн-продажів, інтернет-покупців та кількості кібератак в домогосподарствах України за 2021-2024 рр.

Роки	2021	2022	2023	2024
Онлайн-продажі, млрд грн	129	151	182	239
Інтернет-покупці, млн	11*	8,5	9,9	11
Кількість кібератак	415	684	1536	1999

Джерело: побудовано автором на основі [148-150] *дані виключені з оцінки для кращої апроксимації моделі через сильне відхилення

Показники лінійної регресії онлайн-продажів, інтернет-покупців та кількості кібератак в домогосподарствах в Україні

Онлайн-продажі			
b	36,1	-72837	a
SE b	2,140427194	4331,16	SE a
r²	0,986133016	8,95405	SE y
F	284,4549423	4	df
SS regresion	22806,175	320,7	SS residual
Інтернет-покупці			
b	1,25	-2518,95	a
SE b	0,08660254	175,197	SE a
r²	0,99522293	0,122474	SE y
F	208,3333333	1	df
SS regresion	3,125	0,015	SS residual
Кількість кібератак			
b	560,4	-1132251	a
SE b	75,26499851	152223,5	SE a
r²	0,965180046	168,2977	SE y
F	55,4383299	2	df
SS regresion	1570240,8	56648,2	SS residual

Джерело: розраховано автором

Додаток Е

Результати безособового онлайн-анкетування закритої форми із застосуванням сервісу «Google Forms»

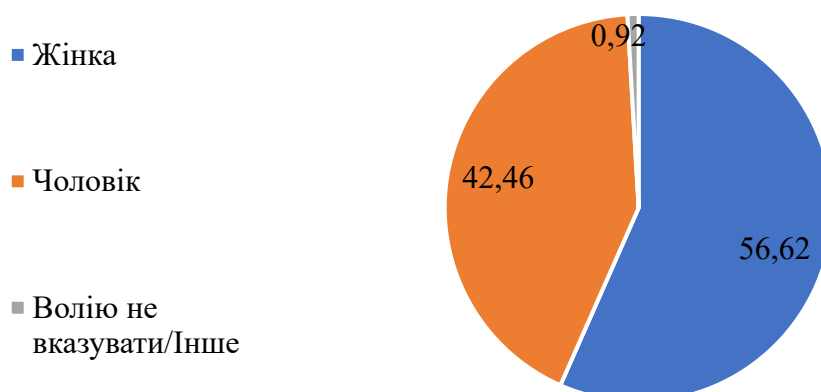


Рис. Е.1. Частка відповідей респондентів на питання «ваша стать»

Джерело: побудовано автором за результатами опитування

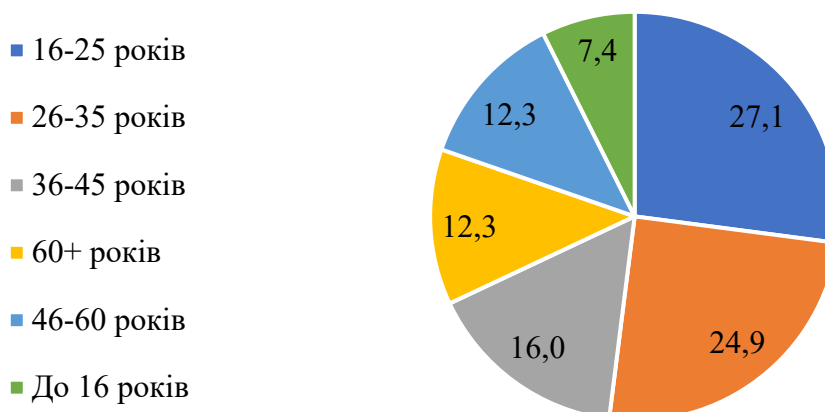


Рис. Е.2. Частка відповідей респондентів на питання «ваш вік»

Джерело: побудовано автором за результатами опитування

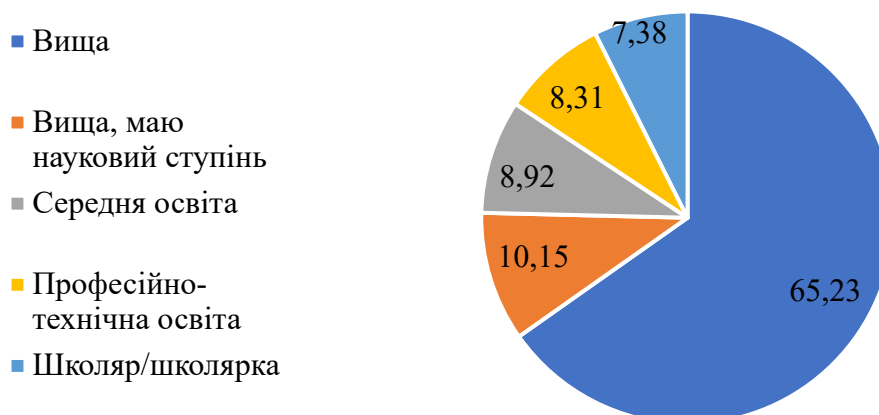


Рис. Е.3. Частка відповідей респондентів на питання «ваша освіта»

Джерело: побудовано автором за результатами опитування

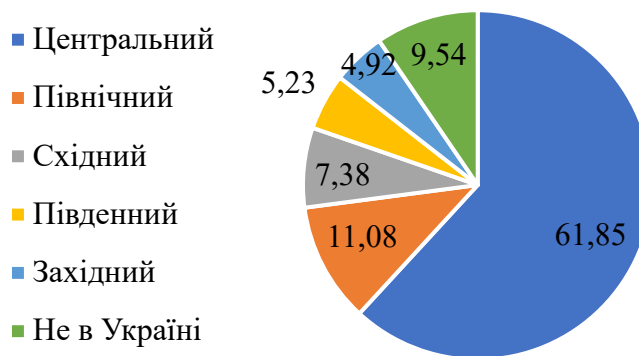


Рис. Е.4. Частка відповідей респондентів на питання «ваше поточне місцезнаходження», за регіонами

Джерело: побудовано автором за результатами опитування

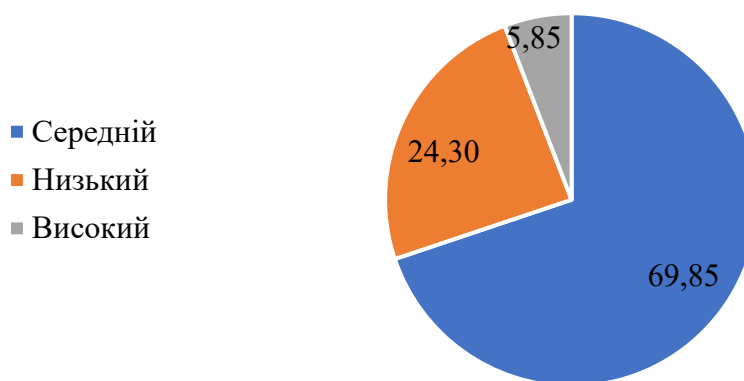


Рис. Е.5. Частка відповідей респондентів на питання «Як ви оцінюєте свій достаток?»

Джерело: побудовано автором за результатами опитування

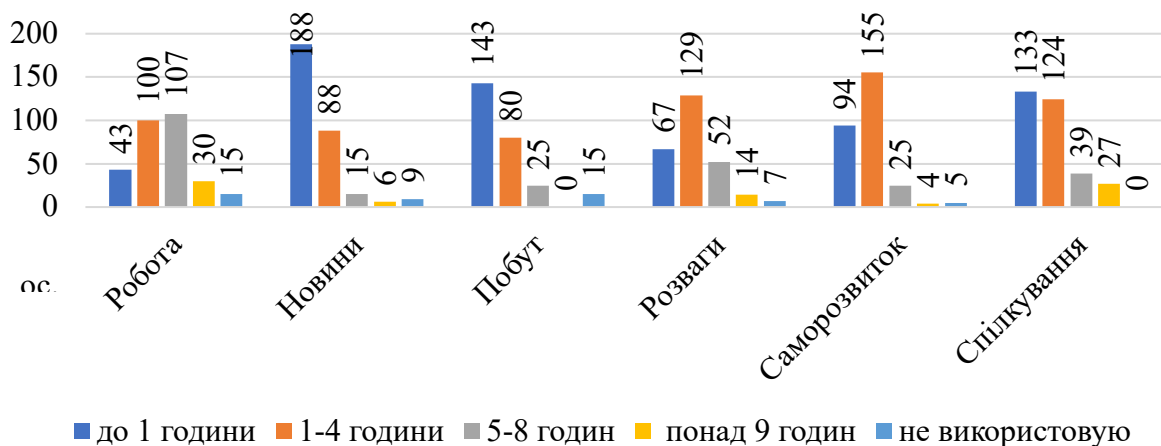


Рис. Е.6. Частота відповідей респондентів на питання «З якою метою і як довго ви використовуєте Інтернет протягом доби?»

Джерело: побудовано автором за результатами опитування

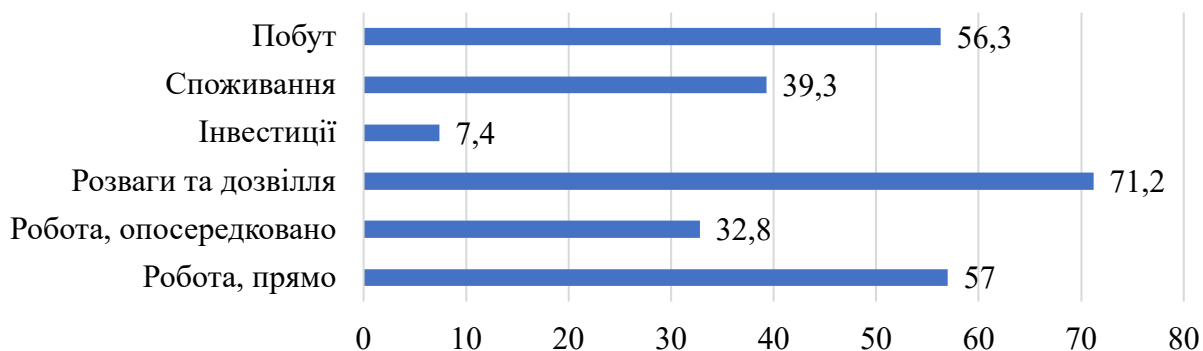


Рис. Е.7. Частка відповідей респондентів на питання «Перелічіть вашу діяльність, де ви постійно потребуєте доступу до мережі Інтернет»

Джерело: побудовано автором за результатами опитування



Рис. Е.8. Частка відповідей респондентів на питання «Як часто ви здійснювали покупки / проводили платежі протягом минулих 3 місяців?»

Джерело: побудовано автором за результатами опитування

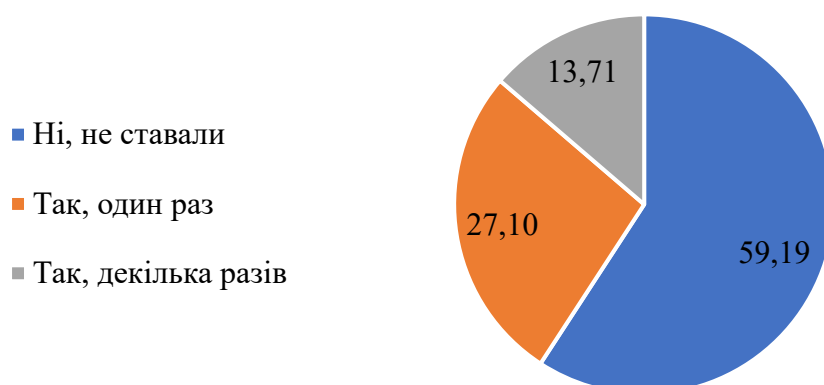


Рис. Е.9. Частка відповідей респондентів на питання «Чи ставали ви або ваші рідні жертвами онлайн-шахрайства, викрадення акаунтів протягом минулого року?»

Джерело: побудовано автором за результатами опитування

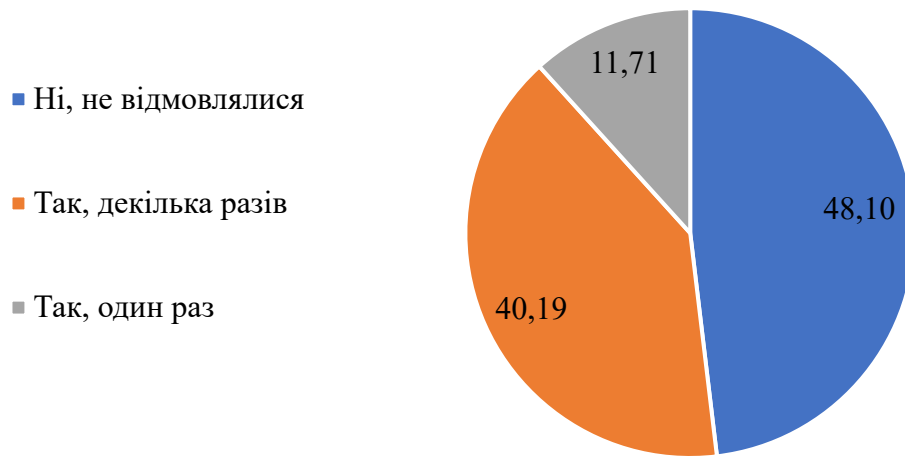


Рис. Е.10. Частка відповідей респондентів на питання «Чи відмовлялися ви, з міркувань безпеки, від замовлення / купівлі товарів онлайн, Інтернет-банкінгу та використання загальнодоступного Wi-Fi протягом минулого року?»

Джерело: побудовано автором за результатами опитування



Рис. Е.12. Частка відповідей респондентів на питання «До яких варіантів споживання інформації ви прагнете або які вам подобаються найбільше»

Джерело: побудовано автором за результатами опитування

Додаток Ж

Таблиця Ж.1

Пріоритети забезпечення економічної безпеки ЄС, визначені в нормативно-правових актах на міжнаціональному рівні

Пріоритети	Нормативно-правова база	Пріоритетні складові
1	2	3
Сприяння конкурентоспроможності та зростанню		
Інвестиційно-інноваційний розвиток	NextGenerationEU; Horizon Europe; Підтримка наукових досліджень і розробок у сфері технологій з потенціалом подвійного використання; Промислова стратегія ЄС; Європейська інноваційна програма.	Спільне фінансування, дофінансування проєктів, експериментальні простори, залучення кадрів та перепідготовка ІКТ-спеціалістів, пріоритизація технологій.
Підтримка виробництва	Закон про промисловість із нетто-нульовими викидами; Тимчасовий кризовий та перехідний механізм для державної допомоги.	Оптимізація процесів, розширення підтримки на складові ланки, підвищення кваліфікації, ринковість.
Захист ланцюгів та інфраструктури	RepowerEU; Закон про критичні сировинні матеріали; Платформа стратегічних технологій для Європи.	Спільні дії, збільшення внутрішньої потужності, диверсифікація виробництва.
Регіональна підтримка	Фонди згуртування; Союз ринків капіталу.	Спільні дії, спільне фінансування, ринковість.
Критичні технології	Європейський закон про напівпровідники.	Інвестиції, рамкові угоди, спільна координація.
Зменшення негативного стороннього впливу		
Захист від третьої сторони	Інструменти торговельного захисту; Регламент про іноземні субсидії; Інструмент ЄС для боротьби з примусом; Регламент про іноземні субсидії.	Спільні дії, пріоритизація технологій, проактивна підготовка до загроз, залучення третіх союзників, фінансовий тиск.
Захист критичних технологій	Регламент про перевірку прямих іноземних інвестицій; Моніторинг та оцінка ризиків зовнішніх інвестицій; Набір інструментів для боротьби з іноземним втручанням у дослідження та інновації.	Подолання регуляторної фрагментації, спільні дії, пріоритизація технологій, ринковість, моніторинг та штрафи, розкриття інформації.
Захист цифрової інфраструктури	Закон про кіберсолідарність; Набір інструментів для 5G; Директива щодо стійкості критично важливих суб'єктів; Переглянута Директива щодо безпеки мережевих та інформаційних систем; Закон про кіберстійкість.	Багаторівневість процесів забезпечення безпеки, практичність інструменти, спільні дії.

Продовження табл. Ж.1

Сприяння міжнародній співпраці		
1	2	3
Критичні аспекти	Ради з питань торгівлі та технологій, Партнерство для інвестицій у глобальну інфраструктуру; Клуб критичної сировини.	Спільні дії, пріоритизації союзників, розвиток міжнародної інфраструктури, геополітична протидія.
Ринковий розвиток	Угоди про вільну торгівлю; Партнерство з країнами, що розвиваються; Global Gateway; Реформа СОТ.	Спільні дії, ринковість, залучення союзників, інвестиції в інфраструктуру.

Джерело: систематизовано автором на основі [162-167; 176-177]

Таблиця Ж.2

Пріоритети забезпечення економічної безпеки України, визначені в наукових працях та звітах організацій

Пріоритет безпеки	Нормативно-правова база	Складові елементи
Стійкість до загроз та диверсифікація ресурсів	Про національну безпеку України, Стратегія національної безпеки України, Про енергетичну ефективність, Про пріоритетні напрями інноваційної діяльності в Україні, Про основні засади забезпечення кібербезпеки України.	Розвиток внутрішнього ринку, зменшення енергетичної залежності, пріоритизація технологій, інвестиції в інфраструктуру, формування і розвиток інститутів та агенцій, довгострокове планування.
Захист внутрішнього ринку та фінансова стабільність	Національна економічна стратегія, Про інформацію, План дій BEPS, Про національний банк, Про фінансові послуги та регулювання ринків фінансових послуг, про боротьбу з корупцією.	Формування і розвиток інститутів та агенцій, ринковість, фінансовий моніторинг, довгострокове планування.
Міжнародна інтеграція	Про індустріальні парки, Про інноваційну діяльність, Про засади внутрішньої і зовнішньої політики, Про підтвердження курсу України на інтеграцію до Європейського Союзу, Угода про асоціацію Україна-ЄС.	Спільні дії, пріоритизація політичних союзів, сприяння інноваційному середовищу, формування і розвиток інститутів та агенцій.

Джерело: систематизовано автором на основі [101; 121; 172]

Пріоритети забезпечення економічної безпеки України, визначені в
нормативно-правових актах

Автори	Пріоритетні напрями
1	2
О. Володимир, [178] С. Веретюк, В. Пілінський [179]	структурна перебудова реального сектору економіки шляхом переорієнтації з експорту сировини на продукцію з високою доданою вартістю; розвиток інноваційної діяльності через створення програм розширення джерел і можливостей залучення інвестицій для науково-інноваційної діяльності підприємств, організацій і науково-дослідних центрів; збереження ресурсів та використання економічного потенціалу для забезпечення макроекономічної стабільності, розвитку та захисту внутрішніх і зовнішніх національних інтересів; євроінтеграція, міжнародне позиціонування для утвердження України як рівноправного та надійного партнера; зміцнення фінансової незалежності шляхом посилення контролю над фінансовими потоками, скорочення зовнішнього боргу та кредитної залежності; адаптація національної економічної політики з урахуванням інтересів кінцевих бенефіціарів забезпечення безпеки та суспільних цінностей; формування єдиної системної державної стратегії цифровізації через одночасний розвиток усіх її складових; удосконалення цифрової інфраструктури шляхом розширення покриття мережі та залучення населення до використання цифрових послуг; розвиток людського капіталу для створення умов переходу до інформаційного суспільства та економіки знань.
К. Шиманська В. Бондарчук [180]	цифровізація публічних послуг з метою інтеграції громадян у цифрову інфраструктуру та формування у них цифрової грамотності для створення запитів до бізнесу та органів державної влади; розробка механізмів і середовища дистанційного навчання, електронне адміністрування освітніх процесів на всіх рівнях; розвиток цифрової інфраструктури у регіонах України для інтеграції локального бізнесу у ланцюги створення доданої вартості; фінансування або організація навчання представників бізнесу щодо роботи на міжнародних онлайн-платформах, використання міжнародних інформаційних баз, а також взаємодії з об'єктами прав інтелектуальної власності.

Продовження табл. Ж.3

1	2
CASE та CASE Україна «Економічні пріоритети повоєнної України» [181]	реформа інституцій та забезпечення верховенства права, антикорупційної політики, децентралізації, органів аудиту, оскільки саме їх недосконалість залишається головним бар'єром для залучення інвестицій та досконалого застосування державних інструментів; гармонізація нормативно-правового забезпечення та ролі держави у економіці, зменшивши її директивний вплив; формування кадрової конкуренції в публічному управлінні та аудит функцій центральних органів виконавчої влади, вдосконалення системи державної закупівлі; забезпечення макроекономічної стабільності, що вимагає оптимізацію податкових і митних процедур, залучення європейських фіскальних практик, адаптацію законодавства до європейських положень; лібералізація та дерегуляція ринку, приватизація і посилення боротьби з монополіями, а також збільшення ліквідності енергетичних ринків, зменшення державного тиску на трудові відносини; завершення земельної реформи, приватизації значимих підприємств та банків з метою їх ефективного ринкового використання; зменшення бюджетних витрат та соціальної допомоги, реформування пенсійної системи, використовувати комплексний підхід до зменшення бідності, проводити приватизацію в сфері охорони здоров'я, інвестувати в людський капітал, інтегрувати освіту, науку та виробництво.
Міністерство фінансів України та Міністерство економіки України у Звіті про пріоритети економічної політики, спрямованої на забезпечення економічного зростання [182]	макроекономічна стабільність, яка має вирішальне значення для загального функціонування економіки, забезпечення базових фінансових потреб, зокрема шляхом залучення фінансування зовнішніх донорів, використання заморожених російських активів та збільшення внутрішніх доходів від зменшення тіні, корупційних загроз та інституційної недосконалості; усунення першочергових обмежень для економічного зростання, зумовленого зовнішнім попитом, шляхом сприяння захисту інфраструктури і виробництва, пільг у доступу на ринок, сприяння поверненню біженців, вдосконалення транспортного сполучення; посилення потенціалу економічного зростання, шляхом реформування та лібералізації бізнес середовища, державних інвестицій, залучення партнерів до спільних проєктів.

Джерело: систематизовано автором на основі [178-182]

Додаток И

Карта експертної оцінки напрямів запобігання загрозам економічної безпеки України в умовах цифровізації

Напрями запобігання загрозам економічної безпеки України – це впорядковані пріоритетні напрями державної політики, управлінських рішень та економічних заходів, спрямованих на ідентифікацію, мінімізацію, нейтралізацію або усунення чинників і ризиків, що можуть завдати шкоди стійкості, ефективності й незалежності національної економіки.

Просимо висловити Вашу думку та оцінити параметри впливу, припущення та зусиль окремих напрямів запобігання загрозам економічної безпеки України в умовах цифровізації:

Reach – охоплення змінами цільової аудиторії, визначення показника розраховано населенням України у 32 млн осіб та, зважаючи на покриття мережі Інтернет у 94% у 30 млн для напрямів, що мають вплив на всіх користувачів, інші значення – пропорційні частці населення, яка безпосередньо відчує наслідки від зазначених дій;

Impact – рівень впливу від рішення, наскільки глобальними будуть результати, де більша оцінка – більш значні результати, від 0,25 до 2;

Effort – час на впровадження змін, відповідно до процесів затребуваних на реалізацію заходів, де більша оцінка – більші потреби часу, від 0,25 до 2;

Confidence – рівень довіри припущенням, де більша оцінка – більша впевненість про достовірність попередніх трьох припущень, в тому числі Reach, від 0,25 до 1.

Напря́м	R	I	E	C
Модернізація економічного законодавства цифровими аспектами	32			
Удосконалення інструментів регулювання впливу цифровізації	30			
Формування єдиної цифрової стратегії	28			
Оновлення методологічного апарату оцінки загроз в умовах цифровізації	27			
Сприяння зростанню цифрової грамотності населення	22			
Навчання цифрових компетенцій, фахівців ІКТ сектору та допомога перекваліфікації працівників галузі ІТ	14			
Удосконалення механізмів захисту зв'язку та мережі Інтернет	30			
Розвиток цифрової демократії	32			
Участь в європейських проєктах розвитку і захисту цифрової інфраструктури	32			
Залучення інвестиційних коштів для розвитку цифрових технологій	14			
Спільні правила цифрового простору	22			
Інтеграція інституцій та агенцій в безпекову архітектуру ЄС	32			

Додаток К

Таблиця К.1

Результати експертної оцінки напрямів запобігання загрозам економічної безпеки України в умовах цифровізації

Показник	Impact											
Респондент / Значення	1	2	3	4	5	6	7	8	9	10	CV	Сер
1	2	3	4	5	6	7	8	9	10	11	12	13
Модернізація економічного законодавства цифровими аспектами	1,3	1,4	0,9	1,4	1,4	1,1	1,3	1,4	1,5	1,3	0,14	1,3
Удосконалення інструментів регулювання впливу цифровізації	1	1,1	0,4	0,6	0,7	1	0,7	0,8	1	0,7	0,28	0,8
Формування єдиної цифрової стратегії	0,6	0,6	0,3	0,6	0,6	0,5	0,5	0,4	0,5	0,4	0,21	0,5
Оновлення методологічного апарату оцінки загроз в умовах цифровізації	0,5	0,5	0,4	0,6	0,5	0,4	0,4	0,5	0,6	0,6	0,16	0,5
Сприяння зростанню цифрової грамотності населення	1,5	1,6	1,4	1,7	1,7	1,6	1,7	1,8	2	2	0,11	1,7
Навчання цифрових компетенцій, фахівців ІКТ сектору та допомога перекваліфікації працівників галузі ІТ	1,4	1,4	1	1,2	1,1	1,3	1,3	1,4	1,6	1,3	0,13	1,3
Удосконалення механізмів захисту зв'язку та мережі Інтернет	0,9	1	0,5	1,1	1	1,1	1	1,3	1,3	0,8	0,24	1
Розвиток цифрової демократії	0,6	0,9	0,5	0,5	0,7	0,6	0,9	0,5	0,9	0,9	0,26	0,7
Участь в європейських проєктах розвитку і захисту цифрової інфраструктури	0,9	0,9	0,8	1	0,9	1,5	1	0,9	1,1	1	0,19	1
Залучення інвестиційних коштів для розвитку цифрових технологій	1	1,1	0,8	1,2	1	0,9	0,8	0,9	1,2	1,1	0,15	1
Спільні правила цифрового простору	1	1,1	0,5	1	1	0,9	0,7	0,8	1	1	0,20	0,9
Інтеграція інституцій та агенцій в безпекову архітектуру ЄС	1,9	1,9	1,5	1,8	1,6	1,6	2	1,9	2	1,8	0,10	1,8
Показник	Confidence											
Модернізація економічного законодавства цифровими аспектами	1	0,9	0,5	0,5	1	1	0,6	0,8	1	0,7	0,26	0,8
Удосконалення інструментів регулювання впливу цифровізації	0,9	0,8	0,6	0,6	0,6	1	0,8	0,9	1	0,8	0,20	0,8
Формування єдиної цифрової стратегії	0,6	0,7	0,4	0,6	0,7	0,5	0,7	0,6	0,6	0,6	0,16	0,6
Оновлення методологічного апарату оцінки загроз в умовах цифровізації	0,9	1	0,4	0,9	0,8	0,8	0,6	0,8	1	0,8	0,23	0,8

Продовження табл. К.1

1	2	3	4	5	6	7	8	9	10	11	12	13
Сприяння зростанню цифрової грамотності населення	1	0,6	0,6	0,9	0,5	0,8	0,9	0,8	1	0,9	0,22	0,8
Навчання цифрових компетенцій, фахівців ІКТ сектору та допомога перекваліфікації працівників галузі ІТ	0,6	0,7	0,6	0,6	0,5	0,6	0,5	0,5	0,8	0,6	0,16	0,6
Удосконалення механізмів захисту зв'язку та мережі Інтернет	0,7	0,8	0,7	0,5	0,5	0,5	0,6	0,8	1	0,9	0,25	0,7
Розвиток цифрової демократії	0,8	0,8	1	1	0,7	0,7	1	1	1	1	0,15	0,9
Участь в європейських проєктах розвитку і захисту цифрової інфраструктури	0,9	0,9	0,7	1	1,1	1	0,8	0,7	1	0,9	0,15	0,9
Залучення інвестиційних коштів для розвитку цифрових технологій	0,8	1	0,7	0,9	0,9	1,1	0,9	0,8	1	0,9	0,13	0,9
Спільні правила цифрового простору	0,6	0,6	0,8	0,8	0,5	1	1	0,9	0,8	1	0,23	0,8
Інтеграція інституцій та агенцій в безпекову архітектуру ЄС	0,9	0,6	0,6	0,7	0,9	0,9	1	0,8	1	0,6	0,20	0,8
Показник	Effort											
Модернізація економічного законодавства цифровими аспектами	1,6	1,6	1,6	1,7	1,8	1,9	1,6	1,5	2	1,7	0,09	1,7
Удосконалення інструментів регулювання впливу цифровізації	1,6	1,5	1,5	1,3	1,4	1,4	1,8	1,6	1,5	1,4	0,09	1,5
Формування єдиної цифрової стратегії	1,1	1,1	0,8	0,9	1	1	1	1,1	1,1	0,9	0,11	1
Оновлення методологічного апарату оцінки загроз в умовах цифровізації	0,5	0,5	0,3	0,6	0,5	0,4	0,5	0,6	0,7	0,5	0,24	0,5
Сприяння зростанню цифрової грамотності населення	2	1,9	1,8	2	2	2	2	1,9	2	2	0,04	2
Навчання цифрових компетенцій, фахівців ІКТ сектору та допомога перекваліфікації працівників галузі ІТ	1	1	0,7	1	1,2	0,8	0,9	1	1,3	1,1	0,18	1
Удосконалення механізмів захисту зв'язку та мережі Інтернет	0,7	0,8	0,7	1	1,1	1,1	1	1,1	1,3	1,2	0,21	1
Розвиток цифрової демократії	1,5	1,6	1,4	1,5	1,6	1,5	1,4	1,3	1,7	1,5	0,08	1,5
Участь в європейських проєктах розвитку і захисту цифрової інфраструктури	0,8	0,7	0,7	1	0,9	0,6	1,1	0,6	1	0,6	0,24	0,8
Залучення інвестиційних коштів для розвитку цифрових технологій	0,8	0,8	1	0,9	1,1	0,9	0,9	1,2	1,4	1	0,19	1
Спільні правила цифрового простору	1	1	0,5	1	0,7	0,7	0,6	0,7	0,9	0,9	0,23	0,8
Інтеграція інституцій та агенцій в безпекову архітектуру ЄС	2	2	1,9	1,9	2	2	1,9	1,9	2	2	0,03	2

Джерело: складено та розраховано автором

Додаток Л

Довідки про впровадження



**НАЦІОНАЛЬНИЙ ІНСТИТУТ
СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ**

вул. Пирогова, 7-а, м. Київ, 01054, Україна
тел. (044) 234-50-07, факс (044) 234-41-03

**NATIONAL INSTITUTE
FOR STRATEGIC STUDIES**

7 A Pyrohova St., Kyiv 01054, Ukraine
tel. (044) 234-50-07, fax (044) 234-41-03

28.04.2025 № 293/313

Національний університет
«Полтавська політехніка імені Юрія
Кондратюка»

ДОВІДКА

про впровадження результатів дисертаційної роботи
на здобуття наукового ступеня доктора філософії з економіки
Максименка Андрія Петровича

Результати дисертаційної роботи Максименка Андрія Петровича на здобуття наукового ступеня доктора філософії щодо впливу цифровізації на економічну безпеку держави використані в діяльності Національного інституту стратегічних досліджень при обґрунтуванні стратегічних напрямів зміцнення економічної безпеки держави в умовах цифровізації.

Відзначаємо наукову та практичну цінність сформованих методичних підходів до ідентифікації й моніторингу цифрових загроз, що дозволили здійснити аналіз рівня інформаційно-цифрової складової економічної безпеки України та обґрунтувати пріоритетні напрями зміцнення економічної безпеки держави в урахуванням дуального впливу цифровізації.

Результати дослідження будуть використані при підготовці аналітичних матеріалів та науково-методичних рекомендацій для спрямування до вищих органів влади України.

Директор д.ф.н.



Олександр БОГОМОЛОВ



**ПОЛТАВСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ
ДЕПАРТАМЕНТ ЕКОНОМІЧНОГО РОЗВИТКУ, ТОРГІВЛІ ТА
ЗАЛУЧЕННЯ ІНВЕСТИЦІЙ**

вул. Соборності, 45, м. Полтава, 36014, факс (+38 0532) 60-93-38
E-mail: gue@adm-pl.gov.ua; Код ЄДРПОУ 02741539

09.05.2025 № 01.1-08/1409 На № _____ від _____

Національний університет
„Полтавська політехніка імені Юрія
Кондратюка”

Про впровадження результатів
дисертаційної роботи

Департаментом розглянуто результати дисертаційної роботи на здобуття наукового ступеня доктора філософії з економіки Максименка Андрія Петровича. 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 забезпечення економічної безпеки в умовах цифровізації. Реалізація запропонованих дисертантом підходів пріоритезації напрямів зміцнення економічної безпеки держави в умовах цифровізації, що дозволяє виявити структурно-функціональні взаємозв'язки між інституційними, нормативно-правовими й техніко-технологічними компонентами та обґрунтувати доцільність концентрації зусиль на формуванні єдиної оптимізованої моделі забезпечення економічної безпеки держави.

Виконувач обов'язків директора
Департаменту економічного розвитку,
торгівлі та залучення інвестицій
обласної військової адміністрації



Андрій СОРОЧИНСЬКИЙ



ПЕНСІЙНИЙ ФОНД УКРАЇНИ

ГОЛОВНЕ УПРАВЛІННЯ ПЕНСІЙНОГО ФОНДУ УКРАЇНИ В ПОЛТАВСЬКІЙ ОБЛАСТІ

вул. Гоголя, 34, м. Полтава, 36000 (для листування 36600) тел. (0532) 56-02-09

E-mail: gu@pl.pfu.gov.ua, код згідно з ЄДРПОУ 13967927

від _____ 20 ____ р. № _____ На № _____ від _____ 20 ____ р.

**Національний університет
«Полтавська політехніка
імені Юрія Кондратюка»**

ДОВІДКА

про впровадження результатів дисертаційної роботи
на здобуття наукового ступеня доктора філософії з економіки

Максименка Андрія Петровича

Наукові та методичні положення, що містяться у дисертаційній роботі Максименка Андрія Петровича, мають практичну цінність та були враховані при розробці пріоритетних напрямків політики Головного управління Пенсійного фонду України в Полтавській області щодо управління його інформаційно-цифровою складовою економічної безпеки.

Запропонована автором модель забезпечення економічної безпеки держави, що інтегрує кількісні та якісні методи аналізу, включаючи соціологічне дослідження населення, та відображає адаптивну динаміку цифрових загроз на макро-, мікро- та нанорівні дозволила оцінити рівень захищеності персональних даних, електронного документообігу та ідентифікації осіб суб'єктів нанорівня забезпечення економічної безпеки держави. Це дало змогу мінімізувати негативний вплив цифровізації на діяльність Фонду.

**Начальник
Головного управління**

Людмила НАУМЕНКО, 0952076319



Володимир ТАРАТОРІН



Тараторін Володимир Никандрович

КНЕДЛ ДПС

624B52830660BA34E2200A63DC5429C1489BA072CD9039556BDD0751171B54D00

08.05.2025

Головне управління ПФУ в
Полтавській області



08.05.2025

1600-0702-8/35409



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

просп. Віталія Грицаєнка, 24, м. Полтава, 36011,
тел./факс (0532) 56 98 94, (0532) 60 87 30 (приймальня), web: www.nupp.edu.ua,
e-mail: rector@nupp.edu.ua, kanc@nupp.edu.ua,
Код ЄДРПОУ 02071100

29 05 2025 № 10-10/2121

На № _____ від ____ 20__

У спеціалізовану вчену раду

Про впровадження результатів
дисертаційної роботи

ДОВІДКА

Наукові розробки, висновки та рекомендації дисертаційної роботи Максименка Андрія Петровича за темою: «Вплив цифровізації на загрози економічній безпеці держави» впроваджені у навчальний процес Національного університету «Полтавська політехніка імені Юрія Кондратюка», зокрема:

- при викладанні лекцій з навчальних дисциплін «Теорія безпеки соціально-економічних систем» та «Фінансово-економічна безпека»;
- при підготовці завдань для практичних занять, самостійної та індивідуальної роботи студентів з дисциплін «Організація та управління системою фінансово-економічної безпеки підприємств», «Глобальні виклики розвитку національної економіки та ЄС».

Проректор з навчальної роботи



Директор департаменту організації
навчального процесу, акредитації та
ліцензування

Олена СТЕПОВА

Олег МАКСИМЕКНО