Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ЛОМОНОСОВА ЛЮДМИЛА СЕРГІЇВНА

УДК 368.8

ДИСЕРТАЦІЯ

РОЗВИТОК СТРАХУВАННЯ КІБЕР-РИЗИКІВ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

072 Фінанси, банківська справа та страхування

07 Управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

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

Науковий керівник:
Приказюк Наталія Валентинівна,
доктор економічних наук, професор

Київ – 2024

АНОТАЦІЯ

Ломоносова Л. С. Розвиток страхування кібер-ризиків в умовах цифрової економіки. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 072 – Фінанси, банківська справа та страхування. – Київський національний університет імені Тараса Шевченка Міністерства освіти і науки України. – Київський національний університет імені Тараса Шевченка Міністерства освіти і науки України. Київ, 2024.

Дисертація присвячена дослідженню основних аспектів страхування кібер-ризиків, а саме: поглибленню теоретико-методичних положень та розробці практичних рекомендацій щодо запровадження й розвитку страхування кібер-ризиків в умовах цифрової економіки.

У дисертаційній роботі поглиблено теоретико-методологічні основи страхування кібер-ризиків в умовах цифрової економіки, розроблено методичні підходи та практичні рекомендації щодо запровадження та розвитку вказаного виду страхування в Україні з метою забезпечення захисту економічних суб'єктів від загроз кіберпростору. Проведене дослідження стало фундаментом для формулювання таких висновків, які відображають виконання поставлених завдань дисертації.

Розкрито економічну природу кібер-ризиків в умовах цифрової економіки на основі зіставлення процесу становлення поняття «цифрова економіка» і трансформації ризиків під впливом цифровізації та виявлено спіральну модель еволюції дефініції «кібер-ризик», яка акцентує увагу на тісному взаємозв'язку проникнення цифрових технологій в економічну діяльність суб'єктів і на характері загроз, що вони становлять. Унаслідок дослідження наведено вдосконалене визначення поняття «кібер-ризику» як константи глобальних процесів цифровізації економіки (з урахуванням джерел виникнення загроз та характеру прояву наслідків їх реалізації). Узагальнено і систематизовано класифікацію кібер-ризиків на основі фасетного підходу за локалізацією,

видимістю, характером наслідків, формою прояву, розміром і ймовірністю настання та доповнено такими ознаками, як рівень економіки, страхувальність, сектор реалізації, що передусім включає розширений перелік кібер-ризиків оборонного сектору, які сформувались під впливом гібридної війни в Україні.

Визначено сутність поняття «страхування кібер-ризиків» на основі компаративного аналізу компонентів трактувань дефініцій «кіберстрахування» та «страхування кібер-ризиків» з доведенням їх тотожності. Виявлено детермінанти функціонування страхування кібер-ризиків, що відображають вплив цифровізаційних процесів на економічні суб'єкти та їхню діяльність, до яких належать: мета, об'єкти, суб'єкти, особливості, принципи, позитивні та негативні аспекти запровадження даного виду страхування, що дало змогу розширити й удосконалити визначення поняття «страхування кібер-ризиків». Завдяки використанню багатоступеневої структури безпеки економічних суб'єктів обґрунтовано позитивну роль застосування страхування кібер-ризиків як інструмента управління ризиком, що впливає на посилення фінансової безпеки страхувальників, оскільки наслідком реалізованого кібер-ризику є прямі або непрямі збитки, що в кінцевому вигляді набувають вияву втраченої економічної вигоди.

Виявлено характерні особливості страхових послуг у сфері страхування кібер-ризиків через застосування декомпозиції процесу реалізації послуги страхування кібер-ризиків та запропоновано: поетапний фреймворк розробки продукту страхування кібер-ризиків, що відображає імплементацію методологічних основ функціонування вказаного виду страхування в фактичний страховий продукт; алгоритм співпраці страховика та потенційного страхувальника під час ухвалення рішення про укладання договору страхування кібер-ризиків, що враховує оптимальний метод прийняття кібер-ризиків на страхування з максимізацією користі для всіх суб'єктів страхових відносин з метою гарантування їм прийнятного рівня фінансової безпеки; класифікацію груп кібер-ризиків для формування страхового покриття з визначенням доцільної форми страхового продукту (самостійного або комплексного). Використовуючи

підсумки проведеного аналізу, розрізнено поняття «послуга страхування кібер-ризиків» та «продукт страхування кібер-ризиків», відповідно визначено, що послуга є вираженням комплексу визначених дій страховика, що вказані в зафіксованих умовах продукту.

Виділено драйвери зростання обсягу глобальних валових премій страхування кібер-ризиків, які є індикатором розвитку цього ринку, а саме: збільшення розміру покриття населення мобільним зв'язком та суми втрат від кіберінцидентів на основі проведеного економетричного моделювання. Отримані результати були використані для визначення етапів періодизації становлення та розвитку глобального ринку страхування кібер-ризиків: підготовчий етап, етап зародження, етап створення самостійних продуктів страхування кібер-ризиків, етап зростання обізнаності про кібер-ризики, етап популяризації, сучасний етап активного розвитку. Натомість виявлення специфічних особливостей кожного етапу розвитку ринку страхування кібер-ризиків є основою для проведення аналізу потенціалу зростання даного сегменту страхового ринку в середньостроковій перспективі, адже дає змогу вчасно відзначити його перехід на новий етап розвитку з огляду на розширення наявних унікальних характеристик.

Встановлено, що використання економічними суб'єктами страхування кібер-ризиків є одним із ефективних складових комплексу заходів, спрямованих на досягнення глобальних Цілей сталого розвитку завдяки вдосконаленню системи моніторингу ризиків страхувальників, підвищенню рівня їхньої цифрової грамотності, зменшенню корупції, шахрайства та відмивання коштів, а також посиленню міжнародних партнерських зв'язків страховиків із фахівцями у сфері кібербезпеки. На основі виявлених локальних показників, що впливають на розвиток ринку страхування кібер-ризиків, а саме: покриття населення мобільним зв'язком та суми втрат від кіберінцидентів – запропоновано регіональний Індекс необхідності розвитку страхування кібер-ризиків, за яким отримано відповідний рейтинг доцільності розвитку вказаного виду страхування, що відображено таким низхідним порядком: Східна Азія й Тихоокеанські країни, Європа і Центральна

Азія, Північна Америка, Південна Азія, Латинська Америка і Карибський басейн, Субсахарська Африка, Близький Схід і Північна Африка.

Проведено діагностування сучасного стану вітчизняного ринку страхування кібер-ризиків, результати якого свідчать про низький рівень розвитку цього сегменту страхового ринку в Україні, адже пенетрація страховиків, які пропонують покриття кібер-ризиків, у 2023 р. не перевищувала 2%. Використовуючи запропонований Індекс потенціалу запровадження страхування кібер-ризиків вітчизняними страховиками, що формується на основі результативних показників страхової діяльності, а саме: приросту валових страхових премій рік до року, обсягу активів, загального рівня виплат, частки валових премій страхування фінансових ризиків у загальних валових преміях та частки валових премій страхування майна у загальних валових преміях – на основі кластерного аналізу було визначено чотири групи українських страхових компаній, що мають різну спроможність запровадження страхування кібер-ризиків: з оптимальним потенціалом, з високим потенціалом, з середнім потенціалом та з низьким потенціалом. Наявність позитивних результатів потенціалу запровадження страхування кібер-ризиків з одночасним низьким рівнем розвитку даного виду страхування на національному рівні свідчать про існування перепон для його розвитку на вітчизняному страховому ринку.

Обґрунтовано наявність та охарактеризовано стимулюючі та стримуючі фактори розвитку страхування кібер-ризиків в Україні, що виникли в умовах нової реальності функціонування цифрової економіки під впливом наслідків глобальної пандемії COVID-19 та повномасштабного вторгнення Російської Федерації в Україну. Розглянуті особливості стали основою формування стратегічної матриці впливу, яка забезпечує подолання стримуючих (недостатній рівень розвитку інституційно-правового забезпечення, середній рівень цифрової грамотності та фінансової інклюзії, низький рівень економічної активності, переміщення ІТ-компаній, еміграція кваліфікованих фахівців, глобальна невизначеність та економічна нестабільність) за допомогою активізації стимулюючих факторів, як от: державний фокус на підтримуванні високого рівня

кібербезпеки, глобальний тренд розвитку страхування кібер-ризиків, наявність вітчизняних досвідчених фахівців у сфері кібербезпеки, розвиток мобільних фінансових сервісів і технологій, цифровізація всіх сфер життя.

Розроблено комплекс заходів, які доцільно запровадити для вдосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні. Це, зокрема, розробка стратегії розвитку страхування кібер-ризиків на вітчизняному ринку, запровадження або гармонізація українського законодавства відповідно до міжнародних вимог у рамках початих 2023 року переговорів щодо вступу України до Європейського Союзу; розробка моделі квантифікації кібер-ризиків. Завдяки синергетичному ефекту розвитку вказаних векторів інституційно-правового забезпечення страхування кібер-ризиків в Україні доцільно здійснювати на основі клієнтоцентричної моделі страхування, що передбачає отримання страхувальником того рівня безпеки (включаючи фінансову та кібербезпеку), яка була зафіксована в умовах страхової угоди між страховими суб'єктами.

Наслідком поглибленого дослідження теоретичних і практичних аспектів страхування кібер-ризиків у глобальному та вітчизняному контексті є авторська пропозиція запровадження та розвитку вказаного виду страхування в Україні, представлена у вигляді дорожньої карти терміном на рік. Ключовими етапами запропонованої дорожньої карти є підготовчий, організаційний та реалізаційний етапи, ефективність втілення яких визначається на основі розрахунку оцінних індикаторів, що відображають широкий спектр даних про зміни в напрямках, пов'язаних зі страхуванням кібер-ризиків, а саме: кількісні та якісні зміни на ринку зі страхування кібер-ризиків; зміни обсягу покриття кібер-ризиків; зміни обізнаності населення про кіберзагрози; зміни кількості кіберінцидентів.

Ключові слова: страхування, страховий ринок, кібер-ризик, кіберстрахування, фінансова безпека, кібербезпека, цифровізація, діджиталізація, цифрова економіка, страхова послуга, інновація, інформаційні технології, сталий розвиток.

ABSTRACT

Lomonosova L. S. Development of the Cyber Risk Insurance in the Digital Economy. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the scientific degree of Doctor of Philosophy in specialty 072 – Finance, Banking and Insurance. – Taras Shevchenko National University of Kyiv, Ministry of Education and Science of Ukraine. – Taras Shevchenko National University of Kyiv, Ministry of Education and Science of Ukraine. Kyiv, 2024.

The dissertation is devoted to the study of the main aspects of cyber risk insurance, namely the deepening of theoretical and methodological provisions and the development of practical recommendations for the introduction and development of cyber risk insurance in the conditions of the digital economy.

The dissertation examines the economic implications of cyber risks in the digital economy by comparing the development of the «digital economy» concept and the changing nature of risks due to digitalization. It presents a spiral model that shows the evolution of the «cyber risk» definition and emphasizes the connection between the integration of digital technologies into economic activities and the threats they pose. The study offers an enhanced definition of «cyber risk» as a constant factor in the digitalization of the economy, considering the sources of threats and their consequences. It also provides a classification of cyber risks based on various factors, such as localization, visibility, consequences, manifestation, size, and likelihood of occurrence, and includes additional features like the economic level, insurability, and sector of implementation. This expanded classification specifically highlights the cyber risks in the defense sector that have emerged due to the hybrid war in Ukraine.

The concept of «cyber risk insurance» have been elucidated through a comparative analysis of the definitions of «cyber insurance» and «cyber risk insurance» to highlight their identity. The determinants of cyber risk insurance operation have been identified, underscoring the impact of digitalization on economic entities. This analysis covered the purpose, objects, entities, features, principles, and both the positive and negative aspects of introducing this type of insurance, thereby expanding, and refining

the definition of «cyber risk insurance». The adoption of a multi-level security structure for economic entities underscores the positive role of cyber risk insurance as a risk management tool, enhancing the financial security of policyholders as cyber risks can lead to direct or indirect losses, ultimately diminishing economic benefits.

The characteristics of cyber risk insurance services have been revealed through the application of the decomposition of the process of insurance services implementation, which includes: a framework for the development of a cyber risk insurance product, which reflects implementation of the operation methodological foundations into the actual insurance product; an algorithm for cooperation between insurer and potential insured during the decision-making process to enter into a cyber risk insurance contract, which includes the optimal method of accepting cyber risks for insurance with the maximization of benefits for all insurance subjects in order to guarantee them an acceptable level of financial security; classification of cyber risk groups for the formation of insurance coverage with determination of the appropriate form of insurance product (independent or complex). Through this analysis, the concepts of «cyber risk insurance service» and «cyber risk insurance product» have been clarified. Consequently, the service has been identified as a set of specific actions performed by the insurer, as outlined in the detailed terms of the product.

The factors driving the growth in global gross cyber risk insurance premiums have been identified, which reflect the progress of this market, include an increase in the number of people covered by mobile communication and the rise in losses from cyber incidents as determined through econometric modeling. These findings were used to define the various stages of the evolution of the global cyber risk insurance market: the preparatory stage, the emergence stage, the stage of developing independent cyber risk insurance products, the stage of raising awareness about cyber risks, the popularization stage, and the current stage of active growth. Analyzing the distinct characteristics of each stage of development in the cyber risk insurance market is essential for assessing its growth potential in the medium term, as it allows for timely recognition of its progression to a new stage based on the expansion of its unique features.

It has been established that the use of cyber risk insurance by economic entities is one of the effective components of a set of measures aimed at achieving the global Sustainable Development Goals by improving the policyholder risk monitoring system, increasing the level of their digital literacy, reducing corruption, fraud and money laundering, as well as strengthening of international partnership relations of insurers with specialists in the field of cyber security. On the basis of the identified local indicators that affect the development of the cyber risk insurance market: coverage of the population by mobile communication and the amount of losses from cyber incidents – a regional Index of the need for the development of cyber risk insurance has been proposed, according to which the corresponding rating of the feasibility of the development of the specified type was obtained insurance, displayed in descending order: East Asia and the Pacific, Europe and Central Asia, North America, South Asia, Latin America and the Caribbean, Sub-Saharan Africa, the Middle East and North Africa.

The diagnosis of the current state of the domestic cyber risk insurance market have been made, the results of which indicate a low level of this insurance market segment in Ukraine development, because the penetration of insurers offering cyber risk coverage did not exceed 2% in 2023. Using the proposed Index of the potential for the introduction of cyber risk insurance by domestic insurers, which is formed on the basis of insurance activity effective indicators: year-on-year increase in gross insurance premiums, the volume of assets, the overall level of payments, the share of gross financial risk insurance premiums in total gross premiums and shares of property insurance gross premiums in total gross premiums – based on cluster analysis, four groups of Ukrainian insurance companies with different capabilities of introducing cyber risk insurance have been identified: with optimal potential, with high potential, with medium potential and with low potential. The presence of positive results of the potential for the introduction of cyber-risk insurance with the simultaneous low level of development of this type of insurance at the national level indicate the existence of obstacles to its development in the domestic insurance market.

The existence of stimulating and restraining factors for the cyber risk insurance in Ukraine development, which arose in the conditions of the new reality with functioning of the digital economy under the influence of the global pandemic COVID-19 consequences and the full-scale invasion of the Russian Federation into Ukraine, have been substantiated and characterized. The considered features became the basis for the formation of a strategic influence matrix that ensures the overcoming of restraining factors (insufficient development level of institutional and legal support, average digital literacy level and financial inclusion, low economic activity level, relocation IT companies, qualified specialists emigration, global uncertainty and economic instability) with the help of activation of stimulating factors, such as: the state focus on maintaining a cyber security high level, the global trend in the cyber risk insurance development, the presence of domestic experienced specialists in the cyber security field, the mobile financial services and technologies development, all spheres of life digitalization.

A set of measures has been developed that should be implemented to improve the institutional and legal provision of cyber risk insurance in Ukraine. This is, in particular, the development of a strategy for the cyber risk insurance development on the domestic market, the introduction or harmonization of Ukrainian legislation in accordance with international requirements within the framework of the negotiations on Ukraine's accession to the European Union, which began in 2023; development of a cyber risk quantification model. Due to the synergistic effect of the specified vectors of institutional and legal provision of cyber risk insurance in Ukraine development, it is expedient to implement it based on a client-centric model of insurance, which provides for the insured to obtain the level of security (including financial and cyber security) that was fixed in the terms of the insurance agreement between insurance entities.

The result of an in-depth study of the theoretical and practical aspects of cyber risk insurance in the global and domestic context is the author's proposal for the introduction and this type of insurance development in Ukraine, presented in the form of a road map for a period of one year. The key stages of the proposed road map are the preparatory, organizational and implementation stages, the effectiveness of which is

determined based on the evaluation indicators calculation that reflect a wide range of data on changes in directions related to cyber risk insurance: quantitative and qualitative changes in cyber risk insurance market; changes in the scope of cyber risks coverage; changes in public awareness of cyber threats; changes in the number of cyber incidents.

Key words: insurance, insurance market, cyber risk, cyber insurance, financial security, cyber security, digitization, digital economy, insurance service, innovation, information technologies, sustainable development.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

Статті в наукових фахових виданнях:

1. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка.* 2020. № 4. URL: https://doi.org/10.32702/2307-2105-2020.4.6. (Особистий внесок автора: визначення характерних особливостей страхового покриття кібер-ризиків як інструменту захисту підприємств від загроз кіберпростору).

2. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Передумови розвитку кібер-страхування. *Інвестиції: практика та досвід.* 2020. № 15-16. С. 28–34. URL: http://dx.doi.org/10.32702/2306-6814.2020.15-16.28. (Особистий внесок автора: розроблено та обґрунтовано періодизацію становлення та розвитку глобального ринку страхування кібер-ризиків).

3. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Дорожня карта впровадження кібер-страхування в Україні. *Innovation and sustainability.* 2021. № 1. С. 64–72. URL: https://doi.org/10.31649/ins.2021.1.64.72. (Особистий внесок автора: запропоновано алгоритм проведення підготовчих заходів для впровадження та розвитку страхування кібер-ризиків в Україні).

4. Prykaziuk N., Lomonosova (Gumenyuk) L. Pandemic COVID-19 as a key factor in the development of DDOS-attacks insurance. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2022. № 1 (218). С. 39–44. URL: https://doi.org/10.17721/1728-2667.2022/218-1/6. (Особистий внесок автора: виокремлено ключові детермінанти розвитку страхування DDoS-атак в світі та здійснено компаративний регіональний аналіз полісів страхування кібер-ризиків).

Монографії:

5. Ломоносова (Гуменюк) Л. С. Фінансова інклюзія як ключовий фактор у відновленні економічного розвитку України після війни. *Transformation of Ukraine's economy: formation of an inclusive economy system and functionality of*

financial inclusion. Рига, 2023. С. 152–169. URL: https://doi.org/10.30525/978-9934-26-321-7-7.

Статті в іноземних наукових виданнях:

6. Lomonosova (Gumenyuk) L. Cyber insurance: modern requirements. *Economics & Education.* 2021. Vol. 6, No. 4. P. 33–36. URL: https://doi.org/10.30525/2500-946x/2021-4-5.

Опубліковані праці апробаційного характеру:

1. Ломоносова (Гуменюк) Л. С. Глобальні соціокультурні тренди поведінкової економіки та їх вплив на розвиток страхування. *Шевченківська весна 2021. Економіка. На шляху до сталого розвитку* : матеріали XIX Міжнар. науково-практ. конф., 18-19 берез. 2021 р. Київ : К., Інтерсервіс, 2021. С. 296.

2. Ломоносова (Гуменюк) Л. С. Трансформація продуктів кібер-страхування в умовах глобальної пандемії COVID-19. *Економіка. Фінанси. Бізнес. Управління. Зміни. Адаптація. Нова економіка : Діджиталізація ринку фінансових послуг: нові можливості та подолання бар'єрів* : матеріали II Міжнар. форуму, 28 верес.-1 жовт. 2021 р. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2021. С. 22-24.

3. Ломоносова (Гуменюк) Л. С. Перспективи розвитку кібер-страхування в Україні. *Проривні інновації на страховому ринку України*: матеріали V Міжнар. науково-практ. інтернет-конф., 27 жовт. 2021 р. Київ : К.: КНЕУ, 2021. С. 152–154.

4. Ломоносова (Гуменюк) Л. С. Особливості кібер-страхування в процесі адаптації до умов пандемії COVID-19. *Фінансові інструменти сталого розвитку економіки* : матеріали IV Міжнар. науково-практ. конф., 12 трав. 2022 р. Чернівці : Чернівецький нац. ун-т, 2022. С. 436–438.

5. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Забезпечення цифрової грамотності населення як складової національної кібер-безпеки. *Грудневі читання 2022. Стійкість бізнесу і добробут домогосподарств: фінансові та соціальні аспекти* : зб. тез доп. XIV Міжнар. науково-практ. конф., 1-2 груд. 2022 р. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2022. С. 84-85.

6. Lomonosova (Gumenyuk) L. Modern risks: anthropogenic or natural? *Modern Trends in The Development of Science and Technology* : Proceedings of the 3rd international scientific and practical conference, 12-13 December 2022. Innsbruck : LIU, 2022. P. 27-31.

7. Ломоносова (Гуменюк) Л. С. Глобальна невизначеність як драйвер переоцінки бізнес-ризиків. *Шевченківська весна 2023. Повоєнне відновлення економіки України: проблеми та перспективи* : матеріали XXI Міжнар. науково-практ. конф. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2023. С. 129.

8. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Кібербезпека фінансового сектору України: нові загрози та захисти в умовах повномасштабного вторгнення. *Страховий ринок України у світлі євроінтеграції: новітні виклики та тренди* : зб. матеріалів VI Міжнар. науково-практ. конф., 12 берез. 2023 р. Київ : К.: КНЕУ, 2023. С. 119-121.

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ

CISA – T he Cybersecurity and Infrastructure Security Agency

ENISA – The European Union Agency for Cybersecurity

EY – Ernst & Young Global Limited

IoT – Internet of things

ВВП – валовий внутрішній продукт

ДССУ – Державна служба статистики України

ЄС – Європейський Союз

ЗУ – Закон України

ІКТ – інформаційно-комп'ютерні технології

НБУ – Національний банк України

НТІ – науки, технології, інновації

ОЕСР – Організація економічного співробітництва та розвитку

ООН – Організація Об'єднаних Націй

СК – страхова компанія

ЦНАП – Центр надання адміністративних послуг

ВСТУП

Актуальність теми. Сучасну парадигму глобального економічного розвитку визначає високий рівень цифровізації всіх сфер життя та діяльності людства. Супутнім аспектом становлення цифрової економіки стає еволюція актуальних загроз, що призводить до формування та розгалуження кібер-ризиків. Оскільки страхування є одним з ефективних інструментів управління ризиками, розвиток страхування кібер-ризиків набуває пріоритетного значення для забезпечення стабільності суб'єктів у кіберпросторі.

Використання інструментів страхування кібер-ризиків дає змогу надавати страхувальникам необхідний персоналізований захист завдяки зменшенню втрат від кіберінцидентів та забезпеченню ефективного і швидкого відновлення після їх настання. Відсутність уніфікованого підходу в теоретико-методологічному та інституційно-правовому забезпеченні страхування кібер-ризиків гальмує процеси запровадження, розвитку та вдосконалення вказаного виду страхування. Однак якісні зміни у відповідних аспектах регулювання страхування кібер-ризиків сприятимуть його розвитку та підвищенню ефективності.

Управління ризиками кіберпростору стало особливо важливим завданням для економічних суб'єктів в умовах гібридної війни, розпочатої Російською Федерацією проти України. Тому розвиток страхування кібер-ризиків в Україні зумовить підвищення рівня захищеності від таких ризиків з одночасною реалізацією механізму відшкодування втрат від кіберінцидентів, що в цілому матиме комплексний вплив на посилення кібербезпеки України. Вказані аспекти проблематики розвитку страхування кібер-ризиків в умовах цифрової економіки підтверджують актуальність та доцільність дослідження обраної теми дисертаційної роботи.

Значний внесок у дослідження теоретико-методичних аспектів страхування кібер-ризиків здійснили іноземні вчені: К. Бінер, Р. Боме, Д. Вірфс, А. Гранато, М. Елінг, М. Камілло, Г. Катарія, Н. Кшетрі, Л. Міллер, Г. Мотт, У. Франке, В. Шнелл та ін. Проблематику ідентифікації та квантифікації кібер-ризиків у

процесі страхування досліджували Р. Боме, Д. Вреде, А. Н. Дук, Г. Катарія, Л. Павлік, Р. Пал, Д. Рак, Т. Стеген, М. Фіцек, А. Чірумаміла, Д. М. Шуленбург та ін. Більш вузько аспекти запровадження продуктів страхування кібер-ризиків на закордонних страхових ринках вивчали Д. Балзаротті, Л. Білге, Л. Гордон, С. Дамбра, М. Лоеб, Г. Перез, С. Романоскі, К. Россі, Т. Сохаіл, Ф. Шульц та ін.

Різнобічно висвітлювали у своїх наукових працях проблематику розвитку страхування кібер-ризиків в Україні та світі вітчизняні вчені, серед яких: С. В. Волосович, О. Є. Гудзь, М. В. Дубина, В. П. Ільчук, Л. М. Клапків, І. В. Ксьонжик, Л. С. Морозова (Селіверстова), О. М. Парубець, Р. В. Пікус, Н. В. Приказюк, Д. О. Сугоняко, А. С. Шолойко та ін. Роль страхування у системі фінансової безпеки в цифрову епоху досліджували В. П. Братюк, З. С. Варналій, Н. Г. Нагайчук, Н. М. Третяк, О. В. Ткаленко та ін.

Враховуючи якісні напрацювання зарубіжних та вітчизняних вчених щодо проблематики розвитку страхування кібер-ризиків у сучасних реаліях, деякі аспекти все ж потребують додаткового дослідження та уточнення. Зокрема, це стосується теоретико-методичних підходів до визначення місця страхування кібер-ризиків у цифровій економіці. Важливим є питання встановлення факторів впливу на зміну ринку страхування кібер-ризиків для виявлення потенціалу розвитку даного сегменту страхового ринку. Подальшого дослідження потребують підходи до гармонізації та вдосконалення вітчизняної інституційно-правової бази, що регулює сферу страхування кібер-ризиків. Нагальним є визначення стримуючих та стимулюючих чинників розвитку страхування кібер-ризиків і створення проєкту популяризації цього виду страхування в Україні, що відображає одне із завдань Національної стратегії кібербезпеки. Особлива важливість даних питань, а також їх недостатня наукова та практична розробка обумовили вибір теми дисертації, визначивши її мету та сформулювавши завдання.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалась у межах теми кафедри страхування, банківської справи та ризик-менеджменту економічного факультету Київського

національного університету імені Тараса Шевченка «Стратегічні вектори розвитку ринку фінансових послуг України» у 2023 р. № 22КФ040-06, де автором досліджено теоретико-методичні підходи та розроблено практичні рекомендації запровадження й розвитку страхування кібер-ризиків в умовах цифрової економіки.

Мета і завдання дослідження. *Метою* дисертаційної роботи є вдосконалення теоретико-методичних засад страхування кібер-ризиків в умовах цифрової економіки та розробка практичних рекомендацій щодо його запровадження й розвитку в Україні для забезпечення захисту економічних суб'єктів від загроз кіберпростору. Щоб досягнути поставленої мети, в дисертаційній роботі були визначені та розв'язані такі *завдання*:

- розкрити економічну природу кібер-ризиків в умовах цифрової економіки;
- визначити сутність та особливості страхування кібер-ризиків як об'єктивного наслідку цифровізації економіки;
- виявити характерні особливості страхових послуг у сфері страхування кібер-ризиків;
- здійснити періодизацію становлення глобального ринку страхування кібер-ризиків;
- оцінити потенціал страхування кібер-ризиків як інструмента забезпечення Цілей сталого розвитку;
- провести діагностування розвитку страхування кібер-ризиків в Україні;
- з'ясувати стимулюючі та стримуючі фактори розвитку страхування кібер-ризиків в Україні;
- визначити вектори удосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні;
- розробити дорожню карту запровадження та розвитку страхування кібер-ризиків в Україні.

Об'єктом дослідження є процеси функціонування і розвитку страхування кібер-ризиків в умовах викликів цифрового простору.

Предметом дослідження є теоретичні, методичні та практичні засади розвитку страхування кібер-ризиків в Україні в умовах цифрової економіки.

Методи дослідження. Задля досягнення поставлених завдань дисертаційної роботи було застосовано такі *методи наукового дослідження*: діалектичний метод – для узагальнення теоретико-методологічних основ страхування кібер-ризиків; методи аналізу та синтезу – для побудови взаємозв'язків між отриманими в процесі дослідження знаннями і для підбивання підсумків та формулювання висновків на їх основі; монографічний метод – для аналізу особливостей використання сучасних технологічних інновацій із встановленням спектру можливих кібер-ризиків, розгляду процесу кібер-страхування, його складових та особливостей; системний метод – для виявлення взаємовпливу факторів досліджуваних процесів у сфері страхування кібер-ризиків; метод порівняння – для порівняння страхових компаній, процесів прийняття ризиків на страхування; порівняльно-історичний метод – для зіставлення розвитку ринку страхування кібер-ризиків і цифрової трансформації економіки; метод формалізації – для відображення узагальнених та запропонованих підходів у вигляді алгоритмів і схем; економетричне моделювання – для визначення наявності впливу показників цифровізації економіки на розвиток глобального ринку страхування кібер-ризиків; метод ранжування – для розробки підходу до оцінювання необхідності використання кібер-страхування як інструмента захисту від загроз кіберпростору залежно від особливих характеристик регіону; метод зведення, групування і зображення статистичних даних – для наочного подання отриманих статистичних результатів у вигляді карт, графіків та діаграм.

Інформаційною базою дослідження є вітчизняні та іноземні інституційно-правові й законодавчі акти з питань регулювання страхової діяльності та кібербезпеки, дорожні карти розвитку, розроблені державними органами України, стратегії розвитку кібербезпеки України та, зокрема, країн Європейського Союзу, Сполучених Штатів Америки, Австралії; статистичні звіти, бази даних Державної

служби спеціального зв'язку та захисту інформації України, Державної служби статистики України, Національного банку України, World Bank, ENISA; вітчизняна і іноземна спеціалізована література, зокрема, монографії, статті, тези доповідей конференцій та інші наукові публікації, що відображають проблематику страхування кібер-ризиків.

Наукова новизна одержаних результатів полягає в поглибленні теоретико-методичних положень та розробці практичних рекомендацій щодо запровадження та розвитку страхування кібер-ризиків в умовах цифрової економіки з метою підвищення рівня кібербезпеки учасників страхових відносин. Найбільш вагомі результати, які становлять новизну дисертації, що їх виносять на захист, відображають особистий внесок автора і є такими:

удосконалено:

- трактування поняття «кібер-ризик» через розкриття особливостей еволюції дефініції на основі спіральної моделі трансформації ризиків (інформаційний – цифровий – кібер-ризик) у процесі цифрової трансформації, що сприяє усвідомленню актуальних кібер-ризиків економічними суб'єктами через встановлення взаємозв'язку між ступенем загрози кібер-ризику та рівнем цифровізації економіки, в якій він існує; та класифікацію кібер-ризиків за допомогою розширення їх фасетних ознак, таких, як рівень економіки, страхувальність, секторальна ознака, що є основою для створення комплексних стратегій для управління даними ризиками в умовах цифрової економіки;

- тлумачення природи «страхування кібер-ризиків», що базується на компаративному аналізі за дефініційними атрибутами наявних у науковій думці визначень, доведенні тотожності понять «кіберстрахування» і «страхування кібер-ризиків» та дає змогу уніфікувати використання даних термінів у науковій думці й інституційно-правовому забезпеченні та є підґрунтям для гармонізації вітчизняного законодавства в рамках поточних євроінтеграційних процесів;

- періодизацію становлення та розвитку глобального ринку страхування кібер-ризиків шляхом побудови економетричної моделі кореляції основних показників цифрової трансформації та показників діяльності даного сегменту

страхового ринку і врахуванні її результатів при формуванні хронічного порядку, що сприяє усвідомленню розвинутості ринку страхування кібер-ризиків у різних регіонах зі специфічними характеристиками та є основою для розробки відповідного комплексу заходів щодо імплементації та активізації даного виду страхування на локальному рівні з метою посилення фінансової безпеки суб'єктів господарювання;

- комплекс стимулюючих (глобальна цифровізація, посилення кіберзлочинності, вдосконалення мобільних фінансових сервісів і технологій, глобальний тренд поширення страхування кібер-ризиків, наявність досвідчених спеціалістів у сфері кібербезпеки та державний фокус на її покращенні) і стримуючих факторів (середній рівень цифрової грамотності та фінансової інклюзії, низький рівень економічної активності, прогалини та колізії у інституційно-правовому забезпеченні, переміщення ІТ-компаній та кваліфікованих фахівців, глобальна невизначеність та економічна нестабільність) розвитку страхування кібер-ризиків на вітчизняному страховому ринку, що передбачає всебічне врахування нових реалій в Україні, та представлений в стратегічній матриці їхнього впливу, задля активізації процесу запровадження і поширення даного виду страхування для досягнення цілей Стратегії кібербезпеки України.

набули подальшого розвитку:

- система заходів зі страхування кібер-ризиків, спрямованих на досягнення глобальних цілей сталого розвитку (оптимізація інфраструктури, проведення інклюзивної індустріалізації завдяки активному залученню інновацій; сприяння розвитку мирних та інклюзивних суспільств, надаючи всім доступ до правосуддя і створюючи ефективні підзвітні та інклюзивні інституції на всіх рівнях; поширення партнерств для підтримання стійкого зростання) через розрахунок регіонального Індексу необхідності розвитку страхування кібер-ризиків на основі виявлених значущих показників цифрової трансформації, що стане допоміжним важелем забезпечення глобального прогресу завдяки

вирізненню характерних особливостей функціонування економічних суб'єктів в кіберпросторі регіону;

- шляхи модернізації інституційно-правового забезпечення страхування кібер-ризиків в Україні, з використанням клієнтоцентричної моделі, що виражені в симбіозі трьох пріоритетних векторів, а саме: формування стратегії популяризації страхування кібер-ризиків, запровадження та гармонізація законодавства, розробка моделі квантифікації кібер-ризиків, що сприяє удосконаленню вітчизняної нормативно-правової бази у страховій сфері задля підвищення прозорості взаємодії та захищеності усіх учасників страхових відносин й підвищує страховий інтерес до відповідних страхових послуг;

- дорожня карта запровадження та розвитку страхування кібер-ризиків в Україні, що побудована на синергії учасників, залучених у процес створення та регулювання страхових послуг, та включає перелік заходів, об'єднаних у три етапи (підготовчий, організаційний, реалізаційний), результативність яких визначається через розрахунок індикаторів ефективності, з метою підвищення рівня інклюзивності національного страхового ринку та його відповідності сучасним цифровим викликам.

Практичне значення одержаних результатів. Науково-практичні рекомендації, запропоновані в дисертації, щодо створення Дорожньої карти запровадження та розвитку страхування кібер-ризиків в Україні і використання методології індикативного інструментарію оцінки ефективності розвитку страхування кібер-ризиків, були використані страховою компанією ARX у місті Києві в процесі розробки та просування інноваційних продуктів страхування (довідка №024/895 від 17.12.2023 р.).

Основні підсумки проведеного дослідження були використані Ірпінською міською радою в частині застосування факторів стимулювання розвитку страхування кібер-ризиків задля підвищення рівня обізнаності населення про кібер-загрози в умовах цифрової економіки та віднайдення шляхів мінімізації ймовірності їх настання як важливого етапу повоєнного відновлення української економіки (довідка № 01-18/691 від 14.02.2024 р.).

Ключові теоретико-методологічні положення розвитку страхування кібер-ризиків в умовах цифрової економіки та рекомендації щодо розвитку вказаного виду страхування в Україні, отримані внаслідок наукового дослідження, були апробовані та запроваджені в навчальний процес під час проведення лабораторних робіт і семінарів для студентів економічного факультету Київського національного університету імені Тараса Шевченка з дисциплін «Страхування» та «Ринок страхових послуг», що є складовою підготовки фахівців за освітнім рівнем «бакалавр», спеціальності 072 «Фінанси, банківська справа та страхування» (довідка №056 / 0095 від 26. 01. 2024 р.).

Особистий внесок здобувача. Наукові положення, висновки та рекомендації, які виносяться на захист, здобуті автором самостійно. Дисертаційна робота становить самостійне наукове дослідження, у якому відображається авторське розуміння особливостей розвитку страхування кібер-ризиків в умовах цифрової економіки. З наукових праць, опублікованих у співавторстві, у дисертації використовувались ідеї та положення, які є результатом особистих досліджень автора.

Апробація результатів дисертації. Основні положення дисертаційної роботи були подані до розгляду та доповідалися на восьми міжнародних науково-практичних конференціях, зокрема таких: XIX Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених «Шевченківська весна 2021. Економіка. На шляху до сталого розвитку» (18-19 березня 2021 р., м. Київ); II Форум EFBM 2021 «Зміни. Адаптація. Нова економіка» (28 вересня-1 жовтня 2021 р., м. Київ); V Міжнародна науково-практична інтернет-конференція «Проривні інновації на страховому ринку України» (27 жовтня 2021 р., м. Київ); IV Міжнародна науково-практична конференція «Фінансові інструменти сталого розвитку економіки» (12 травня 2022 р., м. Чернівці); XIV Міжнародна науково-практична конференція «Грудневі читання. Стійкість бізнесу і добробут домогосподарств: фінансові та соціальні аспекти» (1-2 грудня 2022 р., м. Київ); III Міжнародна науково-практична конференція «Modern trends in the development of science and technology» (12-13 грудня 2022 р., м. Іннсбрук, Австрія); XXI

Міжнародна науково-практична конференція «Шевченківська весна 2023. Повоєнне відновлення економіки України: проблеми та перспективи» (29-31 березня 2023 р., м. Київ); VI Міжнародна науково-практична конференція «Страховий ринок України у світлі євроінтеграції: новітні виклики та тренди» (23 березня 2023 р., м. Київ).

Публікації. Основні положення дисертаційної роботи опубліковано у 14 наукових працях, серед яких: 4 статті у вітчизняних фахових виданнях; 1 стаття у науковому періодичному виданні іноземної держави; 1 розділ у колективній монографії; 8 публікацій за матеріалами міжнародних науково-практичних конференцій.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, дев’яти підрозділів, висновків до розділів, загальних висновків до роботи, списку використаних джерел і додатків. Загальний обсяг дисертації становить 244 сторінки. Дисертація містить 41 рисунок та 24 таблиці (з яких 1 таблиця займає усю площу сторінки), має 10 додатків, що розміщуються на 23 сторінках. Список використаних джерел нараховує 233 найменування, розміщене на 24 сторінках роботи.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СТРАХУВАННЯ КІБЕР-РИЗИКІВ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

1.1. Економічна природа кібер-ризиків в умовах цифрової економіки

Нинішні реалії відзначаються швидкими темпами розвитку цифрових інновацій і технологічних продуктів, водночас розгалужуючи систему сучасних ризиків. Хоча питання історичної видозміни ризиків якісно досліджено іноземними та вітчизняними науковцями, однак малодослідженим залишається теоретико-методичний аспект, пов'язаний із сучасними ризиками цифрових технологій, які набули особливого значення в період цифрової економіки.

Поняття «цифровий» є похідним від загальновживаного англійського «digital», що в сучасних умовах вказує на пов'язаність означеного з використанням цифрових технологій, інструментів та інновацій. За словником «The Digital Europa Thesaurus» концептуально поняття «цифровий» неієрархічно пов'язують із двома групами: категорії, що означають матеріали / вироби з особливими якостями та матеріали / вироби з особливими якостями та режимом роботи (рис. 1.1).

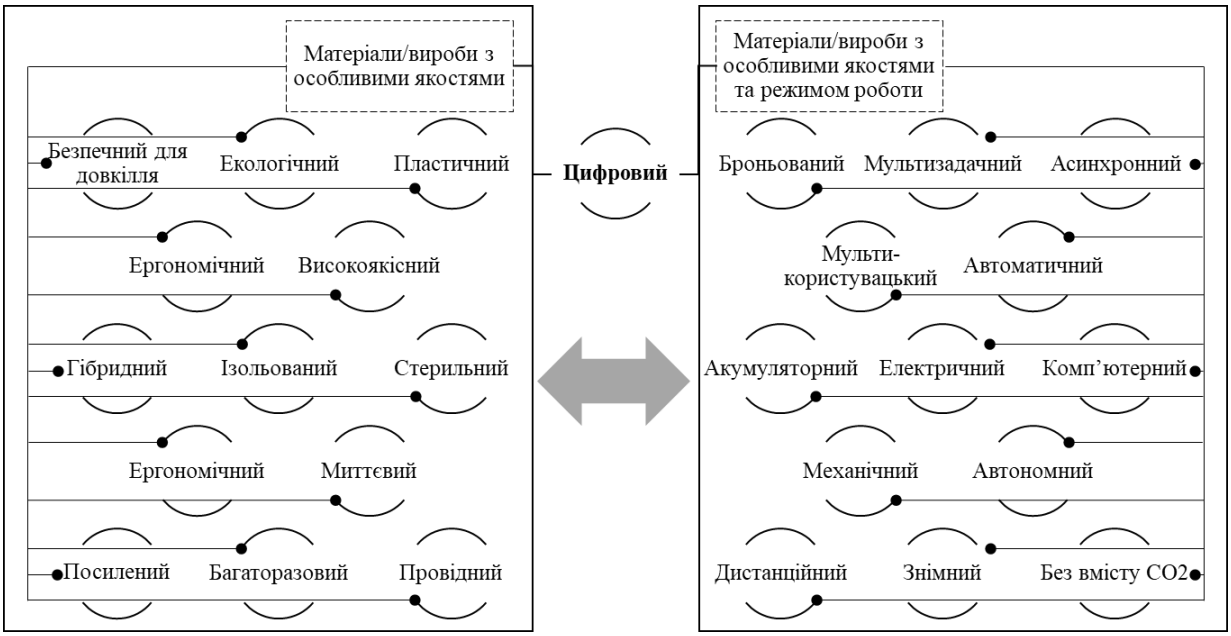


Рисунок 1.1. Концептуальна інтерпретація поняття «цифровий»

Джерело: складено автором на основі [225]

Відповідно сутнісно подібними до поняття «цифровий» є ознаки використання у певній сфері цифрових технологій, інструментів чи інновацій, що покращують ефективність, доступність та автономність певної діяльності, зменшуючи необхідність залучення людського ресурсу до неї. З огляду на це, процес «цифровізації» (англ. «digitalization») означає запровадження чи розширення використання цифрових технологій, інструментів або інновацій в певній сфері з метою її оптимізації. Також у літературі часто використовують поняття «цифрова трансформація» в даному контексті, однак тотожність понять є дискусійною.

Досліджуючи дефініції поняття «цифровізація» та «цифрова трансформація», І. В. Струтинська їх ототожнює за результатом, однак зауважує, що трактування можуть відрізнятися залежно від стейкхолдера, що їх інтерпретує. Так, різниця між трактуваннями стейкхолдерів даних понять виникає через відмінність підходів: для науковців – це процес еволюції відносин у суспільстві, спровокований розвитком цифрових технологій; для бізнесу – це механізм оптимізації бізнес-процесів, для держави – це розширення фізичного використання цифрових технологій та обміну даних між ними, для громадськості – це нова парадигма існування, основою якого є цифрові технології [88, с. 3].

Продовжуючи розгляд даних понять за підходом І. В. Струтинської, Н. І. Гражевська та А. М. Чигиринський здійснюють синтез поняття «цифрова економіка» і погоджуються з тотожністю «цифровізації» та «цифрової трансформації», різниця між якими самостійно визначається стейкхолдерами, проте не впливає на базову сутність поняття [13, с. 3].

Відмінною є думка Д. О'Лієрі, за якою планомірний розвиток цифрової трансформації є наслідком досягнення максимального рівня цифровізації діяльності, що настає після поширення оцифрування на більшість процесів певної сфери (наприклад, зменшення використання друкованих документів, створення електронних довідкових архівів, переведення ділової комунікації в цифровий режим) [201].

Розширений підхід пропонують Г. М. Дергачова та Я. О. Колешня, які трактують поняття «цифровізація» як етап, що передує «цифровій трансформації», оскільки перше свідчить лише про активне залучення цифрових технологій у певну діяльність з метою мінімізації ручної праці, в той час як друге означає процес перебудови наявної моделі ведення бізнесу в цілому. Також у своєму дослідженні вони окреслили поетапний процес становлення «цифрової трансформації» на прикладі сфери економіки: оптимізаційний етап «оцифрування» означає перенесення збору економічних даних у цифровий формат; етап підвищення ефективності «запровадження цифрових технологій» свідчить про формування цифрової інфраструктури економіки з використанням пулу цифрових технологій; партнерський етап «цифровізація» включає формування цифрового простору взаємодії користувачів цифрових технологій, що окреслює створення цифрової моделі економіки; еволюційний етап «цифрова трансформація» – це перехід всіх компонентів економічної системи в цифровий простір та становлення цифрової економіки [17, с.5].

Загалом у процесі компаративного аналізу понять «цифровізація» та «цифрова трансформація» найбільш повним був підхід Г. М. Дергачової та Я. О. Колешні. Однак така концепція не враховує першочергової причини виникнення поняття «оцифрування», а саме, наявності доступної цифрової технології, що є основою всього процесу (рис 1.2).

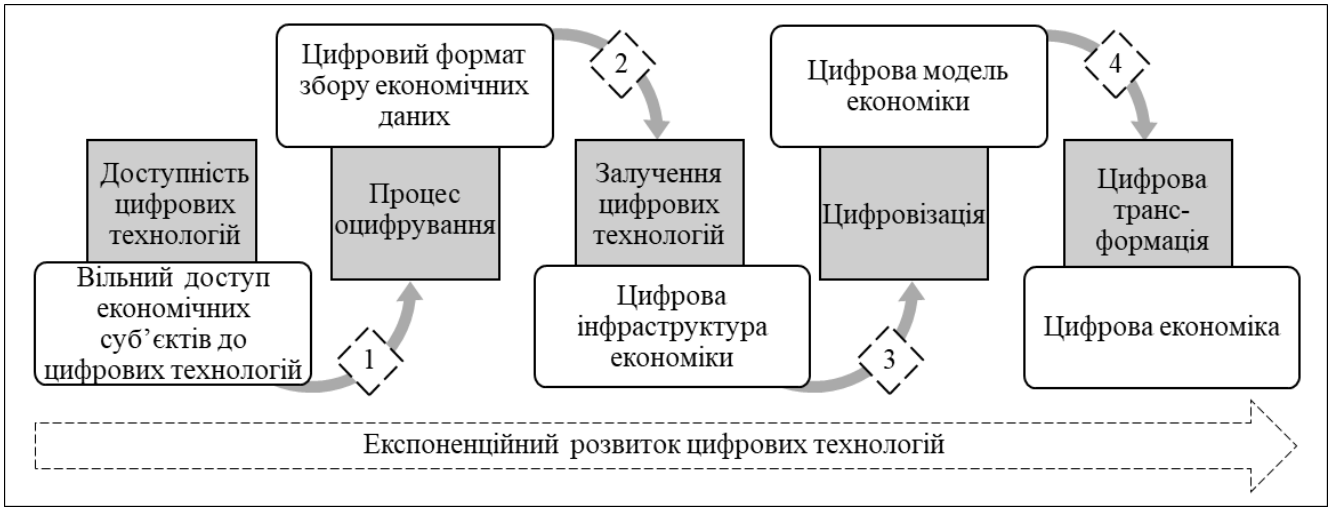


Рисунок 1.2. Дефініційний процес становлення поняття «цифрова економіка»

Джерело: складено та доповнено автором на основі [17]

Відповідно до запропонованого підходу, було простежено генезу впливу розвитку цифрових технологій на економіку, враховуючи поступове зростання їх проникнення в економічні процеси. Отже, згідно з таким підходом, дефініційно поняття «цифрова економіка» ґрунтується на доступності цифрових технологій, тобто можливості вільно отримувати та використовувати їх на безоплатній чи комерційній основі.

Теоретичні підходи сучасної економічної наукової думки щодо визначення поняття «цифрова економіка» також відрізняються (Додаток А). Систематичний огляд праць іноземних та вітчизняних науковців дав змогу класифікувати підходи до трактування поняття «цифрова економіка» (Таблиця 1.1).

Таблиця 1.1

Теоретико-методологічні підходи до визначення поняття «цифрова економіка»

Підхід	Автори
Цифрова економіка як оптимізована похідна економіки	Карчева Г. Т., Огородня Д. В., Опенько В. А., Ковтонюк К. В., Кузнєцова А. Я., Чмерук Г. Г., Пуцентейло П. Р., Гуменюк О. О., Сірко А. В.
Цифрова економіка як доповнення до традиційної економіки	Li K., Kim D.J., Lang K.R., Kauffman R.J., Naldi M., Ус Г.О., Коваль О.О.
Цифрова економіка як ознака зрілості традиційної економіки	Bart V. A., Xia Y., Lv G., Wang H., Ding L.
Цифрова економіка як адаптована економіка, що реалізує свої функції через використання цифрових технологій	R. W. Patterson, Батракова Т. І., Линовецька В. Ю., Коляденко С. В., Ковбатюк М. В., Шевчук В. О., Об'єднання «Digitalized Economy»
Цифрова економіка як окремий сектор економіки	Войнаренко М. П., Пілінський В. В., Веретюк С. М., Чмерук Г. Г.

Джерело: складено автором на основі [4, с. 94; 11, с. 19; 34, с. 14; 38, с. 70; 39, с. 73; 40, с. 107; 42, с. 38; 56, с. 4; 75, с. 136; 78, с. 4; 91, с. 71; 94, с. 4; 105, с. 3-5; 106, с. 11; 155; 167, с. 101010; 203, с. 304]

Відповідно до вищезазначеного, було окреслено п'ять теоретико-методологічних підходів до визначення поняття «цифрова економіка»:

1. Цифрова економіка як оптимізована похідна економіки. За таким підходом науковці визначають цифрову економіку як трансформовану традиційну економіку, основою якої є збільшення використання цифрових технологій в економічних процесах, що сприяє оптимізації, яка полягає в підвищенні ефективності та конкурентоспроможності. Трансформація має природний характер, оскільки поява певних технологій та інновацій здійснюється під

впливом глобальних трендів чи локальних цифрових особливостей регіону. Варто зауважити, через нерегламентований розвиток цифрової трансформації економіки рівень проникнення цифрових технологій у різні сфери економіки може бути нерівномірним.

2. Цифрова економіка як доповнення до традиційної економіки. Даний підхід вказує на можливість одночасного співіснування традиційної та цифрової економіки. Однак друга розглядається як додаткова або допоміжна, тобто акцент зміщується на нематеріальну особливість цифрової економіки та нездатність замінити фізичний процес виробництва. Межі цифрової економіки за означеним підходом не обмежуються економікою, а перетинаються з технологіями. В цьому підході інструменти цифрової економіки покращують та оптимізують традиційну економіку, проте не замінюють її.

3. Цифрова економіка як ознака зрілості традиційної економіки. Відмінністю цього підходу є усвідомлена трансформація традиційної економіки в цифрову. Суб'єкти традиційної економічної системи поетапно якісно вдосконалюють економічні процеси, алгоритми та механізми взаємозв'язків, методи управління, збільшуючи пенетрацію цифрових технологій. Відповідно досягнувши запланованого рівня цифрової трансформації, економіка набуває цифрового статусу.

4. Цифрова економіка як адаптована економіка, що реалізовує свої функції через використання цифрових технологій. Характерною особливістю цього підходу є адаптація цифрових інструментів під наявне функціональне призначення традиційної економіки. Відповідно відбувається активне залучення сучасних цифрових інструментів в економічну діяльність для спрощення певних бізнес-процесів, проте сутнісна економічна діяльність не змінюється.

5. Цифрова економіка як окремий сектор економіки. Вказаний підхід допускає підпорядковане існування цифрової економіки як частини економіки. Цифрову економіку позначають як відділену складову економіки, в якій основними засобами виробництва є цифрові технології. Особливістю даного підходу є визначення нематеріального виробництва як єдиного виду діяльності в

цифровій економіці. Окрім того, деякі науковці визначають цифрову економіку як незалежну від реального світу.

Незважаючи на обґрунтованість кожного підходу, в сучасних реаліях щоденних викликів та змін варто трактувати поняття «цифрова економіка» в рамках синергетичного ефекту двох підходів: цифрова економіка як ознака зрілості традиційної економіки та цифрова економіка як адаптована економіка, що реалізує свої функції через використання цифрових технологій. Синергія буде виражена плановим поступовим процесом цифрової трансформації економіки з можливістю адаптуватися до швидких змін від впливом зовнішніх або внутрішніх факторів. Однак при цьому буде залишатися опціональна можливість відступити від початкового плану та адаптуватись до нових умов через доступність ефективніших нових технологій, що спростять певні трансформаційні процеси, або через певний неуспішний етап трансформаційного процесу, що зможе частково обмежити здійснення функцій економіки.

Опираючись на проведений аналіз становлення поняття «цифрова економіка» як приклад цифрової трансформації, та використовуючи синергетичний концепт поєднання теоретико-методологічних підходів до визначення поняття «цифрова економіка», доцільним вважаємо доповнення наявних трактувань та визначення поняття, за яким цифрова економіка – це система економічних та соціальних відносин, яка реалізує свої функції на основі цифрових технологій та пройшла процес цифрової трансформації з індустріальної до цифрової форми під впливом активного розвитку цифрових технологій і їх проникнення до своєї інфраструктури, що забезпечує її гнучкість і адаптивність.

Оскільки цифрова економіка означає використання широкого спектру цифрових технологій [25, с. 96–97], актуальною стає невизначеність, пов’язана з ними. Невизначеність – це основа формування ризику, тому розвиток цифрової економіки сприяє збільшенню спектру актуальних ризиків. У науковій думці використовуються такі ризики, як інформаційний, цифровий та кібер-ризик, у контексті дослідження загроз сучасного цифрового світу та економіки зокрема.

На думку групи вчених О. Б. Данченко, Є. В. Ланських, О. В Семко, «інформаційний ризик» є супутнім до процесу цифровізації. Також вони зазначають, що шляхи мінімізації таких ризиків полягають в ідентифікації та оцінці ризиків інформаційних активів компанії [15, с. 63].

Г. В. Мельник вважає, що поняття «інформаційний ризик» та «загроза безпеки інформації» є синонімічними. Керівникам підприємств варто здійснювати аналіз і розгляд потенційних загроз з позиції можливості втратити не лише захищеність інформації, що використовується в бізнес-процесах, але і її якість [49, с. 48-53].

2015 року ОЕСР розширила межі поняття ризику, пов'язаного з технологіями, та рекомендувала будувати систему ризик-менеджменту з урахуванням «цифрового ризику», що додатково включає економічний і соціальний ризик, а не лише технологічний [215, с. 1].

Поглибили даний підхід В. Вітлінський та Л. Маханець, які позначають поняття «цифровий ризик» як пов'язане «з функціонуванням усіх процесів генерування, обліку, передачею, обробленням та зберігання даних, з аналітикою в ЗЕД тощо» [10, с. 80].

Дослідження А. Н. Дука та А. Чірумаміла відкривають новий аспект цифрового ризику, відзначаючи не тільки потенційні фінансові втрати та цифрові злами, а й порушення безпеки систем, розкриття конфіденційної інформації, втрату даних клієнтів та загрозу кібербезпеці [151, с. 680-685].

Проте найчастіше науковці використовують поняття «кібер-ризик» для опису загроз цифрових технологій. Дослідженню трактування цього поняття приділено достатньо уваги в сучасній науковій думці, оскільки поняття стосується не лише сфери економіки, а й сфери технологій. Однак різновекторність досліджень провокує виникнення неузгодженого розмаїття трактувань.

Ґрунтовною працею у сфері наукового пізнання кібер-ризиків є дослідження М. Елінга та В. Шнела, в якому деталізовано джерела виникнення кібер-ризиків, їх характерні особливості, підходи до їх страхування як інструмента скорочення межі впливу кібер-ризиків [153, с. 479-486].

К. Россі та Г. Перез пропонують розрізняти поняття «кібер-ризик», залежно від сервісного сектору, в якому здійснюється реалізація кібер-ризику. У своїй праці вони виділяють вісім підходів до даного трактування з позиції таких сервісів: фінансові (включаючи страхові), інфраструктурні, бізнес-саппорт, індустріальні, комерційні, державні, персональні та користувацькі послуги [111, с. 11-12].

Науковці С. В. Волосович та Л. М. Клапків виокремили три підходи під час аналізу трактувань поняття «кібер-ризик», а саме: причинно-наслідковий, за яким поняття формується як поєднання джерела виникнення наслідків реалізації кібер-ризику; секторальний підхід, за яким поняття описує сферу реалізації кібер-ризику; інструментальний підхід, за яким основою поняття є інструмент як джерело реалізації кібер-ризику [12, с. 103].

Концептуальною є праця В. П. Братюк щодо визначення поняття «кібер-ризик» за сутністю потенційної загрози. У ній розглянуто п’ять підходів до трактування з відповідним включенням особливості загрози до визначення: ризик втрати інформації та порушення роботи систем при зламі пароля доступу чи внаслідок DDOS-атаки, ризик фінансових втрат через порушення роботи комп’ютерних систем, ризик фінансових втрат за регрес-позовами при викраденні, розголошенні або використанні персональної інформації, ризик фінансових втрат через здирництво при вірусному блокуванні комп’ютерних систем, ризик фінансових втрат на відновлення програмного забезпечення або інформації [6, с. 425]. Запропонований підхід акцентує визначення поняття «кібер-ризик» саме на потенційних фінансових втратах.

Окрім дефініцій поняття «кібер-ризик», виокремлених у вищезазначених підходах, науковці пропонують та використовують власні трактування, побудовані в рамках персональних досліджень з різними завданнями.

Систематизація запропонованих трактувань поняття довела наявність недоліків та неточностей у сучасній науковій думці (Додаток Б). Аналіз поняття «кібер-ризик» за інституціональним підходом дає змогу точніше виявити важливі аспекти ризику залежно від стейкхолдера (Таблиця 1.2).

Таблиця 1.2

Особливості трактування поняття «кібер-ризик» стейкхолдерами

Група	Автори	Особливість трактування
Група міжнародних організацій	Institute of risk management, Microsoft, National Institute of Standards and Technology, UpGuard	Спільною ознакою дефініцій поняття даної групи є характерність даного ризику саме для підприємств та організацій, а також їхніх мереж і систем, додаючи можливість витоку даних чи порушення їх конфіденційності через кіберінцидент в організації.
Група урядових інституцій	CISA, ENISA, НБУ	Поняття вказаної групи має законодавчий характер, тобто використовується в офіційних інституційно-правових документах і законодавстві, окреслюючи межі існування та поширення даного ризику.
Група страховиків та страхових брокерів	Colonnade, InsArt Insurance Broker, Polis24	Основний акцент визначення поняття стосується спектру джерел ризиків, підкреслюючи потенційний обсяг доступного покриття, що зможе отримати страхувальник у разі укладання договору страхування з конкретним страховиком чи брокером.
Група науковців	Абрамова А. С., Волосович С. В., Клапків Л. М., Гудзь О. Є., Дубина М. В., Середюк І. О., Білоус Н. В., Пікус Р. В., Бабенко Ю.В.	Хоча підходи до формування поняття відрізняються, особливістю визначення поняття є його розподіл на структурні елементи, такі, як джерело (причина), наслідок (втрати, збитки), умови (процес, сфера).

Джерело: складено автором на основі [1, с. 3; 12, с. 103; 14, с. 3; 21, с. 184; 55, с. 103130; 68; 87; 92; 97; 98; 135; 139; 165; 232]

Проаналізувавши наявні підходи до трактування поняття «кібер-ризик», доцільним вважаємо використання структурного підходу для формулювання власного визначення, актуального в умовах цифрової економіки, за яким кібер-ризик – це ймовірність настання події або групи подій внаслідок зловмисного втручання в IT-системи, бізнес-процеси, технології, програмне забезпечення, канали передачі даних, що призводить до отримання фінансових та / або репутаційних збитків через порушення стабільності, вимушену зупинку діяльності, конфіденційності та / або цілісності інформації фізичних і юридичних осіб.

Розуміючи ключові особливості трактувань понять «інформаційний ризик», «цифровий ризик» та «кібер-ризик», варто окреслити можливість одночасного використання цих понять, однак для характеристики ризиків у різні періоди цифрового розвитку економіки (Рис. 1.3).

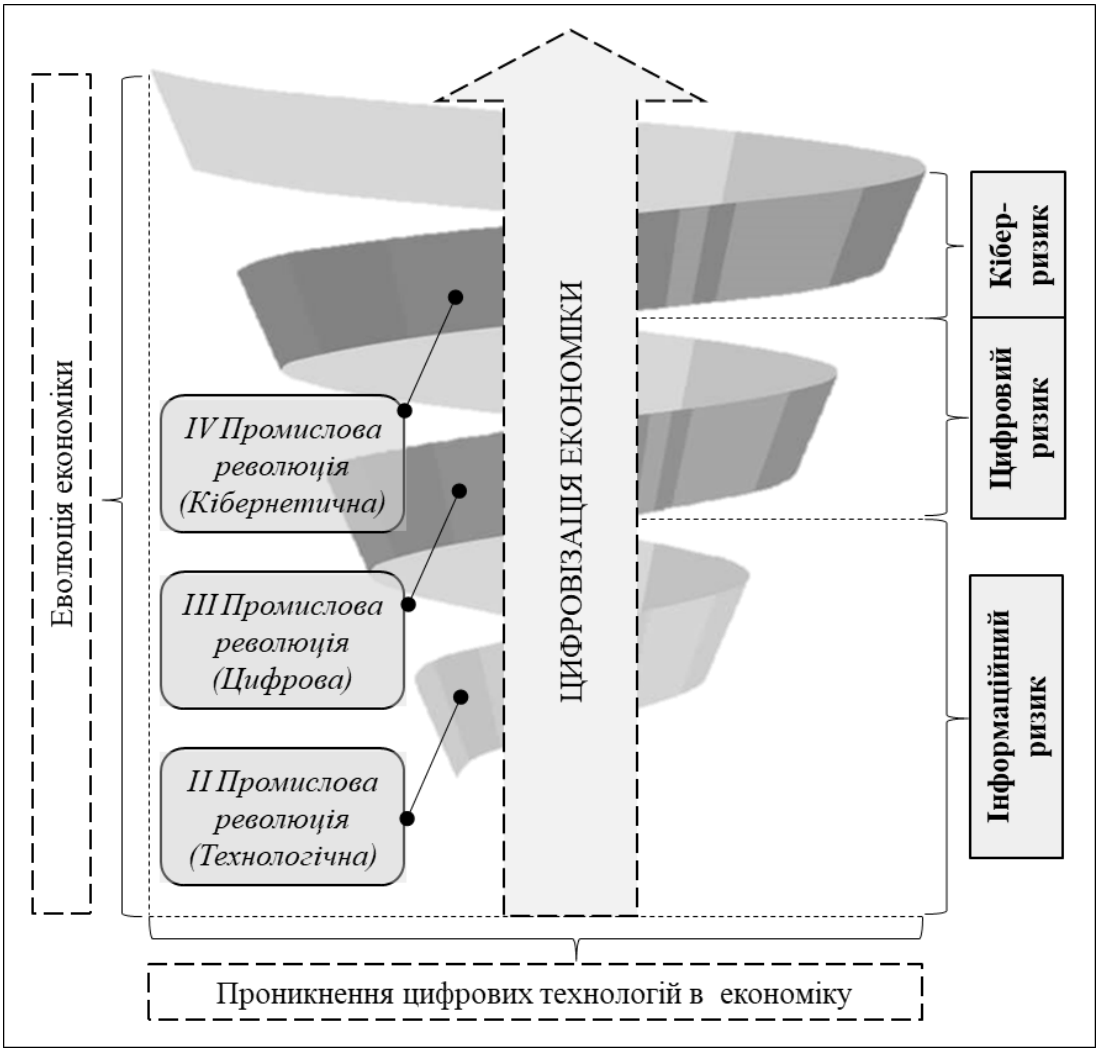


Рисунок 1.3. Спіральна модель виникнення поняття «кібер-ризик»

Джерело: розробка автора

Видозміна ризику характерно відстежується при використанні порівняльно-історичного методу. Цифровізація економіки відбувалась під впливом інновацій, створених у рамках певної промислової революції, що розширювали джерела ризиків. Загалом існує чотири промислові революції:

1. Перша промислова революція (індустріальна) відбувалась у період з другої половини 18 ст. до середини 19 ст. та включала перехід від ручної

ремісничої праці до машинного виробництва на заводах і фабриках. На цьому етапі відсутні ризики, пов’язані з цифровими технологіями.

2. Друга промислова революція (технологічна) відбувалась у період з другої половини 19 ст. до початку 20 ст. та оптимізувала початок Першої промислової революції шляхом розвитку індустріального виробництва завдяки науці й техніці. В цей період стався перехід з вугілля на нафту, була винайдена й поширена електроенергія, електродвигун, телефон тощо. Ці події засвідчили особливу цінність інформації, адже більшість технологій намагались зберігати в таємниці задля уникнення конкуренції чи з міркувань безпеки. Відповідно через загрозу викрадення, спотворення або поширення інформації виникає інформаційний ризик.

3. Третя промислова революція (цифрова) відбувалась у період з 1980-х до початку 21 ст. та включала масовий перехід до цифрових технологій. Значущими подіями цього періоду стало широке використання обчислювальної техніки, комп’ютерів, мобільних телефонів та інших пристроїв. Прискорив процес цифровізації й розвиток мережі «Інтернет», що дало змогу підтримувати з’єднання в режимі онлайн із будь-якої точки світу. Отже, під впливом ще більшого поширення нових технологій і створення умов для їх доступності виникає поняття «цифровий ризик».

4. Четверта промислова революція (кібернетична, Індустрія 4.0, Промисловість 4.0) почалась у перші роки 21 ст. і триває досі. За цей час відбувся стрімкий розвиток автоматизації бізнес-процесів та виробництва, обміну інформацією та зменшення частки людського ресурсу в усіх процесах. До того ж описані зміни часто існують у межах певної автономної системи, що додатково зменшує участь людини в економічних процесах. Таким чином у цей період виникає поняття «кібер-ризик», що стає особливо актуальним у сучасному цифровому світі.

Оскільки Індустрія 4.0 триває, сьогодні спостерігається активне нарощування цифрових технологій і збільшення їх застосування. Проте ризикованість таких дій не залишається поза фокусом уваги науковців.

Щороку міжнародна фінансова група Allianz готує рейтинг актуальних ризиків сучасності, базуючись на результатах широкого аналізу фахівців та експертів у різних галузях, на основі якого формується прогноз на коротко-, середньо- й довгострокову перспективу. Відповідно до вказаного переліку, протягом 2014–2023 років кібер-ризик постійно входив до переліку десяти найбільш критичних і популярних ризиків та щороку підвищував позицію в рейтингу. Так 2014 року кібер-ризик займав восьму позицію, 2017 року піднявся на третю позицію, в 2020 році вийшов на першу позицію та залишався на ній і в 2023 році (рис. 1.4).

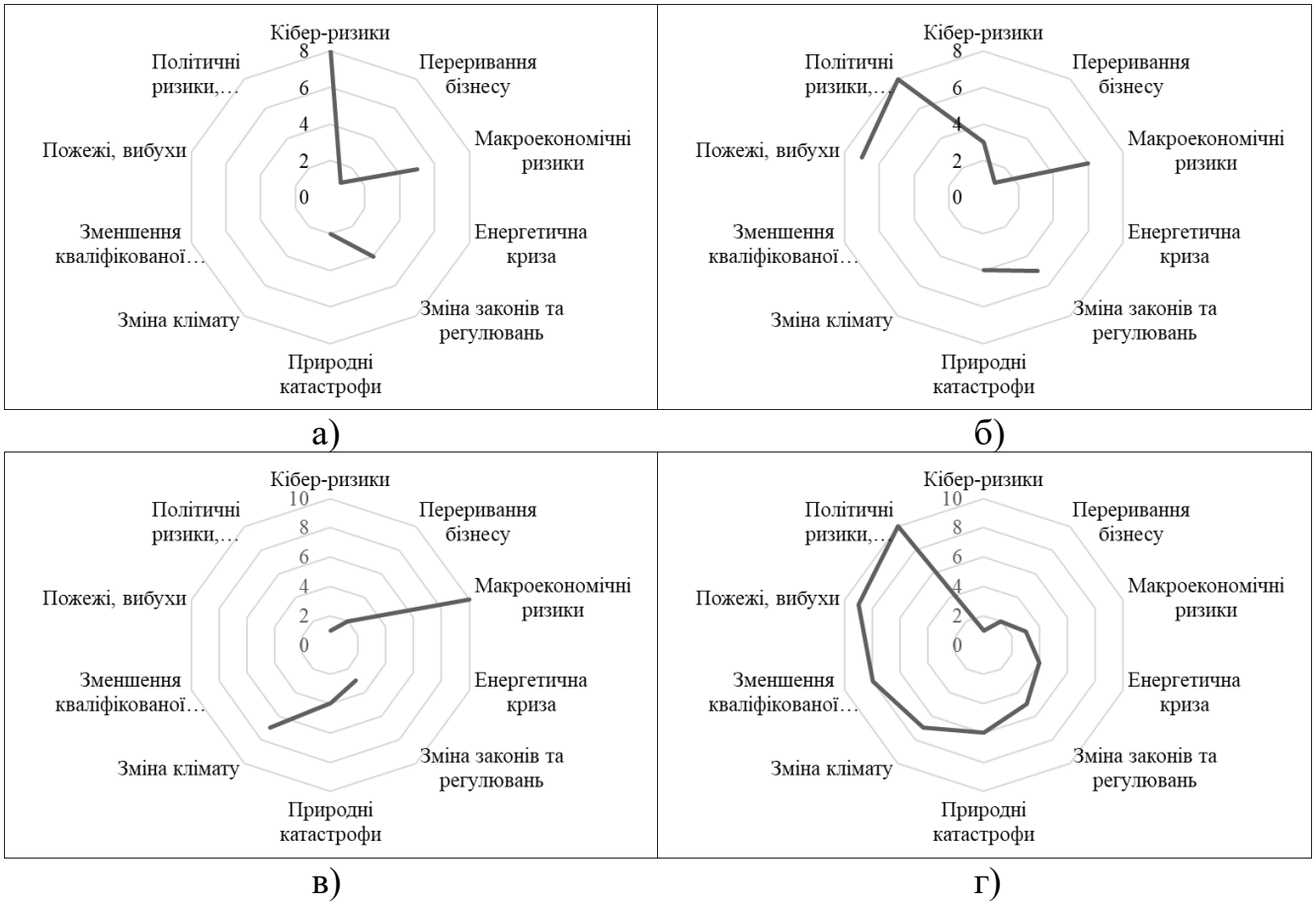


Рисунок 1.4. Трансформація місця кібер-ризиків у глобальному рейтингу ризиків за 2014–2023 рр.: рейтинг ризиків станом на: а) 2014 рік, б) 2017 рік, в) 2020 рік, г) 2023 рік.

Джерело: складено автором на основі [101-104]

Таким чином в умовах сучасного цифрового світу і цифрової економіки кібер-ризики становлять високий рівень загроз, розмаїття яких зростає з кожним

новим етапом розвитку цифрових технологій, тому важливими є дослідження особливостей через класифікацію видів кібер-ризиків для ефективного управління ними.

За даними компанії Imperva, яка є лідером у галузі кібербезпеки, в умовах глобальної цифровізації актуальними класифікаційними ознаками є ініціатори кібер-ризиків, включаючи держави чи державні організації, терористичні організації (міжнародні), злочинні угруповання (локальні), хакери, автономне зловмисне програмне забезпечення; інструменти реалізації кібер-ризиків, а саме: кібератаки, згенеровані програмним забезпеченням, соціальна інженерія, розкриття конфіденційної інформації, Man-in-the-Middle-атаки, Denial-of-Service-атаки, ін'єкційні атаки [141].

Досліджуючи страхування кібер-ризиків як спосіб управління ними в умовах цифрової економіки, Нагайчук Н. Г., Третяк Н. М. і Ткаленко О. В. виділяють такі види страхових кібер-ризиків за особливістю реалізації: ризик порушення конфіденційності інформації та / або її використання; ризик отримання фінансових реквізитів організації та / або її клієнтів; ризик привласнення фінансових активів у фінансових установах; ризик деанонімізації даних платіжних карт та викрадення засобів із них; ризик людської похибки при обробці інформації; ризик порушення стабільної діяльності організації та її інформаційних систем; ризик публікації недостовірних даних, що шкодять репутації організації; ризик знищення носіїв інформації [51, с.103].

Більш розширену класифікацію кібер-ризиків пропонують В. Муравський, Н. Починок та В. Фаріон у межах дослідження кібер-ризиків у бухгалтерському обліку, окреслюючи такі класифікаційні ознаки, як умисел, режим реалізації, інформаційно-фінансовий інтерес, локалізація меж дії кібер-ризику, провокативний суб'єкт, походження або джерело, мета, цілі, масштаб наслідків, аспект впливу загроз, форма прояву, законність (ознака кримінальних дій чи технічні збої), тривалість, видимість (виражена або прихована), ймовірність настання, можливі наслідки [196, с.139-140].

Оскільки цифровізація має нерівномірний характер поширення, вважаємо доцільним поглибити систему класифікації кібер-ризиків за рівнями економіки, на яких вони реалізовуються:

- макроекономічні кібер-ризики, пов'язані з діями та процесами в глобальній цифровій економіці. До таких ризиків відносимо масштабні кіберзагрози, наслідками яких є порушення стабільності економіки окремих країн чи ринків, а також суб'єктів фінансового сектору (міжнародні фінансові установи, банки, посередники тощо);
- мезоекономічні кібер-ризики, актуальні для інституцій, корпорацій та бізнесу даного рівня. Характерними ризиками є зупинка виробничого процесу, провокування обмеженості ресурсів, негативний вплив на ланцюги постачання;
- мікроекономічні кібер-ризики, що реалізовуються в межах діяльності компаній та приватних осіб. Такими ризиками є злам рахунків, виведення чи ануляція криптоактивів; соціальна інженерія.

Незважаючи на широкий спектр наявних ознак класифікації кібер-ризиків, пов'язаних зі способами реалізації ризику, малодослідженою є секторальна ознака. Відповідно до запропонованої ознаки виділяємо:

- ризики фінансового сектору, що включають ризики кібератак на банківські, фінансові установи та платіжні системи, біржі, ринки;
- ризики енергетичного сектору, до яких належать ризики кібератак на енергетичну інфраструктуру, системи контролю та передачу інформації даного сектору, логістичну інфраструктуру транспортування енергетики різних типів;
- ризики екологічного сектору, де типовими є кібератаки на програмне забезпечення моніторингу і контролю якості різноманітних екологічних сфер, втручання в діяльність інформаційних систем, що використовуються для управління відходами й викидами, автоматизований збір екологічних проб;
- ризики сектору охорони здоров'я, до яких належать ризики кібератак на медичні заклади, медичні технології, медичні дані, програмне забезпечення, що використовується для лікування і медичних досліджень;

- ризики сектору виробництва, до яких відносимо ризики кібератак з метою переривання роботи підприємства, збоїв автоматизованого виробництва, зберігання продукції;

- ризики сектору державного управління, до яких належать ризики кібератак на урядові органи, органи самоврядування та, відповідно, на системи, які вони використовують: державні та соціальні дані, державні таємниці, стратегічні плани розвитку;

- ризики оборонного сектору, які включають ризики підриву обороноздатності країни в кіберпросторі.

Останній сектор набув особливого значення в рамках гібридної війни Російської Федерації проти України. До кібер-ризиків оборонного сектору відносимо п’ять характерних підкатегорій:

1. Кібершпигунство – зловмисні дії для отримання засекреченої інформації про військові плани, прогнози, оцінку противника; технології, що використовуються чи виготовляються; стратегії розвитку військової сфери.

2. Кібератаки на канали військової комунікації чи несанкціоноване підключення до них – вплив на супутникові системи, що забезпечують військовий зв’язок; втручання, перешкоджання, вимкнення наземних військових каналів зв’язку.

3. Кібератаки на військову інфраструктуру – вплив на електронні системи, енергетичні мережі, заводи, які є елементами військової інфраструктури; на центри навчання та перекваліфікації військових.

4. Кібератаки на цифрові військові системи – зловмисні дії для спотворення, видалення, підміни інформації, яку використовують військові; вплив на системи моніторингу поточної ситуації на лінії фронту.

5. Кібератаки на зброю – дії, спрямовані на системи, що відповідають за керування та наведення ракет; блокування чи втручання в управління військовими літаками, транспортом і безпілотниками.

6. Цифрова пропаганда – комплекс дій, спрямованих на дискредитацію військового керівництва; викривлення інформації про бойові дії, противника та

військову систему. Кінцевою метою таких дій є підрив обороноздатності країни в середньо- і довгостроковій перспективі та деморалізація особового складу військ.

Отже, гібридна війна, що є наслідком глобальної цифровізації, розширила спектр кібер-ризиків, актуальних для оборонної сфери, в рамках запропонованого підходу класифікації даних ризиків за секторальною ознакою (рис. 1.5).

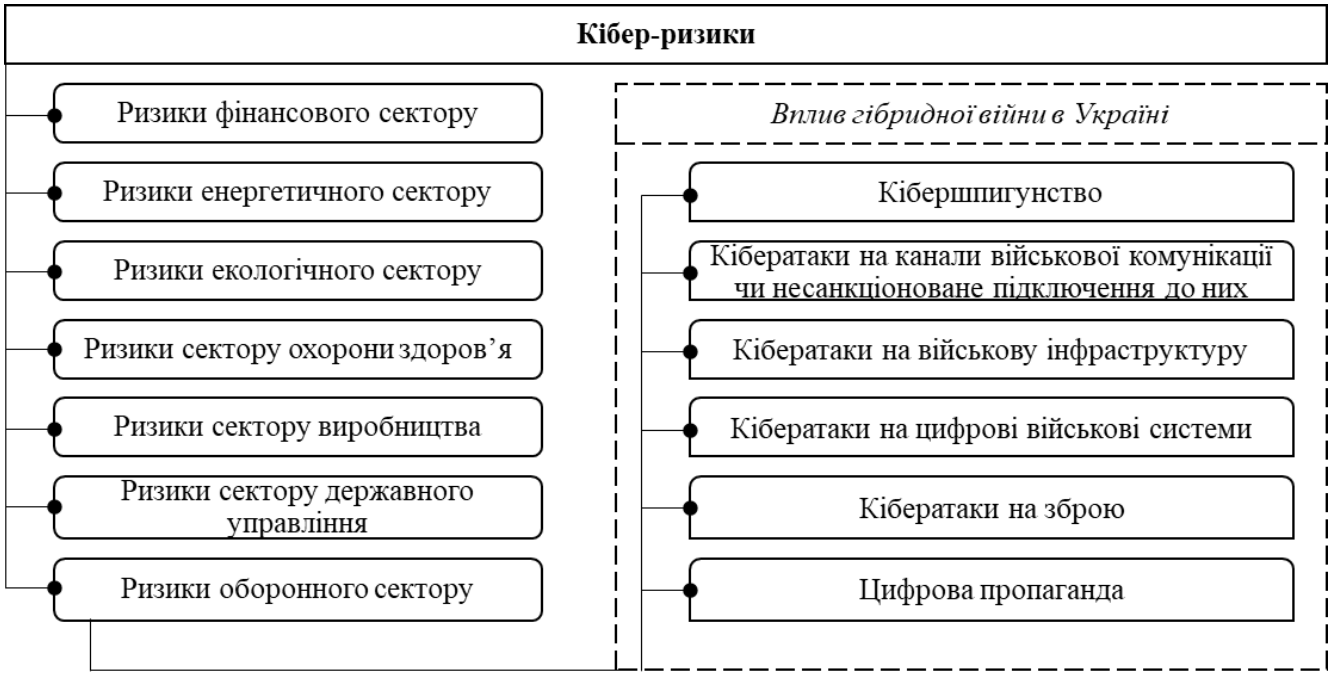


Рисунок 1.5. Класифікація кібер-ризиків за секторальною ознакою

Джерело: розробка автора

Безсумнівно, всі класифікаційні ознаки кібер-ризиків, запропоновані науковцями, є достатньо ґрунтовними та взаємонезалежними. Наукове пізнання описаних підходів дає додаткові можливості суб'єктам цифрової економіки:

- ідентифікувати різноманітність загроз сучасного цифрового світу, їх особливостей та наслідків;
- формувати персоналізовану комплексну стратегію захисту від оцінених кібер-ризиків, спрямовану на посилення кібербезпеки суб'єкта;
- адаптувати діяльність суб'єкта до викликів, що виникають під впливом цифровізації через підвищення пенетрації цифрових технологій у процеси;
- створювати систему міжгалузевих та міжнародних відносин у сфері кібербезпеки з метою обміну інформацією та технологічними інноваціями.

Незважаючи на багатовекторність класифікації кібер-ризиків, додаткового розвитку потребує систематизація їх видів саме в умовах цифрової економіки. На рис 1.6. відображено розширену систематизацію таких ризиків на основі запропонованого підходу до класифікації кібер-ризиків за рівнями економіки.

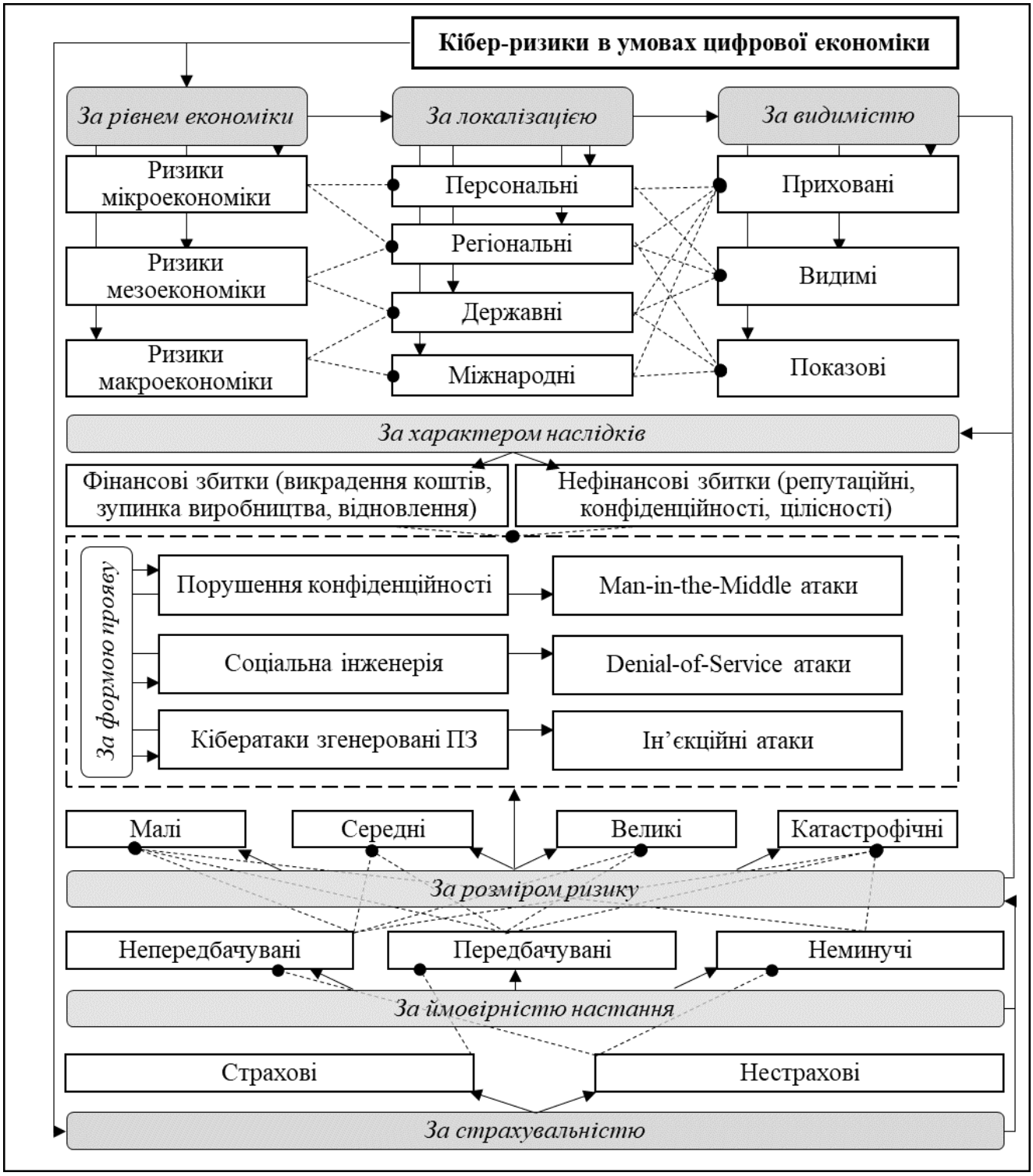


Рисунок 1.6. Класифікація кібер-ризиків в умовах цифрової економіки

Джерело: розробка автора

Варто відзначити, що запропонована класифікація включає в себе ознаку за страхувальністю ризиків як один з методів управління ризиком, оскільки в умовах постійних та стрімких змін в цифровому просторі страховикам варто чітко розмежовувати кібер-ризики, що доцільно чи недоцільно приймати на страхування. У межах цієї ознаки виділяємо:

- страхові ризики, що підпадають під критерії страхування та наслідки яких можуть бути включені до страхового покриття в межах дії страхового полісу;
- нестрахові ризики, що не підпадають під критерії страхування та не можуть бути прийняті страховиком для страхування, співстрахування, перестрахування.

Описане графічне уявлення про фасетний взаємозв'язок видів кібер-ризиків відображає класифікаційну ознаку за формою прояву як центральну, тобто будь-яка інші ознака може бути розширена на підгрупи ризиків саме за формою прояву. Дана концепція враховує потенційний розвиток цифрових технологій та збільшення спектру їх застосування в економіці, відповідно урізноманітнення форм прояву кібератак зумовить розширення підгруп інших ознак через наявну підпорядкованість.

Отже, проведене дослідження природи кібер-ризику в умовах цифрової економіки дало змогу вдосконалити та доповнити наявні теоретико-методологічні засади визначення кібер-ризику в умовах цифрової економіки: запропоновано визначення поняття «цифрова економіка» як приклад цифрової трансформації; доповнено визначення поняття «кібер-ризик» як константи глобальних процесів цифровізації економіки; систематизовано підходи до виокремлення видів кібер-ризиків та доповнено узагальнену класифікацію кібер-ризиків з використанням фасетного підходу на основі ознак рівня економіки та сектору реалізації ризику; зафіксовано значущість ознаки кібер-ризиків за страхувальністю в системі класифікації даних ризиків в умовах цифрової економіки.

1.2. Сутність та особливості страхування кібер-ризиків як об'єктивного наслідку цифровізації економіки

Усвідомлення наявності кібер-ризиків та проведення ідентифікації їх особливостей є базовим етапом створення стратегії захисту від них. Проте в сучасній системі управління ризиком важливим компонентом є страхування як один з видів управління ним. Швидкий темп розширення переліку сфер, що нарощують використання сучасних технологій та інновацій, вимагає розвитку напрямку їх страхування. Наявна науково-методична база страхування кібер-ризиків містить певні прогалини, тому потребує додаткового вивчення й удосконалення.

При аналізі підходів до визначення сутності страхування кібер-ризиків було відзначено два поняття: «страхування кібер-ризиків» та «кіберстрахування» як інструменти страхового захисту.

Однак у сучасній науковій думці відсутній компаративний аналіз цих понять, тому даний аспект є важливим напрямком дослідження. Для здійснення означеного порівняльного аналізу варто розглянути наявні підходи до позиціонування страхування кібер-ризиків зарубіжних та вітчизняних учених.

Учені, які вивчають поняття «страхування кібер-ризиків», використовують метод зіставлення існуючих трактувань поняття, на основі якого конструюють власне, або метод синтезу, відповідно до якого формулюють власне визначення лише в межах персонального дослідження сутнісних характеристик явища без критичного аналізу інших дефініцій.

Науковці Р. В. Пікус та Ю. Л. Лапенко відзначили неповноцінність наявних визначень поняття «кіберстрахування» через відсутність результату процесу страхування в них на основі аналізу понять «страхування кібервідповідальності», «страхування кібербезпеки», «страхування кібер-ризиків» та «кіберстрахування». Окремо було вказано на важливість наслідків використання даного виду страхування для учасників страхової угоди з метою конструювання повнішого визначення категорії [55, с.136].

Ґрунтовною є праця А. С. Шолойко, в якій запропоновано компонентний аналіз визначення «кіберстрахування» через виділення частин дефініції – суть, зміст та результат явища. Компонент «суть явища» включає деталізацію на страховий продукт, інструмент, форму покриття, страховий поліс / контракт, метод захисту. Для критичної оцінки усталених трактувань за даним підходом здійснюється рейтингування визначень за наявністю перелічених компонентів у ньому. В дослідженні також було відзначено актуальність кіберстрахування як наслідку трансформації з простого страхового продукту в інноваційний напрямок страхування через цифровізацію економіки [95, с.99–103].

Трансформацію дефініції «кіберстрахування» під впливом інституційних змін в економіці описує Н. Кшетрі. Науковець зазначає, як впливали причини та наслідки інституційних змін в економіці, а також оновлені інструменти її регулювання на формулювання «кіберстрахування» у різні періоди таких трансформаційних змін [183].

Аналіз праць учених, які вивчають сферу страхування кібер-ризиків у рамках конкретних завдань персонального дослідження, виявив розгалуженість трактувань поняття через різнопланове розкриття їх особливостей (Додаток В).

Для розв’язання завдання, що передбачає виявлення тотожності понять «страхування кібер-ризиків» та «кіберстрахування» було здійснено систематизацію наявних дефініцій за типовими атрибутами (Таблиця 1.3):

- страховий продукт;
- передача ризику;
- захист від ризиків;
- суб’єкт є фізичною особою;
- суб’єкт є юридичною особою;
- об’єктом є технології, ПЗ;
- об’єктом є дані суб’єкта і третіх осіб, їх цілісність та конфіденційність;
- сферою діяльності суб’єкта є кіберпростір;
- джерело ризику – кіберінцидент;

- компенсація через відшкодування збитків.

Таблиця 1.3

Систематизація понять «страхування кібер-ризиків» та «кіберстрахування» за дефініційними атрибутами

Атрибут / Автор	Страховий продукт	Передача ризику	Захист від ризиків	Суб'єкт є фізичною особою	Суб'єкт є юридичною особою	Об'єктом є технології, ПЗ	Об'єктом є дані суб'єкта і третіх осіб, їх цілісність та конфіденційність	Сферою діяльності суб'єкта є кіберпростір	Джерело ризику – кіберінцидент	Компенсація через відшкодування збитків
Поняття «кіберстрахування»										
Böhme R., Kataria G.			■			■			■	■
Mott G. et al			■						■	■
Schütz F. et al	■				■				■	
Гудзь О. Є.	■		■	■	■	■	■	■	■	
Дубина М. В., Середюк І. О., Білоус Н. В.		■		■	■	■			■	
Нагайчук Н. Г., Третяк Н. М., Ткаленко О.	■		■		■	■	■	■		
Пікус Р. В., Бабенко Ю. Л.	■	■	■	■	■	■	■		■	■
Морозова Л. С., Друхан Д. А.			■					■		
Шолойко А. С.	■	■	■	■	■			■		■
Наявність атрибуту	+	+	+	+	+	+	+	+	+	+
Поняття «страхування кібер-ризиків»										
Desjardins			■		■	■	■			
Malwarebytes			■		■	■	■		■	
OECD		■	■	■	■				■	■
Trendmicro	■			■			■	■	■	
Іванова Т. Г.								■	■	
Ксьонжик І. В., Жовта Н. А., Павліна А. А.									■	■
Наявність атрибуту	+	+	+	+	+	+	+	+	+	+
Наявність атрибуту в обох групах	+	+	+	+	+	+	+	+	+	+

Джерело: складено автором на основі [14, с.5; 21, с.190; 28, с.65; 41, с.136; 50, с.25; 51, с.102; 55, с.136; 95, с.103; 107, с.2; 110, с.37; 116, с.523; 129; 131; 154; 230; 231]

Запропонована систематизація понять «страхування кібер-ризиків» та «кіберстрахування» дає змогу назвати унікальні типові атрибути визначень та використати їх для побудови власного трактування поняття.

Оскільки визначення науковців відрізняються між собою через різні методи наукового пізнання та конструювання визначень, варто порівнювати множини унікальних атрибутів кожної групи.

Додатково варто відзначити, що наявність даних атрибутів у дефініції: суб'єкт-фізична особа та суб'єкт-юридична особа – було відзначено в таких авторів: О. Є. Гудзь (оскільки в трактуванні використано категорію «економічні суб'єкти», які можуть бути як фізичними, так і юридичними особами та не потребують додаткової деталізації); М. В. Дубина, І. О. Середюк, Н. В. Білоус (було використано категорію «страхувальник», який, за аналогією, може бути як фізичною, так і юридичною особою).

За підсумком проведеної систематизації вважаємо поняття «страхування кібер-ризиків» тотожним поняттю «кіберстрахування», адже множина унікальних атрибутів визначення першої категорії відповідає аналогічній множині другої. Додатково було встановлено, що наповненість категорій зростала з розвитком наукової думки за тематикою страхування кібер-ризиків, тому майбутні дослідження окремих детермінант даного виду страхування допоможуть сформувати більш повне визначення поняття на основі віднайдених атрибутів.

За визначенням, наведеним у пункті 1 статті 1 Закону України «Про страхування», «страхування – це правовідносини щодо захисту страхових інтересів фізичних та юридичних осіб при страхуванні ризиків» [73]. Ґрунтуючись на законодавчому визначенні та аналізі трактувань науковців досліджуваного поняття, вважаємо, що метою страхування кібер-ризиків є захист страхового інтересу фізичних та юридичних осіб при страхуванні кібер-ризиків.

Зважаючи на те, що правовідносини припускають взаємодію принаймні між двома сторонами, базовими суб'єктами страхування кібер-ризиків є:

- страхувальник, захист страхового інтересу якого є метою страхування кібер-ризиків;

- страховик, якому страхувальник передає кібер-ризик на страхування.

Однак сучасна страхова система є регульованою, відповідно потребує участі держави як суб'єкта страхування, що може бути представлений спеціалізованою державною інституцією. В українській страховій системі таким регулятором є Національний банк України.

Ще одна група загальних суб'єктів страхування – страхові посередники: прямі, тобто страхові брокери (включаючи перестрахових брокерів) та страхові агенти (включаючи субагентів та додаткових страхових агентів); непрямі, тобто банки, поштові відділення, магазини, фінансові консультанти, аудитори тощо.

Оскільки мета страхування кібер-ризиків повністю підпорядковується загальній меті страхування, вважаємо базові суб'єкти страхування відповідними для страхування кібер-ризиків.

Проте страхування кібер-ризиків вимагає участі специфічних суб'єктів, які володіють достатньою експертизою для оцінки стану страхувальника саме у сфері цифрових технологій, інформації та кібербезпеки. Така вимога пояснюється складністю оцінки кібер-ризиків страхувальника та їх потенційних наслідків. Відповідно для страхування кібер-ризиків актуальною є розширена система суб'єктів (рис. 1.7).

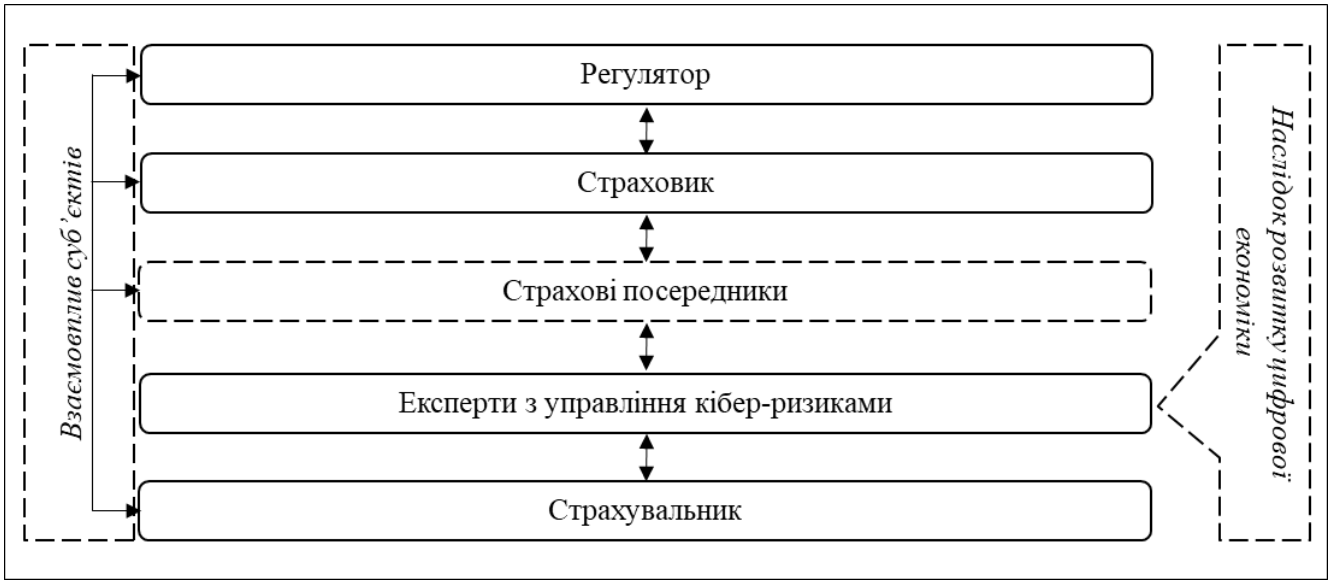


Рисунок 1.7. Суб'єкти страхування кібер-ризиків

Джерело: складено та доповнено автором на основі [81]

На нашу думку, включення експертів з управління кібер-ризиками до системи суб'єктів страхування стало наслідком процесів цифрової трансформації.

Об'єктами страхування кібер-ризиків є майнові інтереси, пов'язані з майном страхувальника у різному вигляді (зокрема, цифрові технології; інформаційні системи; програмне забезпечення; системи обміну інформацією; особисті дані страхувальника) та відповідальністю перед третіми особами (зокрема відповідальність за порушення конфіденційності та цілісності даних третіх осіб; за вплив на стабільну діяльність третіх осіб).

Галузь страхування визначає вид страхування залежно від його об'єктів. У своєму дослідженні про доцільність страхування кібер-ризиків Л. Міллер зазначає, що покриття полісу страхування для організації формується на основі актуальних для неї ризиків, які можуть бути виражені в майновій формі та формі кібервідповідальності [192, с.152-161].

Аналогічною до вищезазначеного підходу є позиція науковців Р. В. Пікус, Ю. Л. Бабенко, Л. С. Морозової та Д. А. Друхан, які характеризують страхування кібервідповідальності та майнове страхування потенційних кібератак як можливі форми страхового покриття кібер-ризиків, відповідно виокремлюючи галузі майнового страхування та страхування відповідальності [55, с.136; 74, с.36].

Оскільки попередньо було визначено, що джерелами кібер-ризиків є не лише цифрові технології, інновації та програмне забезпечення, а й інформація суб'єкта і третіх осіб, що використовується суб'єктом, та канали передачі такої інформації, тому галузями страхування кібер-ризиків визначаємо страхування майна та страхування відповідальності.

Дискусійним залишається питання віднесення страхування кібер-ризиків до галузі особистого страхування, де об'єктом є життя та здоров'я людини. Активний розвиток цифрових технологій розширив можливості сучасної медицини, надавши широкий спектр інструментів, що підтримують здоров'я і життя людини: кардіостимулятори, імплантовані дефібрилятори, інсулінові помпи, нейрочіпи, роботи для малоінвазивної хірургії тощо. Однак сьогодні використання перелічених технологій можливе лише після проведення клінічних

тестувань з дотриманням усіх вимог реалізації такої продукції, що обмежує випуск і продаж дефектних пристроїв (ISO/TC 150, Директива ЄС 90/385/ЕЕС від 20 липня 1990 р.), та отримання спеціальної ліцензії, що підтверджує повну безпечність технології для людини [179; 223]. Тому поки використання описаних технологій захищене від зовнішніх втручань, кібер-ризики злому, зміни конфігурацій чи зупинки – не актуальні для даної сфери, а отже, їх страхування є недоцільним.

У процесі аналізу сучасних наукових досліджень на тему страхування кібер-ризиків більшість авторів відзначали його специфічність та інноваційність, однак підходи до обґрунтування даної тези відрізняються.

Ґрунтовний аналіз особливостей страхування кібер-ризиків було здійснено А. Маротта, Ф. Мартінеллі, С. Нанні, А. Орландо та А. Яцюхіним. Науковці окреслили ключові особливості даного явища, а саме:

- еволюційність, тобто розвиток даного підвиду страхування залежно від розвитку цифрових технологій;
- нерозвинуте законодавство, тобто відсутність або низький розвиток інституційно-правової бази, що регулює цей вид страхування;
- нестачу інформації, тобто неповноту даних для проведення актуарних розрахунків;
- обмеженість часу для виставлення претензії щодо страхового випадку, тобто наслідки після кіберінциденту можуть проявитися після закінчення дії страхової угоди, адже часто факт втручання в діяльність певної системи залишається непоміченим;
- наявність великої кількості винятків страхування, що виникають через специфіку діяльності страхувальника або його технічного забезпечення [136, с.37-52].

Інші особливості описують К. Бінер, М. Елінг та Д. Х. Вірфс у своїй роботі з питань оцінювання страхувальності кібер-ризиків. До них, зокрема, відносять формування покриття страхування на основі гіпотези про можливість як навмисних, так і випадкових дій людей, систем і технологій, внутрішніх і

зовнішніх факторів, наслідки яких призводять до підриву стабільності страхувальника [108].

Додатково Н. Г. Нагайчук, Н. М. Третяк та О. В. Ткаленко виділяють усесторонній аналіз страхувальника, який включає аналіз його непрямих характеристик, зокрема, таких: взаємодія з інформацією, модель ризик-менеджменту компанії, оцінювання рівня цифрової грамотності персоналу, сховища даних, система моніторингу і контролю кібербезпеки [51, с.108].

Ще одну особливість відзначають Л. С. Морозова та Д. А. Друхан, яка виявляється в складності доведення наявності взаємозв'язку між настанням страхового випадку, пов'язаного з кібер-ризиками, та отриманими збитками. Додатковим ускладненням процесу є оцінка наслідків страхового випадку та розрахунок збитків [50, с.36].

Групи вчених: Р. В. Пікус, Ю. Л. Бабенко та В. П. Ільчук, О. М. Парубець, Д. О. Сугоняко – сходяться на думці, що формування попиту на послуги страхування кібер-ризиків відбувається водночас із розвитком кіберзагроз. Тобто страхувальники усвідомлюють потребу в такому страхуванні лише після настання кіберінциденту, що вплинув на стабільність їхньої діяльності [55, с.136; 29].

Окрім того, науковці виділяють нерозвиненість законодавства у сфері страхування як особливість, що гальмує еволюцію інноваційних видів страхування, відповідно стримуючи регіональний розвиток страхового ринку в цілому [170, с.86].

Оскільки дослідження страхування кібер-ризиків стартували від початку IV Промислової революції і тривають досі, а перелік особливостей постійно розширювався та змінювався, відповідно актуальною є необхідність їх структурування залежно від аспекту прояву. Для цього визначаємо характерні класифікаційні ознаки особливостей страхування кібер-ризиків (рис. 1.8):

- обмеження страхової діяльності;
- складності аквізиційного процесу;
- комплікація прийняття ризику;
- аспекти страхового продукту.

Рисунок 1.8. Класифікація особливостей страхування кібер-ризиків за аспектами прояву

Джерело: складено та доповнено автором на основі [29; 50, с.36; 51, с.108; 55, с.136; 108; 136, с.37-52;]

Виявлення економічної сутності страхування кібер-ризиків відбувається через розкриття його специфічних функцій. До загальних функцій страхування, що актуальні для страхування кібер-ризиків, належать: ризикова – прийняття ризиків страхувальника страховиком на певних умовах; резервна – створення страхових фондів; компенсаційна – відшкодування завданих збитків страхувальнику; превентивна – реалізація комплексу заходів для обмеження потенційних ризиків; репресивна – підтримка фінансової безпеки страхувальника через надання відшкодування в разі настання страхового випадку; інвестиційна – генерація додаткового доходу страховиком у разі розміщення страхових внесків страхувальників [84, с.32-35].

Проте вищезазначені особливості страхування кібер-ризиків розширюють перелік базових функцій, додаючи:

- іміджеву функцію, виражену в зобов'язанні страховика відновити репутацію страхувальника до якісного рівня, який був до настання страхового випадку, якщо це передбачено умовами договору страхування. У межах цієї функції страховик або самостійно розробляє стратегію відновлення іміджу, або покриває відповідні витрати. Стратегія може включати публічне вибачення за інцидент, виправлення некоректно опублікованої / озвученої інформації або відшкодування збитків третім особам, що постраждали від цього, рекламні та маркетингові заходи для повернення ринкових позицій тощо;
- розслідувальну функцію, що передбачає проведення, сприяння розслідуванню страхового випадку або покриття витрат на такі заходи. Оскільки у страхувальників (юридичних осіб) іноді відсутні окремі внутрішні відділи або фахівці з кібербезпеки, то процес пошуку джерела ризику ускладнюється. Страховик використовує для цього отриману інформацію про страхувальника для швидкого виявлення вразливих зон або повторно залучає експертів із кібербезпеки для проведення розслідування та покриває супутні витрати, якщо такі включені до умов договору страхування;
- освітню функцію, оскільки залучення страховиком експертів у сфері кібербезпеки відбувається в рамках процесів, спрямованих на мінімізацію ризиків страхувальника. В такому разі одним із заходів є оцінка цифрової грамотності страхувальника (для фізичних осіб) або персоналу організації (для юридичних осіб) та створення стратегії для її покращення у разі негативних висновків. Покращення цифрової грамотності відбувається шляхом проведення лекцій, семінарів, практичних занять з ідентифікації ризиків та використання освітніх тренажерів. Після завершення такого комплексу заходів експерти проводять повторну оцінку цифрової грамотності, а згодом страховик ухвалює рішення щодо доцільності прийняття на страхування ризиків за оновленими вхідними даними про кібербезпеку страхувальника.

Здійснення функцій страхування кібер-ризиків відбувається за набором правил, що окреслюють його особливості, тобто згідно зі страховими принципами. За аналогією до визначення функцій страхування кібер-ризиків ми визначаємо підпорядкованість останнього загальному поняттю страхування, відповідно належним є використання загальних принципів страхування у сфері страхування кібер-ризиків [25, с.13-15].

До групи принципів, що формують попит на страхові послуги у сфері страхування кібер-ризиків, вважаємо за потрібне додати:

- принцип швидкого реагування, що означає зобов'язання страховика негайно реагувати на випадок кіберінциденту та здійснювати необхідну експертизу його ідентифікації як страхового чи нестрахового випадку, оцінюючи короткостроковий вплив на страхувальника. Акцент на негайності реагування у такому разі пов'язаний з особливістю кібер-ризиків – за короткий проміжок часу (іноді це години або навіть хвилини) страхувальник може зазнати катастрофічних збитків. Для реалізації даного принципу страховики пропонують індикатори моніторингу та контролю стану технологій, систем, надійності каналів передачі даних страхувальника за персонально розробленою методологією разом з експертами у сфері кібербезпеки;

- принцип інноваційності страхових продуктів та послуг, що відображає необхідність використання страховиками новітніх технологій, аналізу великих обсягів даних та розвитку сучасних підходів до ризик-менеджменту кібер-ризиків. Створення інноваційних продуктів та послуг страховими компаніями є симетричним до швидких темпів цифрової трансформації потенційних страхувальників, оскільки відповідає запитам та поведінці споживачів у кіберпросторі.

Для обмеження спекулятивних дій при страхуванні кібер-ризиків до групи принципів потрібно додати:

- сприяння розвитку кіберзахисту, як страховиками, так і страхувальниками, тобто формування та впровадження необхідних заходів, для покращення рівня кібербезпеки останніх. Такі дії направлені на мінімізацію

ймовірності настання кіберінциденту та виявлення поточного стану кібербезпеки потенційних страхувальників, що виключає можливість фальсифікації умов реалізації кібер-ризиків;

- відповідність міжнародним стандартам кібербезпеки, адже у разі створення страховиком власної моделі оцінки стану страхувальника, можуть бути проігноровані загальноприйняті методи аудиту, викладені в міжнародних стандартах кібербезпеки. Страховик може бути зацікавлений в обмеженні спектру потенційних страхових випадків і збільшенні винятків з договору страхування; страхувальник, навпаки, може наполягати на включенні в страхове покриття нетипових кібер-ризиків, які, за трактуванням міжнародних стандартів, сприймаються страховими компаніями як нестрахові. Тому для унеможливлення здійснення спекулятивних дій обох сторін базою для страхування кібер-ризиків є уніфіковані міжнародні стандарти кібербезпеки.

Таким чином, принципи страхування кібер-ризиків доцільно розділити на дві групи: загальні, тобто актуальні для страхування в цілому, та специфічні, що сформувались на основі особливостей даного виду страхування (рис. 1.9).

Рисунок 1.9. Принципи страхування кібер-ризиків

Джерело: складено та доповнено автором на основі [25]

У цілому використання страхування кібер-ризиків позитивно впливає на всіх учасників страхових відносин.

Досліджуючи страхування кібер-ризиків як інструмента ризик-менеджменту, А. Канавас визначає такі переваги для страхувальника: передачу ризику, створення фінансового захисту від можливих збитків, покращення системи моніторингу і реагування на кіберінциденти, а також системи ризик-менеджменту підприємства [182, с.33–34].

Л. Гордон, М. Лоеб та Т. Сохаіл акцентують увагу на доцільності страхування кібер-ризиків для організацій, що використовують великі обсяги даних чи зберігають та / або оброблюють інформацію третіх осіб. У такому разі кіберінциденти можуть скомпрометувати чутливу інформацію, що може бути використана в фінансових махінаціях чи кардингу [163, с.82-83].

Позитивними наслідками запровадження страхування кібер-ризиків у систему ризик-менеджменту підприємства Н. Г. Нагайчук, Н. М. Третяк та О. В. Ткаленко вважають зменшення можливих фінансових та репутаційних втрат у разі настання кіберінциденту, ефективний моніторинг діяльності підприємства та вчасну ідентифікацію кібер-ризиків, покращення ринкових позицій страхувальника через проактивне реагування на ризики [51, с.106].

На думку М. В. Дубини, І. О. Середюк та Н. В. Білоус, створення ефективного захисту від кібератак, як прояву сучасних кібер-ризиків, можливе лише за синергії інструментів страхування кібер-ризиків та внутрішніх систем ризик-менеджменту страхувальника, що забезпечують мінімізацію ймовірності настання кіберінциденту. Відповідно, завдяки такому синтезу відбувається обмеження деструктивних чинників, що впливають на фінансовий результат страхувальника [21, с.191-194].

Також узагальнюючи сучасні наукові підходи до визначення сутності страхування кібер-ризиків, можемо виокремити додаткові його переваги:

- підвищення рівня автоматизації систем страхувальника;
- зниження участі людини в певних бізнес-процесах, відповідно зменшення «ручних» помилок у роботі;

- забезпечення високого ступеня захисту даних страхувальника та його партнерів чи клієнтів;
- запровадження онлайн-систем моніторингу стану страхувальника (його систем, технологій, з'єднання з мережею);
- зниження адміністративних витрат страхувальника, пов'язаних із його кібербезпекою;
- зменшення кількості кіберінцидентів у системі (на локальному та державному рівнях);
- розширення каналів продажу страхових продуктів (експерти у сфері кібербезпеки можуть додатково просувати послуги страхування на партнерських умовах).

На противагу описаним позитивним аспектам запровадження страхування кібер-ризиків науковці виділяють низку загроз та недоліків, які справляють негативний вплив на перспективи розвитку цього напрямку.

На сучасному етапі розвитку П. Ю. Курмаєв, Л. С. Морозова, О. С. Бондаренко та Н. В. Гузаревич виділяють такі проблеми, що стосуються досліджуваного виду страхування: нерівномірність інформації при оцінці кібер-ризику; необхідність персоналізованого підходу до кожного окремого страхувальника через істотну різницю в наявних бізнес-процесах, тобто неможливість уніфікації підходів до страхування для страхувальників однакового роду діяльності; відсутність стандартів регулювання страхування кібер-ризиків; обмеженість страхового покриття через неможливість коректної оцінки певних видів кібер-ризиків; локальна нерівномірність розподілу фахівців у сфері кібербезпеки; швидке зростання розмаїття кібератак [128, с. 71].

Науковці Н. Г. Нагайчук, Н. М. Третяк та О. В. Ткаленко відзначають загрозу того, що страхувальники можуть не виконати рекомендацій з удосконалення своїх систем, наданих експертами з кібербезпеки. Окрім цього, страхувальники можуть вчиняти внутрішні деструктивні дії щодо систем задля отримання страхового відшкодування, тому перед страховиками постає додатковий виклик верифікації кіберінциденту [51, с.104].

Доповненням до цього, на думку Р. В. Пікус та Ю. Л. Бабенко, є наявність низки винятків зі страхового договору, що знижує привабливість страхування кібер-ризиків для потенційних страхувальників. Також ускладненням для страховиків є нестача історичних даних, необхідних для актуарних розрахунків [55, с.138].

Досліджуючи страхування кібер-ризиків, як один з інструментів ризик-менеджменту банків, М. В. Дубина, І. О. Середюк та Н. В. Білоус зауважують неможливість знизити ймовірність настання кіберінциденту до 0%, тому при використанні цього інструменту страхувальники мають усвідомлювати рівень ризику, що залишається [21, с.192].

Проте під час дослідження характерних особливостей страхування кібер-ризиків було відзначено його супутні негативні впливи:

- катастрофічність наслідків кібер-ризиків, які страховик може прийняти на страхування через некоректність актуарних розрахунків;
- високу вартість даного виду страхування, адже воно включає в себе послуги оцінки поточного стану, визначення та розвитку цифрової грамотності, імплементації моніторингової системи ризиків та інші партнерські сервіси;
- вилучення страхувальників із низьким рівнем доходу з кола потенційних страхувальників через високий вхідний поріг вартості страхування кібер-ризиків;
- легітимізацію вимагань, що вказує на покриття страховиком суми, яку вимагає зловмисник для припинення шантажування, якщо подібне передбачено умовами договору. Однак це означає створення певного механізму, який регулюватиме взаємини між страхувальником і вимагачем, що є правовим прецедентом.

Часто в дослідженнях страхування кібер-ризиків науковці визначають вплив страхових продуктів на покращення рівня його захищеності.

Р. Пал доводить вплив залучення страхових продуктів на покращення продуктивності роботи внутрішніх систем страхувальника, розширюючи їхні

вміння розпізнавати потенційні загрози та вчасно підбирати належні інструменти їх нейтралізації [202].

Для А. Маззокколі та М. Налді страхування кібер-ризиків організації є одним із найефективніших видів інвестицій у її кібербезпеку. Підсумки їхніх досліджень свідчать про доцільність страхування кібер-ризиків для бізнесу всіх розмірів, пояснюючи значимість впливу вразливості філій чи відділень на материнську організацію. Залучення страхових інструментів дає змогу значно обмежити кібер-ризики, незважаючи на високу вартість страхування [191, с. 22].

Група вчених, зокрема, С. М. Обушний, К. В. Арабаджи та К. О. Костікова вбачають у страхуванні кібер-ризиків спосіб уникнення ризиків, пов'язаних із кібербезпекою. Вони відзначають особливу актуальність послуг страхування для сучасних FinTech-компаній, адже часто такі компанії не приділяють належної уваги власній кібербезпеці [53, с. 68].

Як бачимо, науковці часто використовують поняття «кібербезпека» в контексті страхування кібер-ризиків. Однак трактування цієї дефініції в умовах цифрової економіки відрізняються між собою.

Б. Мат, С. Д. М. Перо, Р. Вахід та Б. Суле розглядають кібербезпеку як систему, що побудована на категоризації даних, забезпеченні цілісності та конфіденційності даних і дозволів, захищеності пристроїв, послуг, мереж та систем контролю, які є основою цифрової економіки. Питання кібербезпеки фігурує в дослідженні не лише в контексті фізичних та юридичних осіб, а й держави в цілому завдяки ланцюговому ефекту [137, с. 215].

Ще одним дослідженням, що підтверджує вплив кібербезпеки на розвиток цифрової економіки, є праця Ю. В. Кіндзерського. На основі кореляційного аналізу Глобального індексу кібербезпеки та рівня цифрового розвитку відстежується пряма залежність цифрового розвитку економіки від рівня кібербезпеки [37, с. 123].

На думку групи вітчизняних учених, кібербезпека є комплексом засобів захисту від кіберінцидентів сучасної економіки. Водночас вони наголошують на

взаємопов’язаності цих факторів, адже низький рівень кібербезпеки стримує розвиток процесів цифровізації економічних суб’єктів [146, с.2027].

Інший підхід пропонує А. Леаховценсо, визначаючи «кібербезпеку» не лише захистом від кіберінцидентів, а й інструментом управління ризиками. Відповідно, до комплексу кібербезпеки входять стандарти, процедури та інструменти, включаючи заходи для захисту різних інформаційних систем та їх пристроїв від кібератак, а також інструменти управління і протидії ризикам [185, с. 98].

К. С. Теох та А. К. Махмуд під кібербезпекою також розуміють комплекс заходів, що підвищують захищеність суб’єктів та створюють систему управління ризиками в різних сферах. Порівняння доступних інструментів кібербезпеки в декількох країнах вказує на те, що розширення сфер їх застосування стимулює розвиток цифрових сервісів, а тому й цифрової економіки [222, с.141-143].

З огляду на вищезазначене, якщо для певного суб’єкта господарювання існує актуальний кібер-ризик, одночасно з кібербезпекою під загрозу потрапляє і його фінансова безпека, оскільки наслідком кіберінциденту є прямі або непрямі втрати, що в кінцевому вигляді набувають вияву втраченої економічної вигоди.

Ґрунтовне дослідження фінансової безпеки в умовах цифрової економіки здійснив З. С. Варналій. Відповідно до проведених досліджень, науковець окреслює національну безпеку держави як багатоступеневу структуру. Згідно з даним підходом, фінансова безпека є частиною економічної безпеки, яка так само є структурним елементом національної безпеки держави [8, с.92].

Поглиблюючи досліджуваний рівень фінансової безпеки, З. С. Варналій та А. М. Мехед розглядають мікрорівень, тобто фінансову захищеність суб’єктів господарювання. Дослідники вважають, що завданнями підприємств в умовах цифрової економіки є, зокрема: забезпечення комплексу заходів із виявлення загроз, підвищення цифрової компетентності персоналу та перевірка рівня кібербезпеки суб’єкта [9, с.59].

Також науковці відзначають, що запровадження системи ризик-менеджменту організаціями є крайньою ланкою ієрархії: «цифрова економіка –

національна фінансова безпека – фінансова безпека суб'єктів господарювання», що позитивно впливає на фінансову безпеку макрорівня [7, с.59].

Відповідно використання страхування як одного з інструментів управління ризиком має висхідний позитивний вплив на всі суб'єкти, які перебувають на різних ієрархічних рівнях фінансової безпеки. Зі свого боку, страхування кібер-ризиків, наслідки реалізації яких виражені у фінансових втратах, є ефективним заходом покращення рівня кібербезпеки страхувальника, що водночас підвищує і його фінансову безпеку.

Зважаючи на вищезазначене, страхування кібер-ризиків може бути однією зі складових кібербезпеки в умовах сучасної цифрової економіки. Тобто, крім підтримки фінансової безпеки страхувальника (через виплату відшкодування в разі настання страхового випадку), страхування кібер-ризиків спрямоване на підвищення його кібербезпеки (рис. 1.10).

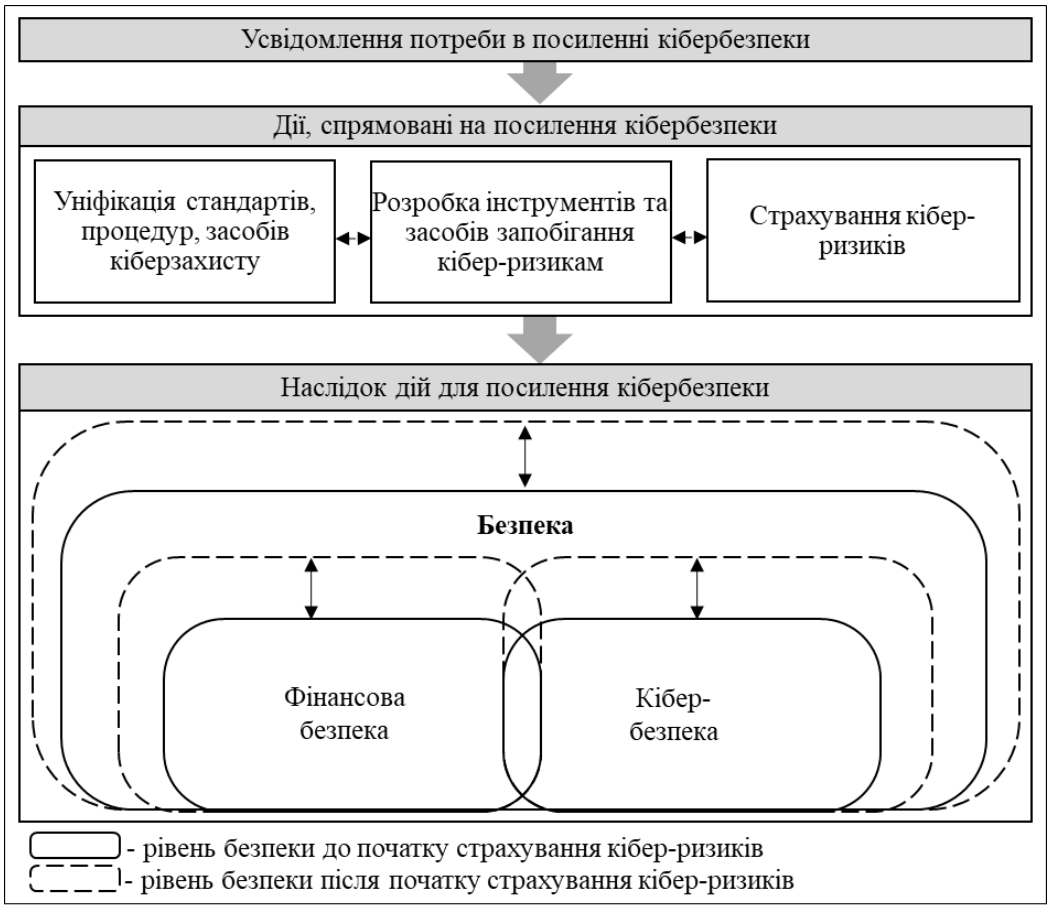


Рисунок 1.10. Місце страхування кібер-ризиків у системі безпеки страхувальника в умовах цифрової економіки

Джерело: складено та доповнено автором на основі [7; 8; 9; 23, с. 169; 37, с. 123; 53, с. 68; 137, с. 215; 146, с.2027; 185, с.98; 191, с. 22; 202; 222, с.141-143]

Таким чином, на основі дослідження теоретичних засад страхування кібер-ризиків ми пропонуємо розширене визначення даного поняття, за яким страхування кібер-ризиків – це правовідносини, що виникають між страхувальником та страховиком у процесі передачі кібер-ризику останньому для захисту його безпеки, включаючи фінансову та кібербезпеку, через асекурацію майнових інтересів страхувальників від наслідків настання страхових подій у кіберпросторі шляхом виплати страхового відшкодування та / або пост-інцидентного супроводу до повного відновлення постраждалих об'єктів.

1.3. Страхові послуги у сфері страхування кібер-ризиків

Страхова послуга є фінальним результатом діяльності страховика, що забезпечує захист страхових інтересів страхувальника. В умовах цифрової економіки актуалізація теоретико-методологічної основи надання послуг страхування кібер-ризиків є запорукою розвитку вказаного виду страхування як одного з інструментів управління кібер-ризиком.

Однак у сучасній науковій думці в контексті страхового захисту від кібер-ризиків вчені часто використовують поняття «послуга» без теоретичного обґрунтування його сутності.

Група вчених визначає послугу зі страхування кібер-ризиків як частину страхового продукту, який створений для захисту страхувальників від кібер-ризиків. Для комерційних користувачів такі послуги також є способом покриття витрат на залагодження проблем із третіми особами [172, с.163-166].

М. Камілло вважає послуги зі страхування кібер-ризиків актуальними фінансовими послугами для юридичних осіб, що зменшують фінансове навантаження на страхувальників. Проте дослідник зауважує, що «поняття послуги страхування кібер-ризиків» змінювалось із нарощенням цифрових технологій та систем. Відповідно, в майбутньому трактування може значно видозмінитись через додатковий вплив інновацій [113, с.54-56].

Водночас Р. Боме та Г. Катарія в рамках дослідження моделей та алгоритмів, що використовуються для визначення страхувальності ризиків, характеризують продукт страхування кібер-ризиків як комплекс заходів, спрямованих на нівелювання ризиків, джерелами яких є технології, системи, інформація, її викрадення, кібервимагання, кібертероризм, злам, фізичне викрадення певних технічних засобів, штрафи, пов'язані з кіберпростором [109, с.5].

Для повноцінного використання поняття «послуга страхування кібер-ризиків» у дослідженні потрібно сформувати власне трактування даного терміну, актуальне для сучасних реалій цифрової економіки.

Поняття «страхової послуги» науковці розглядають у широкому та вузькому значеннях.

У широкому значенні під «страховою послугою» розуміють діяльність, спрямовану на забезпечення страхового захисту страхувальників [82, с. 11].

У вузькому значенні трактування поняття «страхова послуга» є правом на отримання страхувальником захисту при настанні страхового випадку та зобов'язання страховика реалізувати це право [84, с. 517].

Також деякі науковці ототожнюють поняття «страхова послуга» та «страховий продукт», відповідно визначаючи їх як комплекс цивільно-правових відносин щодо захисту майнових інтересів страхувальників у разі настання страхових випадків, зазначених договором страхування [85].

Однак законодавчо поняття розмежовані: відповідно до пункту 1 статті 1 Закону України «Про страхування», «страхова послуга – вид фінансової послуги, що надається страховиком для забезпечення потреби потенційного страхувальника у страховому захисті на підставі договору страхування», в той час як «страховий продукт – умови страхування, які задовольняють визначені потреби та інтереси клієнтів в отриманні страхової послуги» [73].

Відповідно, при страхуванні кібер-ризиків страхувальник отримує страхову послугу, визначену концепцією обраного страхового продукту.

Проте для визначення актуального трактування понять «послуга страхування кібер-ризиків» та «продукт страхування кібер-ризиків» варто додатково дослідити особливості процесу надання послуг страхування кібер-ризиків.

Для отримання послуги страхування кібер-ризиків потенційний страхувальник має укласти страхову угоду зі страховиком. Проте даному етапу ведення страхової угоди передують інші кроки, спрямовані на встановлення контакту між страховиком і страхувальником задля подальшої співпраці.

На основі усталеної процедури укладання страхової угоди варто дослідити етапи реалізації послуги страхування кібер-ризиків (рис. 1.11).

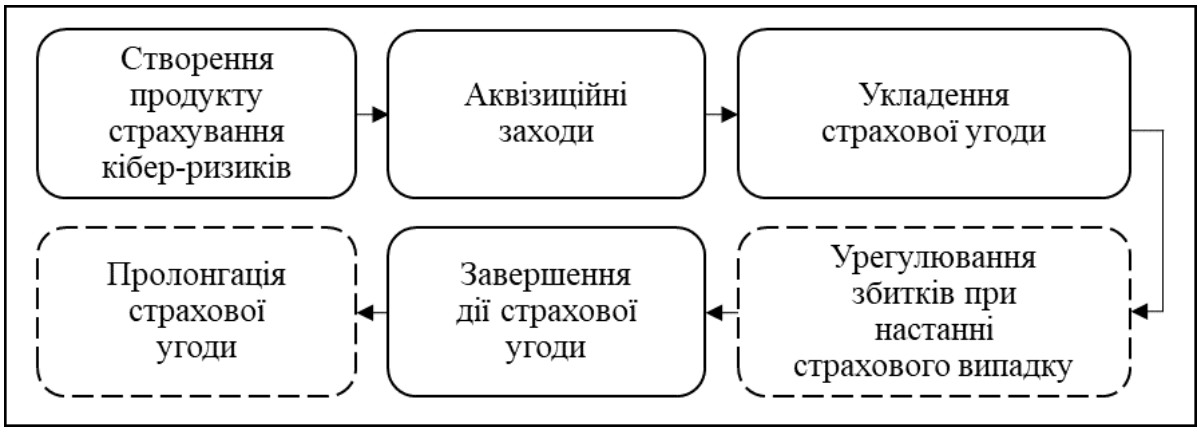


Рисунок 1.11. Етапи реалізації послуги страхування кібер-ризиків

Джерело: складено та доповнено автором на основі [59; 83, с.35-42]

Початковим етапом є осмислення концепції страхової послуги, яку в майбутньому страховик пропонуватиме потенційним страхувальникам, тобто створення страхового продукту. На думку Д. Швігер та К. Ладвіг, страховик має проводити розробку страхового продукту таким порядком:

1. Ідентифікація та кваліфікація сучасних кібер-ризиків, що характерні для регіону, де представлені страховики. Цей крок включає побудову стратегії роботи з кожним окремим ризиком, за необхідності із залученням спеціалістів у сфері кібербезпеки.

2. Виокремлення груп кібер-ризиків, які є страхувальними та нестрахувальними. На цьому етапі обговорюють якісні та кількісні міри для оцінювання доцільності прийняття кібер-ризиків на страхування.

3. Оцінка системного ризику сфери кібербезпеки в цілому та в групах за сферами діяльності потенційного страхувальника. Очевидно, що поділ на сфери є доволі умовним, оскільки технічне оснащення страхувальників може значно відрізнятися через ступінь їх цифровізації. Також даний етап включає аналіз можливого впливу третіх сторін на групи страхувальників, тобто оцінюється ймовірність настання катастрофічного страхового випадку через клієнтів, підрядників, партнерів тощо. Для уникнення відповідних наслідків розроблюють систему стрес-тестів, які сигналізуватимуть про низький рівень системної кібербезпеки.

4. Створення «data-oriented» моделі скринінгу страхувальника. Даний етап є ключовим для страховика з погляду прийняття відповідальності за той обсяг ризиків, який буде йому переданий за підсумками опрацювання моделі. В цей період відбувається активна співпраця з партнерськими організаціями у сфері кібербезпеки задля широкого наповнення аналітичної моделі. Базовими елементами є корпоративна система, система ризик-менеджменту, методи шифрування інформації, модель управління наслідками кіберінцидентів, стандарти та політика співпраці з третіми особами.

5. Навчання страховиків і страхових посередників. Задля ефективного просування послуг персонал в усіх каналах продажу має навчитися розуміти потреби страхувальників та якісно підбирати актуальний для них продукт.

6. Залучення додаткового персоналу з експертизою в сфері кібербезпеки. Задля уникнення випадків недобросовісної співпраці, прискорення верхньорівневого опрацювання питань, пов’язаних зі страхуванням кібер-ризиків, та якісної консультації наявних співробітників страхової компанії, страховик наймає необхідну додаткову кількість фахівців.

7. Створення механізму співпраці з органами влади задля вчасної передачі інформації про критичні кіберінциденти, що мають потенційний вплив на конфіденційність та цілісність даних страхувальників [217, с.58-61].

Проте такий підхід стосується саме методичного аспекту здійснення розробки страхового продукту страхування кібер-ризиків. На нашу думку, варто

доповнити запропонований фреймворк характеристиками етапів фактичної розробки страхового продукту, тобто його наповнення (рис. 1.12).

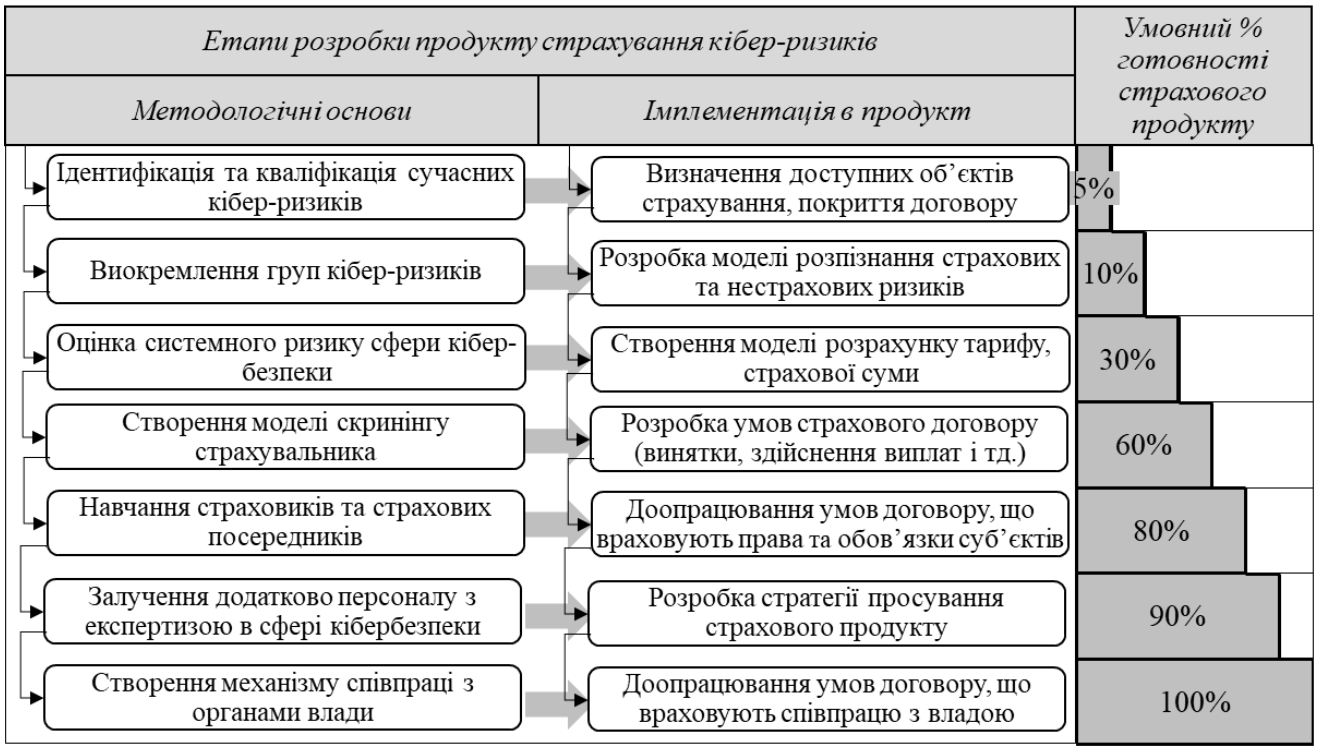


Рисунок 1.12. Фреймворк розробки продукту страхування кібер-ризиків

Джерело: складено та доповнено автором на основі [217, с.58-61; 220, с.52]

Відповідно до запропонованого фреймворку, створення страхового продукту відбувається поетапно на основі визначених методологічних основ та нівелює наявні загрози діяльності страховиків при запровадженні інновацій, такі, як відсутність стратегічних планів розвитку, недовіра до страхових компаній, проблеми з кваліфікованим персоналом [220, с.52].

На першому етапі ідентифікації кібер-ризиків страховик визначає актуальні об'єкти страхування кібер-ризиків, після чого формує перелік доступного покриття майбутнього договору. До цього переліку входять усі кібер-ризики, оскільки для різних страхувальників доцільність страхування одного й того ж ризику може відрізнятися через особливості їхньої діяльності.

На другому етапі формуються пули типових кібер-ризиків для груп подібних страхувальників задля спрощення підготовки індивідуальних пропозицій у майбутньому. Відповідно, маючи різні набори кібер-ризиків, страховик формує індивідуальну пропозицію для страхувальника та за

необхідності доповнює релевантними кібер-ризиками в кожному окремому випадку.

На третьому етапі розраховується базовий рівень ризику, пов'язаний з кібербезпекою, навантажувальні ризики, пов'язані з попередніми специфічними групами ризиків, вагу індивідуального коефіцієнта, що буде застосовуватися на основі даних про страхувальника для корегування страхового тарифу.

На четвертому етапі розробляється проєкт страхової угоди, яка регулює страхування кібер-ризиків. Також збирається інформація попередніх етапів та імплементується у страхову угоду: доступне покриття кібер-ризиків, страхові та нестрахові випадки, винятки, страховий тариф, страхова сума, умови визнання страхового випадку, межі страхових виплат залежно від групи ризиків, період дії страхової угоди.

На п'ятому етапі здійснюється узгодження прав та обов'язків, а також відповідальності за невиконання чи неналежне виконання умов договору сторонами. У разі страхування кібер-ризиків цими сторонами є страховик, експерти у сфері кібербезпеки, потенційний страхувальник, для якого прописують базові права та обов'язки, що можуть бути відкориговані в персональній пропозиції.

На шостому етапі страховик вже має значний обсяг інформації про особливості надання послуги потенційним страхувальникам, а тому починає розробку стратегії просування продукту. В рамках цього етапу страховик тестує та запроваджує комплекс маркетингових заходів: публікація інформації про продукт, робота з цільовою аудиторією, формування впізнаваності бренду та продукту. Для того, щоб цільова аудиторія усвідомила потребу в даному виді страхування, потрібно проводити освітні заходи, що висвітлюють переваги його використання, такі, як зменшення загрози від наявних кібер-ризиків та зменшення витрат на управління ними.

На сьомому етапі створюється механізм співпраці з органами влади, яким презентують продукт та його місце в системі кібербезпеки страхувальників. За необхідності обговорюється можливість надання страховиком інформації про

факти кіберінцидентів органам влади, якщо вони мають потенційний вплив на кібербезпеку інших. На цьому етапі завершується робота над страховим продуктом і типовим договором страхування.

Після того, як продукт страхування кібер-ризиків готовий до продажу, страховики та страхові посередники проводять аквізиційні заходи.

На думку Ю.-А. Квак та Ю.-А. Чо, ініціатором аквізиційних заходів є страховик, навіть у тому разі, коли страхувальник самостійно звертається до страхової компанії. Науковці пов'язують це з наслідком успішної (в деяких випадках агресивної) маркетингової політики страховика. Найбільш оптимальною стратегією продажу є мультиканальна дистрибуція, що передбачає залучення страхових посередників, партнерів та в деяких випадках регулятора (держави) в процес просування страхування кібер-ризиків [184, с. 68].

Інша група вчених вважає онлайн-канали найбільш доцільними для продажу продуктів страхування кібер-ризиків. Також страховикам варто сконцентруватися на співпраці з технологічними компаніями та стартапами. Такий підхід дасть змогу страховим компаніям поглибити експертизу у сфері технологій і кібербезпеки, а відповідним компаніям отримати вигідні умови страхування. Ще однією перевагою співробітництва для стартапів є додаткове тестування власних систем кібербезпеки перед початком дії страхової угоди, оскільки компанії такого типу через швидке зростання та вузьку спеціалізацію часто ігнорують базові правила кібербезпеки [219, с.604].

На нашу думку, попри широке застосування онлайн-каналів продажу, поки що не варто відкидати традиційні канали зі стратегії просування продуктів страхування кібер-ризиків. Відповідно, використання мультиканальної дистрибуції продуктів вказаного виду страхування дасть змогу охопити всю цільову аудиторію.

На аквізиційному етапі відбувається встановлення контакту між потенційним страховиком та страхувальником. При цьому страхувальник може самостійно звернутися до страховика в пошуках необхідної послуги.

Наступним етапом є укладання договору між страховиком і страхувальником, якщо жодна зі сторін не відкидає варіанту співпраці (рис. 1.13).

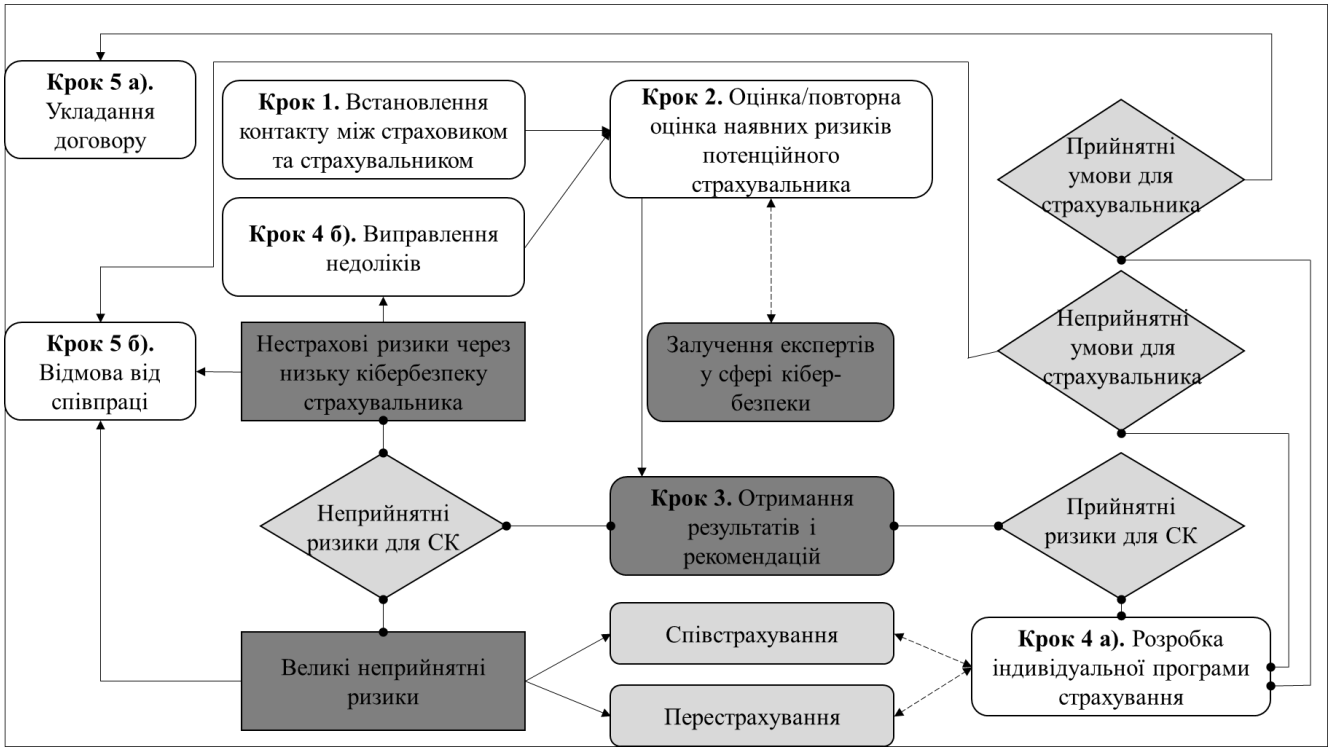


Рисунок 1.13. Алгоритм співпраці страховика та потенційного страхувальника при ухваленні рішення щодо укладання договору страхування кібер-ризиків

Джерело: розробка автора

Запропонований алгоритм визначає п’ять кроків під час ухвалення рішення про укладання договору страхування кібер-ризиків:

1. Крок 1. Встановлення контакту між страховиком та страхувальником. При усвідомленні кібер-ризиків і визначенні страхування як інструмента управління ними страхувальник починає пошук страховиків, які надають такі послуги. Іншим варіантом є звернення страховика з пропозицією страхування кібер-ризиків у рамках аквізиційних процесів. Після обрання страхувальником одного або кількох варіантів страхових компаній починається процес перемов між учасниками страхових відносин. Для цього страхувальник подає заяву на страхування. Додатково до заяви страхувальник може подавати декларацію щодо правдивості наданої ним інформації.

2. Крок 2. Оцінка наявних кібер-ризиків страхувальника. Зі свого боку, страхова компанія починає оцінку поточного стану страхувальника: аналізує її IT-інфраструктуру, обізнаність працівників, захищеність інформації та каналів передачі даних та ін. Окремі страховики здійснюють двоетапну оцінку: поверхневий скринінг без залучення експертів у сфері кібербезпеки та поглиблений скринінг, який проводять спеціалісти у сфері кібербезпеки. При цьому другий етап оцінки відбувається після отримання позитивного результату про доцільність прийняття на страхування кібер-ризиків страхувальника на основі поверхневого скринінгу.

Поверхневий скринінг страхувальника спрямований на встановлення особливостей його діяльності та кібер-ризиків, що характерні для неї. Зазвичай використовують типові групи запитань щодо організації бізнес-процесів, політики конфіденційності та передачі даних, особливостей технічного й мережевого обладнання, загальних характеристик підприємства.

Для ширшого поверхневого скринінгу, що не вимагає додаткового залучення експертів у сфері кібербезпеки, пропонуємо використовувати такі групи даних (Додаток Г) [119; 120]:

- загальна інформація про потенційного страхувальника;
- бажаний вид страхування;
- інформація, яку використовує потенційний страхувальник;
- сервіси передачі інформації, які використовує потенційний страхувальник;
- особливості передачі інформації;
- особливості веб-сайту потенційного страхувальника;
- ризик-менеджмент кіберсфери потенційного страхувальника.

При отриманні прийнятних результатів поверхневої оцінки потенційного страхувальника страховик залучає експертів у сфері кібербезпеки для глибокого аналізу актуальних для нього кібер-ризиків.

3. Крок 3. Отримання результатів і рекомендацій. Експерти у сфері кібербезпеки надають свій висновок про стан страхувальника. Після отримання

результатів перевірки страховик визначає рівень ризику: прийнятний чи неприйнятний для страхування. Також на даному етапі страховик самостійно або із залученням експертів створює дорожню карту виправлення недоліків для підвищення рівня захисту страхувальника.

4. Крок 4. а) У разі, якщо ризики є прийнятними для страховика, то починається розробка індивідуальної страхової угоди на основі потреб страхувальника. б) Якщо ризики є великими, страхова компанія може прийняти об'єкт на страхування з одночасною передачею частини ризику у перестрахування. Рішення про перестрахування страховик ухвалює самостійно та не зобов'язаний повідомляти про це страхувальника. В такому разі починається розробка індивідуальної страхової угоди на основі його потреб. в) Якщо ризики є великими чи надмірними, а тому неприйнятними, страхувальнику пропонують співстрахування таких ризиків. При згоді на такі умови починається робота страхової компанії з партнерами у сфері співстрахування і відбувається розробка індивідуальної страхової угоди. Якщо страхувальник відмовляється від такого варіанту, тоді фіксують відмову від співпраці. г) У разі, якщо ризики є неприйнятними через незадовільний стан кібербезпеки, страхувальнику пропонують виправити недоліки на основі отриманих рекомендацій. При погодженні виправити недоліки страхувальник проходить повторну перевірку (Крок 3).

На думку практиків у сфері кібербезпеки, під час андерайтингу страховикам варто приймати такий рівень кібер-ризиків на страхування, який виключає ймовірність катастрофічних наслідків. Для цього попередньо проводять заходи з уникнення, обмеження та трансферу частини наявних у страхувальників кібер-ризиків, а лише після цього ризики, що залишились, розглядають для прийняття на страхування. Такий підхід визначає оптимальний метод прийняття кібер-ризиків на страхування, як для страховиків, так і для потенційних страхувальників (рис. 1.14) [216].

Якщо страхувальник відмовляється виправляти ідентифіковані недоліки, фіксують відмову від співпраці.

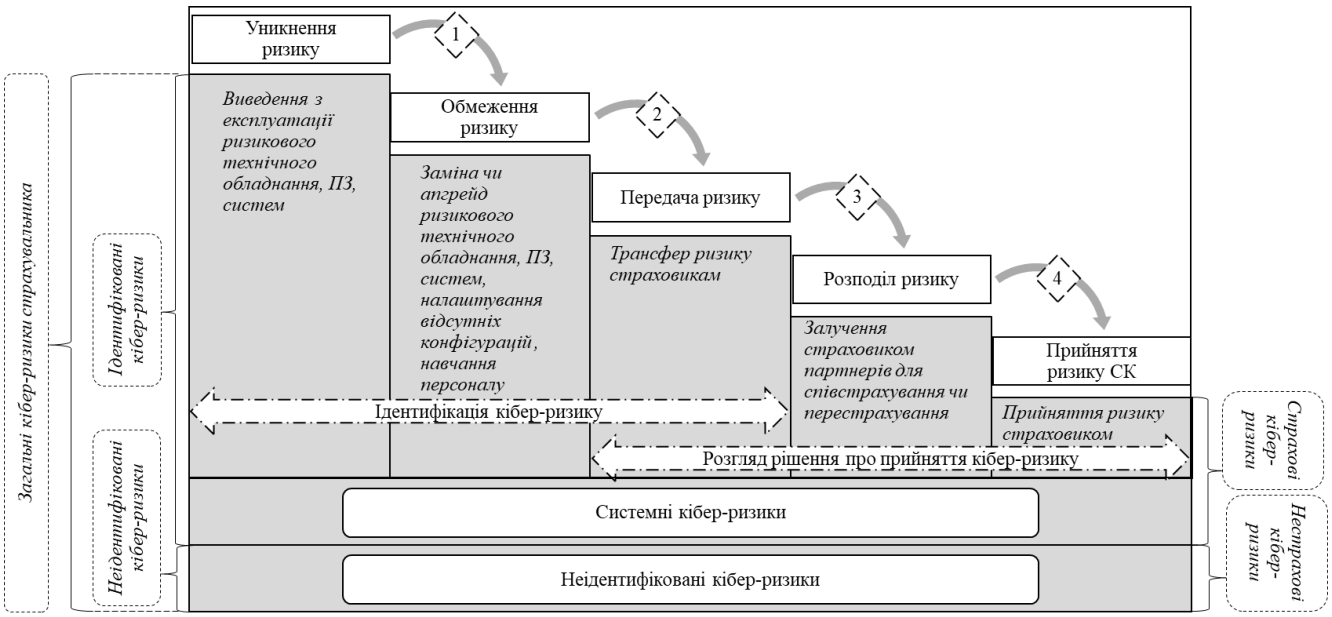


Рисунок 1.14. Оптимальний метод прийняття кібер-ризиків на страхування

Джерело: складено та доповнено автором на основі [216]

5. Крок 5. Після розробки індивідуального страхового полісу з необхідним покриттям і тарифом страхувальник ухвалює рішення щодо того, чи підходить йому запропонований варіант. а) У разі, якщо умови є прийнятними для страхувальника, відбувається укладення договору. б) Якщо умови є неприйнятними для страхувальника, фіксують відмову від співпраці.

Формування персоналізованої пропозиції для страхувальника означає підбір доцільних груп покриття кібер-ризиків, розрахунок страхового тарифу, окреслення винятків, визначення терміну дії угоди, умов припинення угоди, порядку дій при настанні страхового випадку, умов отримання страхової виплати, умов врегулювання спорів, опис прав та обов'язків сторін тощо.

Для визначення актуальних кібер-ризиків страхувальника страховик разом з експертами у сфері кібербезпеки проводить андерайтинг. Як було зазначено у пункті 1.1., науковці виділяють види кіберстрахування залежно від релевантного для потенційного страхувальника кібер-ризику. Відповідно, віднайдення страховиком у процесі андерайтингу актуального кібер-ризику є основою формування страхового покриття в індивідуальному страховому полісі.

На думку У. Франке, оцінка кібер-ризиків дає змогу сформувати основний продукт страхування, що покриває базовий ризик, характерний для сфери

діяльності страхувальника, та додатковий продукт, що покриває специфічні ризики за додаткову плату. До додаткових груп можуть належати: покриття людських помилок, технічних помилок, нормативні вимоги (переривання діяльності через проведення розслідування), покриття репутаційних втрат [156, с.134].

К. М. Рангу, Н. Пана та К. М. Счеу додатково виокремлюють покриття ризиків кібератак, спрямованих на критичну інфраструктуру страхувальника. Прикладом цього є перешкоджання роботі електрогенераторів, серверів та інших технологічних пристроїв [211, с.390-397].

Окремо Б. Гупта та А. Дахія виділяють покриття DDoS-атак, оскільки ризики такого типу відрізняються цільовим характером впливу на страхувальника з метою створення умов недоступності його серверів, веб-сайтів та інших онлайн-сервісів [166].

Деталізовану класифікацію груп кібер-ризиків, що можуть входити до страхового покриття, запропонували Д. Д. Кебула, М. Е. Попек та Л. Р. Янг. Науковці виділили чотири групи кібер-ризиків: дії людей (навмисні, ненавмисні, навички людей), системні й технологічні помилки (пов'язані з обладнанням, програмним забезпеченням, системами), проблеми у внутрішніх процесах (некоректне планування чи застосування, процедурні контролі, допоміжні процеси), зовнішні події (катастрофічні події, нормативні обмеження, обмеження бізнесу, сервісні проблеми) [114, с.3–8].

Однак, на нашу думку, запропоновані класифікації є неповними, оскільки не враховують нових викликів сучасного цифрового світу. Одним із таких ризиків є кібервійна, що означає зловмисний вплив через комп'ютерні засоби і мережі однієї держави або її хакерських угруповань на комп'ютерні засоби і мережі іншої держави [218]. Оскільки жертвами кібервійни можуть бути не лише державні чи військові організації, тому потенційний страхувальник може потрапити в групу даного ризику. В умовах автоматизації виробництва поширюється використання роботів і роботизованої техніки. Відповідно втрата контролю над ними може

призвести або до повної зупинки бізнесу, або до значних збитків через їхню некоректну роботу.

Також варто розглядати вплив дронів або ж безпілотних літальних апаратів на діяльність страхувальника. Дану технологію страхувальник може використовувати для моніторингу і контролю своєї діяльності, тестування готової продукції (наприклад, для віддаленого фіксування результатів випробувань, перевірки логічних ліній), логістики, тому втрата контролю чи зв'язку з ними призведе до порушення бізнес-процесів. З іншого боку, дрони можуть використовувати зловмисники для спостерігання, проникнення чи шпіонажу за страхувальником.

Ще одним ризиком є застосування штучного інтелекту, оскільки точно спрогнозувати результати такої імплементації неможливо навіть в умовах обмеженого середовища. Проте більшість компаній використовують ліцензовані платформи штучного інтелекту, тому ризики на даному етапі є мінімальними. Однак при застосуванні цієї технології під час спілкування з третіми особами (чат-боти, автоматичні відповіді на листи, кол-центри, тощо), варто враховувати ймовірність неточної чи некоректної відповіді, що призведе до репутаційних втрат.

Враховуючи запропоновані доповнення, актуалізована класифікація груп кібер-ризиків для формування оптимального страхового покриття представлена у Таблиці 1.4. Відповідно до такого підходу, класифікація включає наступні ознаки кібер-ризиків, згруповані за джерелом виникнення та формою прояву під час діяльності страхувальника:

- дії людей;
- системні та технологічні помилки;
- проблеми у внутрішніх процесах;
- зовнішні події.

Систематизовані групи кібер-ризиків є базою для обчислення можливого страхового покриття, що буде розраховуватись на основі завданих страхувальнику збитків за реалізованими кібер-ризиками.

Таблиця 1.4

Класифікація груп кібер-ризиків для формування страхового покриття

Дії людей	Системні та технологічні помилки	Проблеми у внутрішніх процесах	Зовнішні події
Внутрішні -помилки -упущення Зовнішні -саботаж -шахрайство -шантажування (кібер-вимагання) -соціальна інженерія -фішинг -крадіжка -вандалізм -кібератаки (DDoS-атаки) Навички людей -вміння -навички -доступність -управління -залучення AI	Обладнання -ємність -продуктивність -технічне обслуговування -зношення -використання роботів -використання IoT -використання дронів ПЗ -сумісність -конфігурація -контроль змін -індикатори безпеки -особливості кодування -тестування -блокчейн Системи -специфікація -дизайн -комплексність -інтеграційність	Некоректне планування чи застосування -хід процесу -документація -ролі та обов'язки -оповіщення -потоки інформації -ескалація питань Процедурний контроль -моніторинг -ключові метрики -періодичний огляд -стейкхолдери процесу Допоміжні процеси -прийом працівників -фінансування -навчання і розвиток -закупівлі	Катастрофічні події -природні -пожежа -пандемія -кібервійна -нестабільність Нормативні обмеження -відповідність нормативним вимогам -оновлення законів -судовий процес Обмеження бізнесу -невиконання третіми особами зобов’язань -стан ринку -економічна ситуація -втрата репутації Сервісні проблеми -логістичні -енергетичні

Джерело: складено автором на основі [114, с.3-8; 156, с.134; 166; 211, с.390-397; 218; 233, с.665-668]

Після проведення андерайтингу потенційного страхувальника та прийняття рішення про доцільність страхування окреслених ризиків страховики здійснюють актуарні розрахунки для обчислення страхового тарифу.

Загальна формула страхового тарифу ризикового страхування (брутто-ставка) складається з нетто-ставки та страхового тарифу [2]:

$$T_B = \frac{T_N}{1-N}, \quad (1.1)$$

де T_B – страховий тариф, або брутто-ставка;

T_N – нетто-ставка;

N – навантаження до нетто-ставки, що покриває витрати страхової компанії на організацію та ведення страхової справи.

Нетто-ставка складається з базового тарифу (середня збитковість) та ризикової надбавки [2]:

$$T_{\text{Н}} = T_0 + R, \quad (1.2)$$

де T_0 – базовий тариф або середня збитковість;

R – ризикова надбавка.

Розрахунок нетто-ставки ускладнюється особливістю страхування кібер-ризиків – відсутністю історичних даних щодо кількості кіберінцидентів та втрат від них. Відповідно для формування нетто-тарифу страхування кібер-ризиків актуально використовувати методологію для нових видів страхування [2]:

$$T_{\text{Н}} = r * K_P * K_V * 100 = \frac{r_I}{r_A} * \frac{\overline{IP}}{\overline{IS}} * (\frac{1-K_0*(1-K_R)}{K_R}), \quad (1.3)$$

де r – можлива ймовірність настання страхового випадку;

K_P – поправний коефіцієнт;

K_V –коефіцієнт вибірковості;

r_I – можлива кількість страхових випадків;

r_A – можлива кількість об'єктів страхування;

$\overline{IP}$ – середня можлива страхова виплата;

$\overline{IS}$ – середня можлива страхова сума;

K_0– коефіцієнт відставання відносної зміни страхових виплат порівняно з рівнем розвитку страхового ринку;

K_R – коефіцієнт потенційного розвитку страхового ринку.

Оскільки розрахунок нетто-тарифу для нових видів страхування враховує багато умовностей, науковці досліджують можливі втрати для кожного окремого ризику, тоді як ймовірність настання страхового випадку визначають експерти у сфері кібербезпеки на основі проведеного поглибленого скринінгу.

Досліджуючи тему страхування ризиків, пов'язаних із програмним забезпеченням, а також інформацією та її цілісністю, Л. Павлік, М. Фіцек та Д. Рак розраховують потенційні втрати від кіберінцидентів на основі даних страхувальника. Відповідно, для коректного й точного розрахунку взаємодія між страховиком і страхувальником має основуватись на принципі прозорості [205].

Для розрахунку втрат від перерви у виробництві науковці пропонують використовувати порівняння даних за перерву та період стабільності [205]:

$$L_P = \sum_{i=1}^{n} CV_h * \sum_{i=1}^{n} H_h, \quad (1.4)$$

де L_P – можливі втрати від перерви у виробництві;

CV_h – ціна продукції, що виробляється страхувальником за годину;

H_h – кількість годин перерви.

Ще однією групою втрат є витрати на реконструювання та відновлення інформації [205]:

$$L_D = C_d * \sum_{i=1}^{n} P_d, \tag{1.5}$$

де L_D – можливі збитки від втрати, викрадення чи пошкодження даних;

C_d – вартість втрачених, викрадених чи пошкоджених даних на одну особу;

P_d – кількість втрачених, викрадених чи пошкоджених даних.

Для визначення наслідків витоку інформації пропонується розраховувати витрати, спрямовані на залагодження кризових ситуацій [205]:

$$L_C = \sum_{i=1}^{n}(Q_C * S_C * H_C), \tag{1.6}$$

де L_C – можливі втрати від витоку даних чи порушення конфіденційності;

Q_C – кількість осіб, що постраждали від інциденту;

S_C – заробітна плата працівників, які здійснюють залагодження ситуації, за годину;

H_C – кількість годин, витрачених на залагодження ситуації.

Додатково науковці досліджують наслідки впливу кіберінциденту на репутацію страхувальника [205]:

$$L_R = \left(\overline{AI}_C * \frac{\sum_{i=1}^{n} N_{ki}}{n} - \overline{AI}_C * \frac{\sum_{i=1}^{n} Z_{ki}}{n}\right) - \frac{\sum_{i=1}^{n} N_{ir}}{n}, \tag{1.7}$$

де L_C – можливі втрати, що покривають витрати на відновлення репутації;

$\overline{AI}_C$ – середній дохід від клієнтів;

N_{ki} – кількість нових клієнтів за рік;

Z_{ki} – кількість втрачених клієнтів за рік;

N_{ir} – маркетингові витрати за рік (спрямовані на відновлення репутації);

n – кількість спостережень.

Досліджуючи кібер-ризики, що пошкоджують технології чи обладнання, науковці розраховують втрати, опираючись на його вартість [205]. Для першого року використання технології чи обладнання:

$$L_{o_0} = \frac{PC}{K_0}, \quad (1.8)$$

де L_{o_0} – можливі втрати через пошкодження технології чи обладнання, що використовується перший рік;

PC – вартість купівлі пошкодженого активу;

K_0 – податковий коефіцієнт першого року використання, що відрізняється в різних країнах, залежно від законодавства.

Для другого і наступних років використання технології чи обладнання:

$$L_{o_1} = \frac{(2*ZC)}{(K_1 - n)}, \quad (1.9)$$

де L_{o_1} – можливі втрати через пошкодження технології чи обладнання, що використовується другий чи наступні роки;

ZC – балансова вартість пошкодженого активу;

K_1 – податковий коефіцієнт другого і наступних років використання, що відрізняється в різних країнах, залежно від законодавства;

n – рік амортизації пошкодженого активу.

Однак, незважаючи на значну активізацію зловмисників, що використовують DDoS-атаки як засоби переривання чи блокування діяльності, єдиного підходу до оцінки втрат від них не існує. Відповідно пропонуємо розраховувати можливі втрати на основі оцінки діяльності страхувальника в стабільний період:

$$L_{DDoS} = \sum_{i=1}^{n} CV_h * \sum_{i=1}^{n} H_h + S_C * T_C, \quad (1.10)$$

де L_{DDoS} – можливі втрати від DDoS-атаки;

CV_h – ціна продукції, яку виробляє / продає страхувальник через атаковані канали за годину;

H_h – кількість годин перерви;

S_C – заробітна плата працівників або найманих спеціалістів, що працюють над відновленням сервісів, за годину;

T_C – кількість годин, витрачених на відновлення пошкоджених сервісів (включаючи веб-сайти та сервери).

Розраховані суми збитків страховик збирає від пулу наявних страхувальників, а також від потенційних. Формування власної бази даних та особливостей страхових випадків дає змогу щоразу підвищувати точність розрахунку страхового тарифу. Відповідно використання розрахованих можливих втрат стає основою для формування страхового тарифу під час процесу створення персоналізованої страхової угоди.

Ще одним важливим компонентом майбутньої страхової угоди є винятки. Дослідники вважають, що винятками зі страхової угоди щодо страхування кібер-ризиків можуть бути: втрати через електричні або телекомунікаційні проблеми; збої через використання неповних потужностей обладнання страхувальника; втрата даних, системних конфігурацій, технологій чи програмного забезпечення через відсутність резервних копій; низький рівень безпеки через невиконання взятих обов'язків на покращення рівня захищеності від кіберзагроз; шахрайство з боку страхувальника [190].

Асоціація страховиків Британії окреслює такі типові винятки при страхуванні кібер-ризиків: витрати через збої в критичній інфраструктурі, пов'язані з нестабільністю подачі електроенергії, газу, води, перебої у телекомунікаціях чи супутниковому зв'язку; кібервійна; штрафи та санкції за невідповідність діяльності страхувальника законодавчим нормам і стандартам; позови, подані пов'язаними особами, тобто персоналом, підрядниками чи дочірніми організаціями; тілесні ушкодження чи ушкодження майна, оскільки зазвичай втрати такого типу покривають інші види страхування [115].

Оскільки процес ухвалення страховиком рішення щодо страхування кібер-ризиків для нових страхувальників має доволі високу вартість та займає багато часу на деталізовану оцінку кібер-ризиків, в рамках аквізиційних заходів вказані послуги пропонують уже наявним клієнтам. Такий підхід дає змогу скоротити термін прийняття на страхування, оскільки страховик вже має основну інформацію про страхувальника. З огляду на це страховики пропонують два варіанти покриття ризиків: комплексний, що покриває кібер-ризики та ризики інших сфер в одному страховому продукті; самостійний страховий продукт, що

покриває лише кібер-ризики [152]. Покриття кібер-ризиків теж може бути комплексним, тобто включати страхування відповідальності та майнове страхування у цифровій сфері, або частковим, тобто страхування відповідальності або майнове страхування у цифровій сфері (рис. 1.15).

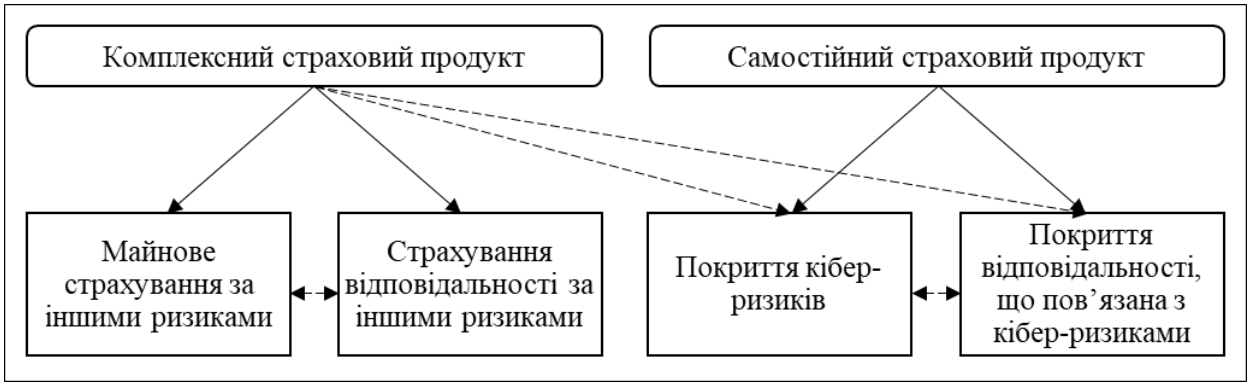


Рисунок 1.15. Типи страхового продукту, що покриває страхування кібер-ризиків

Джерело: складено та доповнено автором на основі [152]

У рамках укладення страхової угоди після визначення типу страхового продукту, його покриття, винятків і страхового тарифу, страховик та страхувальник узгоджують термін дії угоди й умови її припинення.

Страхувальник може обрати короткострокову угоду – термін дії до одного року, або середньострокову – від одного до двох років з періодичним переглядом умов договору. Необхідність перегляду пов'язана з особливостями цифрової трансформації страхувальника, оскільки запровадження нових технологій у процес діяльності може істотно змінити обсяг актуальних для нього кібер-ризиків. У страховій угоді додатково описують умови дострокового припинення її дії, однак про свої наміри будь-яка зі сторін має завчасно повідомити іншу.

Ще одним обов'язковим компонентом страхової угоди є визначення порядку дій при настанні страхового випадку та порядку отримання страхового відшкодування.

При страхуванні кібер-ризиків страхувальник зобов'язаний звернутися із заявою до страховика про настання страхового випадку та отримати він нього інструкції щодо наступних кроків. Подальші рекомендації можуть включати залучення експертів у сфері кібербезпеки задля усунення наслідків

кіберінциденту та оцінки понесених втрат. Хоча в загальному майновому страхуванні необхідно зберігати об'єкт страхування в незмінному вигляді до проведення аналізу страховиком чи його представником, у страхуванні кібер-ризиків часто невтручання в роботу системи чи технології може спровокувати ще більший обсяг втрат. Відповідно страхувальник має локалізувати чи обмежити загрозу самостійно (якщо наявні компетентні фахівці) або залучити експертів у сфері кібербезпеки для припинення негативного впливу від кіберінциденту, що триває. Таким чином, узагальнений порядок дій страхувальника для отримання відшкодування при настанні страхового випадку визначається:

1. Сповіщенням страховика про настання страхового випадку у найбільш швидкий спосіб. Звернення може бути як у письмовій, так і в усній формі.

2. Збереженням максимально можливої недоторканності доказів кіберінциденту. Зрозуміло, що в разі критичної необхідності спеціалістів у сфері кібербезпеки (персонал страхувальника або запрошені фахівці від страхової компанії) можуть залучати для припинення негативних наслідків. Однак збереження доказів дасть змогу страховикам оцінити причини настання страхового випадку, а тому й ухвалити рішення про можливість надання відшкодування.

3. Поданням заяви на страхове відшкодування. В заяві страхувальник вказує свої дані, обставини настання страхового випадку, інші необхідні додаткові деталі.

4. Наданням необхідної документації для визначення обставин страхового випадку та його наслідків. Для того, щоб об'єктивно оцінити завдані страхувальнику збитки, страховик має отримати супровідні документи, в яких міститься інформація про балансову та реальну вартість постраждалого об'єкта, специфікацію, конфігурацію системи на дату настання страхового випадку, завдані втрати, обґрунтовані фактичними або приблизними розрахунками, звіти комісій чи слідчих органів, висновки від експертів у сфері кібербезпеки та інші можливі звіти за їх наявності.

5. Співпрацею між страхувальником та експертними організаціями. Страхові компанії можуть залучати профільних фахівців не тільки для оцінки збитків, а й для відновлення роботи постраждалих об’єктів.

6. Виконанням страхувальником інших зобов’язань, що вказані в умовах страхової угоди (вчасне подання документів, повнота та коректність інформації, допуск представників страховика та інших спеціалістів, яких залучає страховик, безпосередньо до місця / системи, де трапився кіберінцидент).

7. Отриманням страхового відшкодування у вигляді компенсації завданих страхувальнику збитків або комплексного відновлення страховиком об’єктів, що постраждали внаслідок кіберінциденту.

Оскільки наслідок реалізації кібер-ризику не завжди може бути виявлений одразу, то науковці пропонують трьохкомпонентний підхід до визнання страхового випадку:

- кіберінцидент був виявлений протягом дії страхового полісу;
- страхувальник вчасно повідомив страховика про настання кіберінциденту (залежно від різних груп кібер-ризиків час повідомлення може відрізнятися, період встановлює кожний страховик самостійно);
- деталізована сума потенційних збитків економічно обґрунтована та усуває можливість спекуляцій з боку страхувальника [117].

Визначення прав та обов’язків сторін при страхуванні кібер-ризиків здійснюється на основі політики страхової компанії та нормативного регулювання регіону, де перебувають сторони.

Після узгодження всіх особливостей персоналізованої індивідуальної пропозиції сторони укладають страхову угоду, що може бути представлена у формі договору, полісу, сертифікату тощо.

Наступним етапом після укладення страхової угоди є надання страховиком самої послуги зі страхування кібер-ризиків протягом визначеного терміну за обраним страховим продуктом.

У разі, якщо протягом визначеного періоду дії страхової угоди страховиком було визнано страховий випадок, страхувальнику має бути надано страхове відшкодування, що може покривати різні групи втрат від вищезазначених ризиків.

Якщо протягом визначеного періоду дії страхової угоди страховий випадок не відбувся, то термін дії угоди завершується, тому страхувальник після цього не зможе звернутися до страховика у разі настання кіберінциденту.

Оскільки страховики зацікавлені в збереженні страхувальника як свого клієнта, страхові компанії можуть запропоновувати вигідні умови для пролонгації страхової угоди. Відповідно, вартість страхування в такому разі є нижчою для страхувальника, оскільки страховик вже володіє інформацією про стан, особливості діяльності, кібер-ризики та потенційні загрози свого клієнта.

У разі, якщо страхувальника не влаштовують поточні умови страхування і він бажає змінити страховика, страховик може на комерційній основі передати верифіковану інформацію про страхувальника новому страховику для більш точної оцінки кібер-ризиків та розрахунку тарифу страхування.

Врахування віднайдених особливостей страхування кібер-ризиків та проаналізованих підходів до визначення поняття «страхова послуга» дає змогу розширити трактування дефініції «послуга страхування кібер-ризиків» та визначити вказане поняття як комплекс дій страховика, які він зобов’язаний виконати і які спрямовані на страховий захист страхувальника від ризиків, що впливають на його кібербезпеку, на підставі договору страхування.

Проаналізувавши процес надання страхових послуг у сфері страхування кібер-ризиків та місце страхового продукту в ньому, доцільно використовувати трактування поняття «продукт страхування кібер-ризиків» як визначені страховиком порядок та умови страхування кібер-ризиків, яких мають дотримуватися всі учасники страхових відносин для забезпечення визначеного рівня кібербезпеки страхувальника.

ВИСНОВКИ ДО РОЗДІЛУ 1

На основі аналізу теоретичних основ страхування кібер-ризиків в умовах цифрової економіки було зроблено такі висновки:

1. Обґрунтовано, що поняття «кібер-ризик» виникло під впливом цифровізації економіки, оскільки форма прояву вказаних ризиків міститься в кіберпросторі. Відповідно до віднайдених особливостей, запропоновано власне визначення поняття «кібер-ризик» – це ймовірність настання події або групи подій внаслідок зловмисного втручання до ІТ-систем, бізнес-процесів, технологій, програмного забезпечення, каналів передачі даних, що призводить до отримання фінансових та / або репутаційних збитків через порушення стабільності, вимушену зупинку діяльності, конфіденційності та / або цілісності інформації фізичних і юридичних осіб.

2. Визначено класифікацію кібер-ризиків за рівнями економіки, на яких вони реалізовуються: макроекономічні, мезоекономічні та мікроекономічні кібер-ризики. Розроблено класифікацію кібер-ризиків за секторальною ознакою, включаючи ризики: фінансового сектору, енергетичного сектору, екологічного сектору, сектору охорони здоров’я, сектору виробництва, сектору державного управління, оборонного сектору. Окрім того, деталізовано кібер-ризики оборонного сектору на основі сучасних реалій гібридної війни, а саме: кібершпигунство, кібератаки на канали військової комунікації чи несанкціоноване підключення до них, кібератаки на військову інфраструктуру, кібератаки на цифрові військові системи, кібератаки на зброю, цифрова пропаганда.

3. З’ясовано, що використання страхування кібер-ризиків як одного з інструментів управління ризиком позитивно впливає на розвиток кібербезпеки страхувальника, що також підвищує рівень фінансової безпеки суб’єкта завдяки комплексному характеру заходів страховика, які включають оптимізацію діяльності страхувальника в кіберпросторі, встановлення моніторингових систем діяльності та продуктивності, розвиток цифрової грамотності страхувальника

та / або його персоналу, зниження адміністративних витрат на підтримку кібербезпеки, зменшення кіберінцидентів.

4. Запропоновано наступне визначення поняття «страхування кібер-ризиків» – це правовідносини, що виникають між страхувальником та страховиком у процесі передачі кібер-ризику останньому для захисту безпеки страхувальника, включаючи фінансову та кібербезпеку, через асекурацію майнових інтересів страхувальника від наслідків настання страхових подій у кіберпросторі шляхом виплати страхового відшкодування та / або пост-інцидентного супроводу до повного відновлення постраждалих об’єктів.

5. Виявлено та описано особливості етапів реалізації послуги страхування кібер-ризиків: створення продукту страхування кібер-ризиків, проведення аквізиційних заходів, укладення страхової угоди, врегулювання збитків при настанні страхового випадку, завершення дії страхової угоди, пролонгація страхової угоди. Відзначено особливість розробки продукту страхування кібер-ризиків, що полягає у відсутності історичних даних, необхідних для актуарних розрахунків, тому систематизовано наявні підходи для обчислення компонентів страхового тарифу та запропоновано власну формулу потенційних втрат від DDoS-атаки.

6. Ґрунтуючись на віднайдених особливостях страхування кібер-ризиків, розмежовано та визначено поняття: «послуга страхування кібер-ризиків» – комплекс дій страховика, спрямованих на страховий захист страхувальника від ризиків, що впливають на його кібербезпеку, які він зобов’язаний виконати на підставі договору страхування; «продукт страхування кібер-ризиків» – визначені страховиком порядок та умови страхування кібер-ризиків, яких мають дотримуватися всі учасники страхових відносин для забезпечення визначеного рівня кібербезпеки страхувальника.

РОЗДІЛ 2. ТЕНДЕНЦІЇ ТА ОСОБЛИВОСТІ РОЗВИТКУ СТРАХУВАННЯ КІБЕР-РИЗИКІВ В ЦИФРОВУ ЕПОХУ

2.1. Періодизація становлення глобального ринку страхування кібер-ризиків

Сьогодні світ перебуває в умовах глобальної цифровізації, що означає швидкий розвиток та залучення новітніх технологій у всі сфери діяльності. Проте водночас розвиваються кіберзагрози, що все частіше стають причинами нестабільності в локальному та глобальному вимірах. Відстежування періодів становлення ринку страхування кібер-ризиків є необхідним кроком оцінки його потенційних можливостей для нейтралізації сучасних кібер-ризиків.

На думку спеціалістів у сфері ризик-менеджменту, процес становлення ринку страхування кібер-ризиків розпочався в період 1990-х років і триває досі. Перший етап стартував у 1990-х роках, коли страхування кібер-ризиків було додатком до основного полісу майнового страхування. Другий етап охоплює період із 2005 р. по 2010 р., коли страховики почали запроваджувати покриття відповідальності, наприклад, негативний вплив на діяльність третьої особи в системах чи програмах. Третій етап тривав із 2010 р. по 2016 р., коли кібератаки на бізнес стали регулярними, провокуючи тривалі простої виробництва. Саме в цей час страхування кібер-ризиків повністю оформилось в окремий вид страхування. Четвертий етап зайняв період з 2016 р. по 2018 р., коли викрадення даних і злами систем ставали все частішими і завдавали більше втрат для компаній, що їх використовували. В цей час необхідність страхування кібер-ризиків стала очевидною та сприяла його активному розвитку. П’ятий етап почав свій відлік із дати початку застосування General Data Protection Regulation (GDPR) у 2018 р., в якому були описані умови зберігання, передачі та обробки персональних даних, що значно посилило рівень захищеності інформації. Шостий етап стартував 2020 року і триває досі, оскільки глобальна пандемія COVID-19 змінила звичний режим ведення бізнесу на дистанційний формат, а тому

використання інформаційних технологій стало більш ризикованим через низький рівень контролю [100].

Учені вважають період із 1996 р. по 2000 р. першим етапом розвитку та популяризації страхування кібер-ризиків, оскільки перші поліси, що покривали кібер-ризики, пов'язані з хакерством, були продані саме в цей час. Наступний етап охопив період розвитку законодавства, що регулює обіг електронних даних та їх конфіденційність, тобто 2000–2005 роки. Останній етап після 2005 року відзначався трансформацією страхових продуктів під впливом нових викликів, відповідно страхування кібер-ризиків стало самостійним видом страхування [190, с.4-6].

Для визначення особливостей розвитку страхування кібер-ризиків та виокремлення відповідних характерних періодів варто розглянути основні детермінанти глобальної цифровізації.

Одним із ключових показників цифровізації, що відображає масштабність та глобальність цього процесу, є наявність постійного доступу до мережі «Інтернет» (рис. 2.1). Онлайн-з'єднання між організаціями, установами та людьми дає їм змогу не лише взаємодіяти між собою, а й отримувати необхідну інформацію та створювати додаткові нові блага. За даними The International Telecommunication Union (ITU), збір даних про доступність мережі «Інтернет», види зв'язку та покриття проводиться з 2005 р. на щорічній основі [181].

Станом на 2005 р. кількість користувачів мережі «Інтернет» становила 1022 млн осіб (покриваючи 15,6% світового населення). Протягом наступних п'яти років відбулось активне поширення мережевих технологій, що спровокувало ріст проникнення мережі «Інтернет» до 28,5% (+12,9 в.п. порівняно з 2005 р.), відповідно в даний період приріст користувачів мережі «Інтернет» мав найвищий темп +95%. Додатковим стимулом росту стало створення доступних та зрозумілих для користувачів браузерів, а також програм: для спілкування в режимі онлайн (Skype, WhatsApp, Viber), соціальних мереж (Instagram, Facebook, Twitter або X), сервіси для блогів та мікроблогів (Reddit, Tumblr), стрімінгові платформи і відео- та музичні сервіси (YouTube, Spotify, SoundCloud).

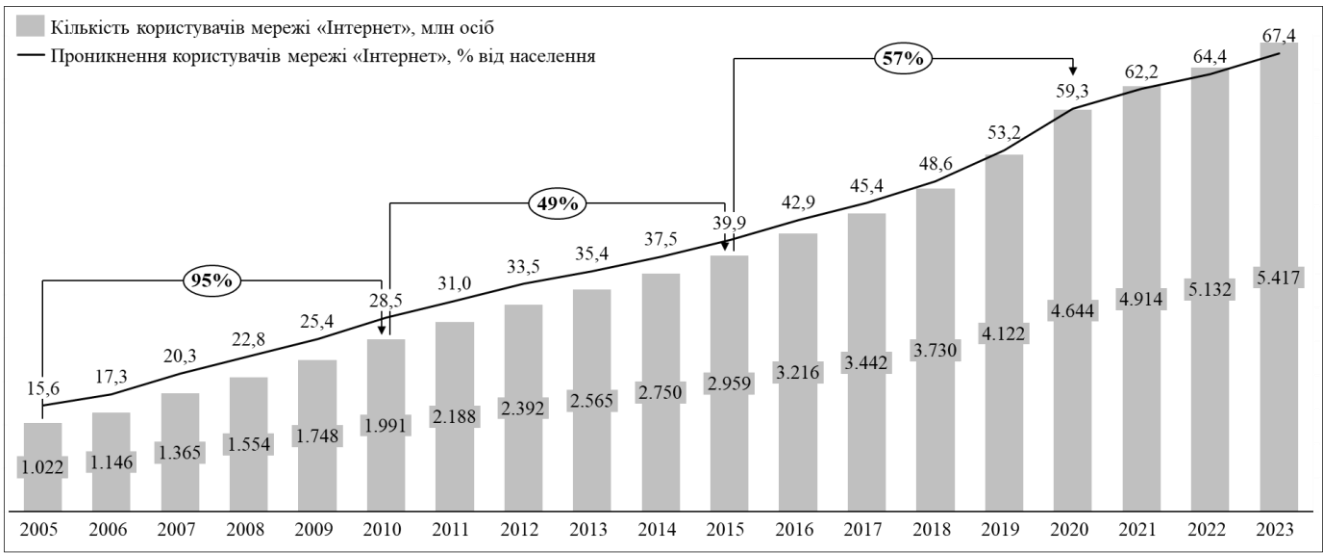


Рисунок 2.1. Динаміка росту користувачів мережі «Інтернет» у 2005–2023 рр., млн осіб, % від населення

Джерело: складено автором на основі [181]

Період 2011–2015 рр. демонстрував нижчий темп приросту користувачів мережі «Інтернет» (+49%), ніж у попередній період, однак це пояснюється обмеженою на той час доступністю девайсів, які підтримують з'єднання з мережею «Інтернет» у країнах з низьким рівнем економічного розвитку. Проникнення мережі «Інтернет» зросло до 39,9% (+11,4 в.п. порівняно з 2010 р.) та в абсолютному вимірі становило 2959 млн осіб.

Наступний період з 2016 р. по 2020 р. продемонстрував швидший темп приросту (+57%), що пояснюється активною сматрфонізацією населення, збільшенням доступності мережевого обладнання і покриття та розширенням можливостей соціальних мереж і стрімінгових платформ (створення TikTok, геймінгових сервісів). Однак найбільший вплив на зростання числа користувачів мережі «Інтернет» в даний період мала пандемія COVID-19, внаслідок якої більшість бізнесів перейшли в режим онлайн, відповідно населення було змушене підключати інтернет до власного домогосподарства. Тому станом на 2020 рік кількість користувачів мережі «Інтернет» становила 4644 млн осіб, а рівень проникнення зріс до 59,3% (+19,4 в.п. порівняно з 2015 р.).

У період 2021–2023 рр. зростання даного показника сповільнилось через наближення проникнення користувачів мережі «Інтернет» до граничного

значення. Частина населення, що залишається без мережі «Інтернет», не може дозволити підключення через високу вартість обладнання, або ж через недоступність покриття мережею в певному регіоні. Таким чином, станом на 2023 р. кількість користувачів мережі «Інтернет» становила 5417 млн осіб, демонструючи рівень проникнення 67,4% (+8,1 в.п. порівняно з 2020 р.).

Окрім використання мережі «Інтернет», ще одним показником цифровізації є перехід користувачів із фіксованого телефонного з'єднання на мобільне, оскільки сьогодні для здійснення багатьох операцій (фінансових, побутових, адміністративних) необхідна лише реалізація мобільного виклику (рис. 2.2).

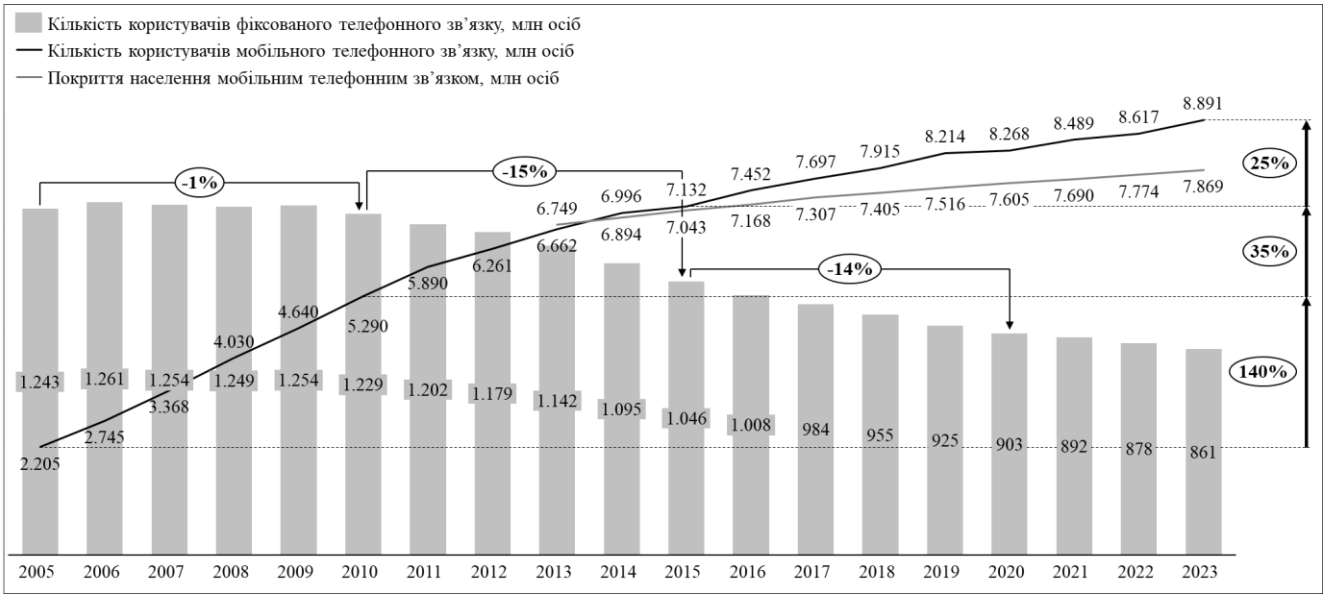


Рисунок 2.2. Динаміка переходу користувачів із фіксованого телефонного зв'язку на мобільний телефонний зв'язок та покриття населення мобільним телефонним зв'язком у 2005–2023 рр., млн осіб

Джерело: складено автором на основі [181]

Аналогічно до темпів приросту користувачів мережі «Інтернет» спостерігається приріст користувачів мобільного телефонного зв'язку у 2005–2023 рр. Період 2005–2010 рр. відображає найвищий приріст користувачів мобільного зв'язку – на +140%: із 2205 млн осіб до 5920 млн осіб, оскільки в цей період відбувався активний розвиток телекомунікацій і запровадження 2G-, 3G- та 4G-технологій у різних регіонах світу (однак швидкість запровадження нових поколінь зв'язку відрізнялась залежно від готовності регіонів до їх імплементації,

включаючи інвестування в необхідну інфраструктуру). У цей же період спостерігається незначне падіння користувачів фіксованого телефонного зв'язку – на -1%, оскільки в цей час користувачі обирали одночасне використання обох технологій.

Проте в 2011–2015 рр. від використання фіксованого телефонного зв'язку відмовились 15% користувачів, що підтверджувалось збільшенням користувачів мобільного телефонного зв'язку на +35% (7132 млн осіб у 2015 р. порівняно з 5290 млн осіб у 2010 р.). Варто зазначити, що стримувальними факторами розгортання мобільного зв'язку є висока вартість телекомунікаційного обладнання та олігополізований ринок. Часто в країнах може існувати від однієї до п'яти телекомунікаційних компаній, які мають стабільну частку ринку та не готові інвестувати в розвиток нових видів технологій без стимулів від держави.

Відповідно у 2016–2020 рр. темп приросту становив +16% або 8268 млн осіб в абсолютному вимірі. Однак у 2018 році була представлена технологія 5G, що значно оптимізує можливості мобільного спілкування та передачі даних. Тому потенціал розвитку технологій даного типу є основою для максимізації покриття населення мобільним зв'язком. У цей період кількість користувачів фіксованого телефонного зв'язку зменшилась на -14% порівняно з 2015 р., тобто поступово відбувався відплив у мобільний сегмент.

Станом на 2023 рік кількість користувачів мобільного зв'язку становить 8891 млн, в той час як фіксованого – майже в 10 разів менше (861 млн). Однак особливістю підрахунку користувачів мобільного телефонного зв'язку є визначення активних абонентів кожного мобільного оператора, відповідно такий підхід не відображає унікальних користувачів. Основними причинами використання кількох мобільних операторів одночасно науковці вважають:

- використання користувачем різних технологій, що відрізняються швидкістю передачі даних та покриттям [227];
- недоступність покриття одного оператора на всіх локаціях, де часто перебуває користувач [206];

- користувач часто подорожує, відповідно використання одного оператора є недостатнім через особливості послуг роумінгу;
- використання користувачем кількох операторів у межах однієї країни, оскільки наявна можливість безкоштовного з'єднання з користувачами аналогічного оператора;
- висока вартість послуг, до яких входять мобільний голосовий та інтернет-зв'язок, відповідно користувачі купують продукти з голосовим наповненням у одного оператора, а продукти з інтернет-наповненням – в іншого залежно від цінової пропозиції;
- використання різних операторів для збереження анонімності із зловмисною метою: шахрайство, фішинг, створення фейкових акаунтів тощо.

Таким чином, у 2023 р. проникнення користувачів мобільного зв'язку на 100 осіб становило 110,6 активних користувачів, порівняно зі 103,1 користувачів у 2018 р. та 93,1 користувачів у 2013 р. Відповідно стан ринку телекомунікацій відображає наявність мультикористувачів, а отже, послуги телекомунікаційних операторів доцільно оптимізувати шляхом розширення покриття та введення обов'язкової ідентифікації абонентів для зменшення рівня зловмисних дій.

Дотичним показником є покриття населення мобільним зв'язком, що відображає максимальну доступність сервісу мобільного зв'язку у світі. Однак через відсутність повних історичних даних з 2005 р. розглянемо період 2013–2023 рр.

Станом на 2013 р. доступне покриття населення мобільним зв'язком було вищим, ніж кількість користувачів мобільного зв'язку через високу вартість мобільних телефонів та зв'язку в цілому. В цей період існувала тенденція використання одного мобільного телефону на домогосподарство.

Однак, починаючи з 2014 р., тренд змінився завдяки масштабуванню випуску доступних девайсів та створенню операторами доступних пакетів, що мали нижчу вхідну вартість через обмежене наповнення тарифів продуктами операторів мобільного зв'язку. Таким чином, з 2014 р. по 2023 р. спостерігається перевищення кількості користувачів мобільного зв'язку над покриттям населення

мобільним зв’язком через зазначену особливість телекомунікаційних ринків-мультикористувачів.

Темп приросту покриття населення мобільним зв’язком був стабільним протягом проаналізованого періоду, оскільки залежав від рівня інвестування держав та організацій у розвиток вказаного напрямку: у 2017 р. приріст становив +4,4% порівняно з 2013 р.; у 2020 р. – +4,1%; однак у 2023 р. приріст дещо сповільнився до +3,5% через зростання нестабільності, що спровокувала зупинки у виробництві та постачанні обладнання. Також, аналізуючи регіональний розріз, спостерігаємо відставання темпів розвитку покриття населення мобільним зв’язком у країнах Африки – 93,3%; та Америки – 97,4%, порівняно з середнім значенням по світу – 98,9% у 2023 р.

Отже, станом на 2023 р. покриття населення мобільним зв’язком сягнуло 7669 млрд осіб, демонструючи середній щорічний темп приросту +1,5% починаючи з 2014 р., через повільний розвиток технологій мобільного зв’язку внаслідок високої вартості інвестицій у їх розбудову.

Ще одним показником цифровізації є обсяг інвестицій у розбудову IT-інфраструктури, що розширює сфери застосування інформаційних технологій та збільшує їх розмаїття. Також показник експорту високих технологій пов’язаний з інвестиціями в розбудову IT-інфраструктури, оскільки на основі наявної IT-інфраструктури можливе створення інноваційної продукції (рис. 2.3).

Оскільки початок збору даних про обрані показники почався пізніше за статистичний збір інформації про користувачів інтернету і телефонного зв’язку, для аналізу було обрано період останніх десяти років. Варто зазначити, що через технічні обмеження доступності інформації в регіональному розрізі деяких країн дані про обсяг експорту високих технологій відсутні в базі World Bank.

Обсяг інвестицій у розбудову IT-інфраструктури формується як сума CAPEX (Capital expenditures) телекомунікаційних операторів, CAPEX у гіпермасштабне обладнання і програмне забезпечення та CAPEX в IT-системи організацій [180].

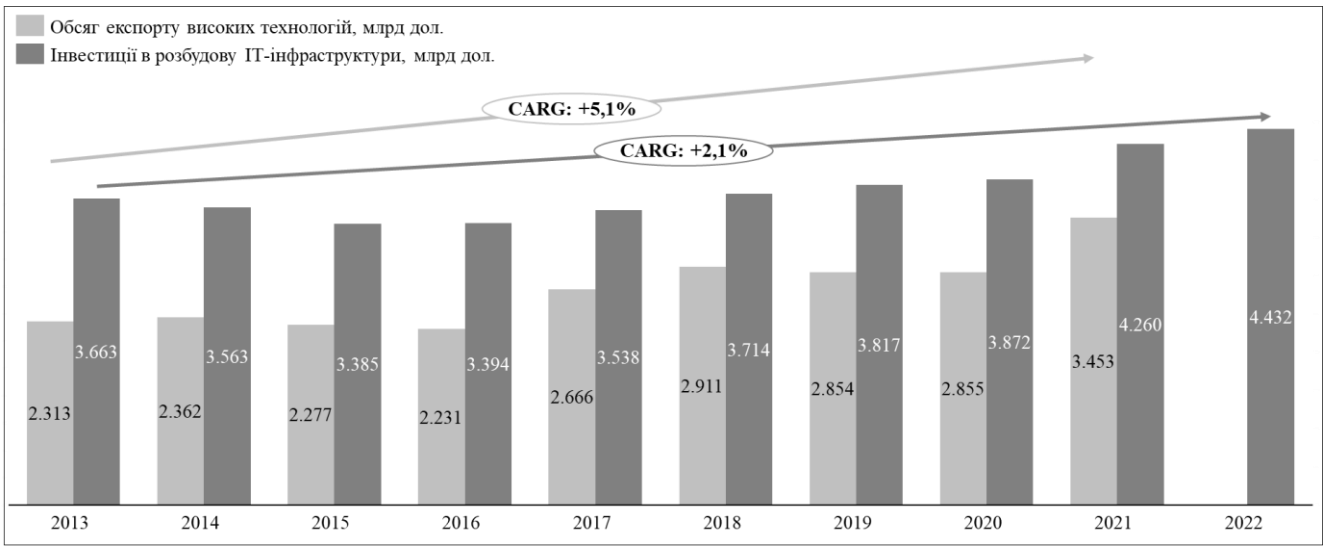


Рисунок 2.3. Динаміка обсягу інвестицій у розбудову IT-інфраструктури та обсягу експорту високих технологій у 2013–2022 рр., млрд дол.

Джерело: складено автором на основі [167; 180]

Так, протягом 2013–2022 рр. середньорічний темп зростання (CAGR) обсягу інвестицій у розбудову IT-інфраструктури становив 2,1%, тоді як обсягу експорту високих технологій – 5,1%.

Інвестиції в розбудову IT-інфраструктури зменшувались зі 3663 млрд дол. до 3385 млрд дол. у період 2013–2015 рр. через зміну пріоритетів урядів та організацій щодо стратегічного розвитку IT-сфери. Відповідно протягом даного періоду відбувались дослідження особливостей та специфіки функціонування нових технологій, на основі яких ухвалювали рішення щодо їх запровадження та розгортання.

У період із 2106 р. по 2020 р. вказаний показник поступово зростав (у середньому на 2,7%), передусім завдяки збільшенню CAPEX у гіпермасштабне обладнання, програмне забезпечення та IT-системи компаній-інвесторів і транснаціональних організацій.

Однак у 2021 р. інвестиції зросли до 4260 млрд дол., що на +10% більше, ніж у 2020 р. Збільшення обсягу інвестицій пояснюється глобальним трендом переорієнтації на цифровий формат ведення та обслуговування бізнес-діяльності, що зумовлює зменшення похибок і недоліків, а тому підвищення ефективності процесів.

Особливої уваги заслуговує значення обсягу експорту високих технологій у 2021 р., який зріс на 20,9% порівняно з 2020 р., що свідчить про значну активізацію розвитку інноваційних продуктів та їх конкурентоздатність на глобальних ринках. Також щорічне збільшення експорту формувалось на основі зростання попиту на відповідні товари через автоматизацію виробництва, розширення можливостей інноваційних технологій та необхідність економічного підйому після кризи, спровокованої COVID-19.

Однак, окрім покращення показників, що відображають розвиток глобальних цифровізаційних процесів, протягом останнього десятиліття спостерігався ріст зловмисних дій з використанням інноваційних систем і технологій. Відповідно, на даному етапі почався збір однорідних даних про ризики кіберпростору. Тому для наступного аналізу було обрано період останніх десяти років.

Проблемою відстежування динаміки зростання кіберінцидентів з використанням сучасних технологій є відсутність централізованого механізму збору та впорядковування даних, а також визначення самого факту настання кіберінцидентів.

На основі оцінних значень міжнародних агрегаторів даних доцільно розглянути динаміку кіберінцидентів, реалізованих через використання шкідливого програмного забезпечення (рис. 2.4) [132; 197].

Рисунок 2.4. Динаміка кіберінцидентів, що реалізовані через шкідливе програмне забезпечення у 2013-2022 рр., млрд

Джерело: складено автором на основі [134; 200]

На основі віднайденої інформації бачимо, що умовно виділяються три періоди змін у динаміці кіберінцидентів, які реалізовані через шкідливе програмне забезпечення у 2013–2022 рр.

Перший період – 2013–2016 рр., протягом якого середній рівень кіберінцидентів за рік був приблизно однаковим та становив 7,7 млрд, демонструючи незначне зростання з 7,1 млрд у 2013 році до 7,9 млрд у 2016 р. (+11,3%).

У період 2016–2019 рр. кількість кіберінцидентів почала інтенсивніше зростати (на +25,3% у 2019 р. порівняно з 2016 р.) та досягла 9,9 млрд через розвиток розмаїття програм, сервісів, мережевих каналів спілкування та проникнення мережі «Інтернет», що спростило доступ зловмисників до девайсів та чутливої інформації. Ще однією причиною росту кіберінцидентів в цей проміжок часу була відсутність глобальної стратегії розвитку кібербезпеки.

На противагу цьому, починаючи з 2020 р. кількість кіберінцидентів скоротилась майже вдвічі порівняно з 2019 р. (-44,4% станом на 2022 р.) через низку факторів, що обмежили дії зловмисників, а саме: активна робота над покращеннями технологій захисту після переходу на дистанційний формат роботи через пандемію COVID-19; вдосконалення інституційно-правового регулювання сфери кібербезпеки на локальному, національному та міжнародному рівнях; концентрація національних стратегій розвитку кібербезпеки на підвищенні рівня цифрової грамотності населення, оскільки перший рік після початку пандемії, для якого був характерний масовий перехід на віддалений формат роботи, довів низький рівень кваліфікації населення в кіберпросторі; зміна стратегій зловмисників, які обирали більші і дорожчі цілі для атаки, щоб не витрачати ресурси для маловигідних результатів. Також варто зауважити, що відображена інформація сформована на основі зафіксованих та зареєстрованих випадків, відповідно кіберінциденти, які не були простежені чи були приховані, не входять до вказаної динаміки.

Результативність реалізованого кіберінциденту визначається обсягом завданих втрат. Обсяг збитків від кіберінцидентів також обраховують на основі

експертних оцінок, оскільки підходи до визнання і підрахунку втрат відрізняються, а також тому, що факт настання кіберінциденту постраждалі часто приховують, щоб уникнути репутаційної шкоди (рис. 2.5) [157].

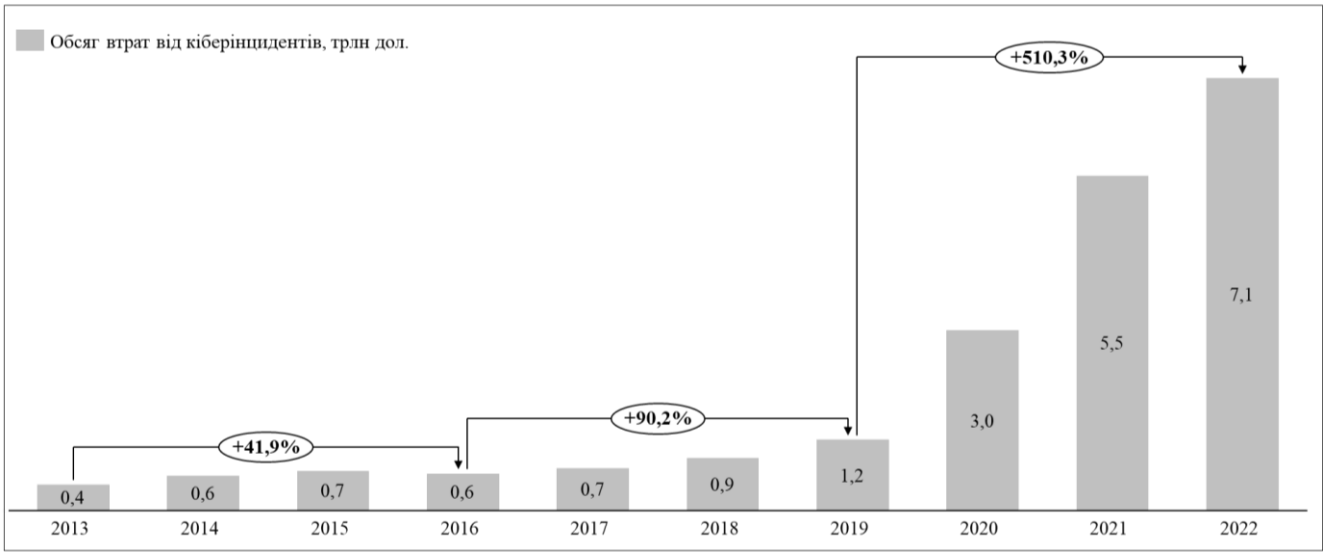


Рисунок 2.5. Динаміка втрат від кіберінцидентів у 2013–2022 рр., трлн дол.

Джерело: складено автором на основі [159]

Як бачимо, динаміка втрат від кіберінцидентів є оберненою до динаміки кількості кіберінцидентів, реалізованих через шкідливе програмне забезпечення у 2013–2022 рр. Зрозуміло, що варто враховувати різницю в підходах до оцінювання вказаних показників, однак періодизація динаміки їх змін є взаємопов'язаною. Аналогічно до попереднього показника можемо умовно розділити динаміку втрат від кіберінцидентів на три періоди.

За перший період – 2013–2015 рр. – втрати від кіберінцидентів у середньому становили 0,55 трлн дол. через нецільовий характер кіберінцидентів, а також відсутність значної кількості хакерских угруповань.

На другому періоді – 2017–2019 рр. – позначився ріст втрат до 0,83 трлн дол. в середньому за рік (+90,2% у 2019 р. порівняно з 2016 р.) через розвиток та поширення різнопланових додатків, встановлення яких було неліцензованим, збільшення доступності смартфонів та зростання проникнення мережі «Інтернет». Упродовж цього періоду найбільший приріст було зафіксовано 2019 року (1,2 трлн дол., на 34,9% більше, ніж 2018 року), що

пов’язано з початком пандемії COVID-19 та першими хвилями виходу на віддалений формат ведення бізнесу.

Третій період, що почався з 2020 р., відзначився стрімким темпом приросту втрат від кіберінцидентів (середньорічний темп зростання становив 54,9% порівняно з 18,0% у 2013–2019 рр.) через зміну підходів до реалізації кіберінцидентів зловмисниками. В цей період багато ІТ-спеціалістів втратили роботу через скорочення, пов’язані з кризою внаслідок пандемії, тому дехто обирав кіберзлочинність як спосіб заробітку.

Окрім цього, хакери об’єднувались у групи задля більшої ефективності, а також починали співпрацювати з організаціями та урядами з метою отримання фінансування. Відповідні хакерські об’єднання здійснювали цілеспрямовані багатокомпонентні атаки, завдаючи катастрофічних збитків компаніям, міжнародним організаціям та навіть урядам. Таким чином, у 2023 р. оцінні втрати від кіберінцидентів зросли на +510,3% порівняно з 2019 р. та становили 7,1 трлн дол.

Оскільки протягом 2013–2022 рр. збільшувалась різноманітність кібер-ризиків, а також зростали втрати від кіберінцидентів, ринок страхування підлаштовувався та реагував на новітні виклики. За даними GlobalData, валові премії страхування кібер-ризиків постійно збільшувались протягом проаналізованого періоду [126; 159]. Однак варто враховувати, що відображені дані є оцінними, оскільки страховики поки не публікують деталізованої інформації про страхування кібер-ризиків через відсутність єдиної уніфікованої методології виокремлення вказаного виду страхування.

Для здійснення порівняльного аналізу варто розглядати динаміку валових премій страхування кібер-ризиків і співвідношення втрат від кіберінцидентів та валових премій страхування кібер-ризиків (рис 2.6).

У період 2013–2022 рр. ринок страхування кібер-ризиків пройшов три ключових етапи розвитку. Перший етап – з 2013 по 2015 рр. – характеризувався незначним обсягом премій страхування кібер-ризиків (у середньому 1,9 млрд дол.), в той час як співвідношення втрат від кіберінцидентів до валових

премій страхування кібер-ризиків зростало та досягло 32,2 тис до 1 у 2015 р., оскільки темпи приросту кіберінцидентів перевищували інвестиції в управління кібер-ризиками, тобто в їх страхування.

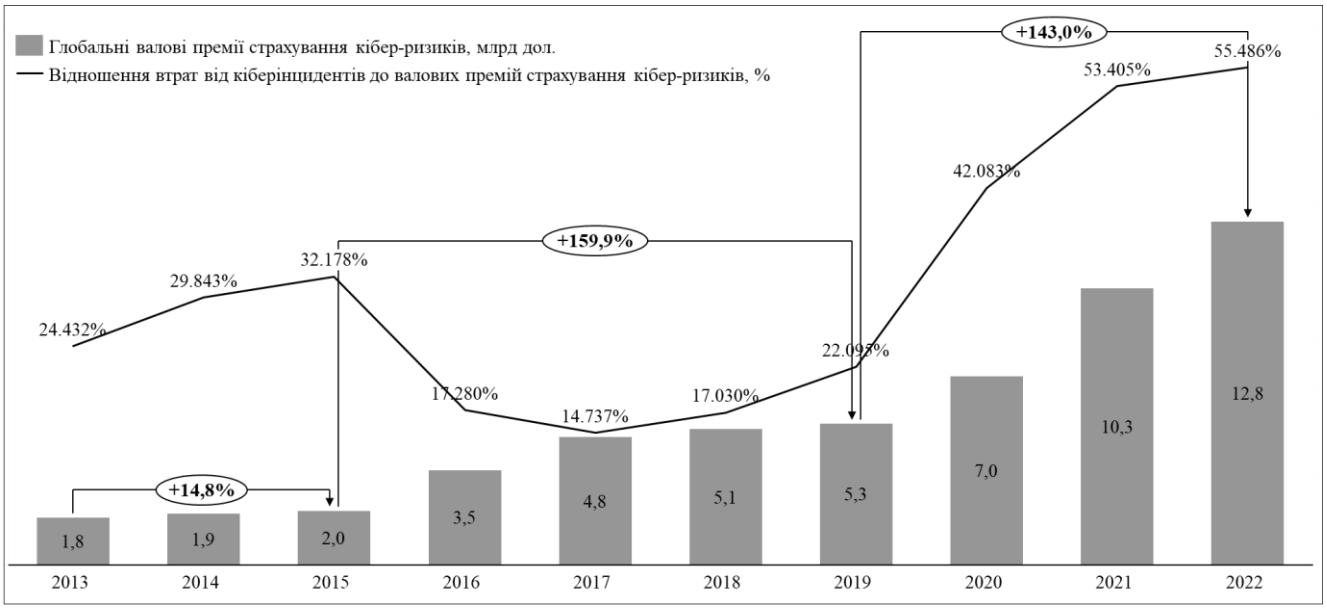


Рисунок 2.6. Динаміка валових премій страхування кібер-ризиків та співвідношення втрат від кіберінцидентів до валових премій страхування кібер-ризиків у 2013–2022 рр., млрд дол., %

Джерело: складено автором на основі [126; 159]

Наступний етап, що охоплює 2016–2019 рр., відзначився зростанням валових премій страхування кібер-ризиків на 159,9% порівняно з 2015 р. через активну популяризацію даного виду страхування в контексті глобальних стратегій підвищення рівня кібербезпеки. Відповідно, співвідношення втрат від кіберінцидентів до валових премій страхування кібер-ризиків впало і становило в середньому 16,4 тис до 1. Проте у 2019 р. спостерігався найбільший приріст співвідношення втрат від кіберінцидентів на даному етапі внаслідок ефекту пандемії COVID-19.

Третій період динаміки активного росту валових премій страхування кібер-ризиків тривав упродовж 2020–2022 рр. (+143,0% у 2022 р. порівняно з 2019 р.). Проте значне зростання даного показника пов’язане з аналогічним зростанням співвідношення втрат від кіберінцидентів до валових премій страхування кібер-ризиків (у середньому 50,32 тис до 1). Відповідно, усвідомлення обсягу реальних

збитків від кіберінцидентів стало основою зростання страхових премій як інструмента управління ризиком.

За прогнозами експертів, глобальні валові премії страхування кібер-ризиків у 2023 р. можуть зрости до 16,66 млрд дол. через розвиток ринку криптоактивів та оптимізацію вартості страхових полісів [123]. Основними сферами, де використовували страхування кібер-ризиків, були: охорона здоров'я, дистрибуція, фінансовий сектор, IT-сектор і телекомунікації, виробництво.

Як бачимо, за останні 10 років відбулось стрімке зростання показників цифрового розвитку. Проте варто дослідити, чи існує вплив вказаних показників на валові премії страхування кібер-ризиків, тобто чи дійсно на розвиток страхування кібер-ризиків впливає цифрова трансформація. Ми вважаємо, що на розвиток страхування кібер-ризиків впливають:

- покриття населення мобільним зв'язком, оскільки сьогодні доступ до телекомунікаційної мережі є мінімальною вимогою для реалізації навмисних кібер-ризиків;
- обсяг втрат від кібератак, оскільки особливістю страхування кібер-ризиків є формування попиту на страхові продукти водночас з усвідомленням їх наслідків. Відповідно, приклади фактично завданих збитків від реалізованих кібер-ризиків підвищують інтерес до вказаного страхування;
- обсяг інвестицій в IT-системи, оскільки інвестиції в розбудову IT-інфраструктури збільшують сфери їх застосування.

На основі переліченого сформуємо гіпотезу, що описує драйвери розвитку страхування кібер-ризиків.

Збільшення покриття населення мобільним зв'язком, обсягу втрат від кібератак та обсягу інвестицій в IT-системи спричиняє зростання валових премій страхування кібер-ризиків.

Для перевірки даної гіпотези варто використовувати методи економетричного моделювання. Доцільно застосувати метод найменших квадратів, оскільки він може враховувати випадкові варіації даних, характерні для кіберсфери, що дасть змогу побудувати адекватну модель.

Перевірку гіпотези здійснюємо з використанням досліджуваних показників із Таблиці 2.1.

Таблиця 2.1

Вхідні дані для перевірки гіпотези про фактори впливу на зростання валових премій страхування кібер-ризиків

Показник	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Покриття мобільним зв'язком, млн осіб	6749	6894	7043	7168	7307	7405	7516	7605	7690	7774
Втрати від кібератак, трлн дол.	0.43	0.57	0.65	0.61	0.70	0.86	1.16	2.95	5.49	7.08
Інвестиції в IT-системи, млрд дол.	3663	3563	3385	3394	3538	3714	3817	3872	4260	4432
Валові премії страхування кібер-ризиків, млрд дол.	1.76	1.91	2.02	3.53	4.75	5.05	5.25	7.01	10.28	12.76

Джерело: складено автором на основі [126; 159; 180; 181]

Унаслідок побудови моделі, в якій валові премії страхування кібер-ризиків (Cyber_insurance_premiums) є результативним показником (залежна змінна), а покриття мобільним зв'язком (Population_cover), втрати від кібератак (Cyber_damage), інвестиції в IT-системи (IT_costs) є впливовими показниками (незалежні змінні), було отримано такі результати (Таблиця 2.2).

Таблиця 2.2

Результати перевірки математичної моделі досліджуваної гіпотези

Показник	Коефіцієнт	Статистична похибка	t-статистика	p-значення
const	−32,0502	752,245	−4,261	0,0053
Cyber_damage	0,823256	0,238834	3,447	0,0137
Population_cover	0,0042137	0,000867721	4,856	0,0028
IT_costs	0,00132069	0,00161165	0,8195	0,4438

Джерело: розрахунки автора на основі Таблиці 2.1

Для перевірки статистичної гіпотези моделі було прийнято рівень значущості 0,05 (5%). Відповідно p-значення є статистичною мірою, що

відображає ймовірність 95% отримання залежності між показниками вибірки при багаторазових повтореннях експерименту у разі, якщо гіпотеза правильна.

Р-значення для показника «IT_costs» є більшим за прийнятий рівень 0,05 та становить 0,4438, що свідчить про незначущість обраного показника у моделі гіпотези, тому приймаємо гіпотезу Н0 про незначущість даного показника. Однак р-значення для показників «Population_cover» та «Cyber_damage» менші за прийнятий рівень 0,05. Відповідно модифікуємо запропоновану гіпотезу, що описує драйвери розвитку страхування кібер-ризиків:

Збільшення покриття населення мобільним зв'язком та обсягу втрат від кібератак спричиняє зростання валових премій страхування кібер-ризиків.

У процесі проведення тестування моделі перевірки модифікованої гіпотези було отримано такі результати (Таблиця 2.3).

Таблиця 2.3

Результати перевірки математичної моделі досліджуваної модифікованої гіпотези

Показник	Коефіцієнт	Статистична похибка	t-статистика	p-значення
const	−28,3828	590,284	−4,808	0,0019
Cyber_damage	0,990464	0,121179	8,174	7,95e-05
Population_cover	0,00434508	0,000832546	5,219	0,0012
Ср. зал. змін.		5,432000	Ст. відх. зал. змін.	3,673998
Сума кв. залишків		2,106095	Ст. похибка моделі	0,548517
R-квадрат		0,982664	Випр. R-квадрат	0,977710
F(2, 7)		198,3880	P-значення (F)	6,86e-07

Джерело: розрахунки автора на основі Таблиці 2.1

Побудовану модель модифікованої гіпотези можна подати у вигляді рівняння:

$$Cyber\_insurance\_premiums = -28.4 + 0.990 * Cyber\_damage + \\ +0.00435 * Population\_cover, \quad (2.1)$$

де $Cyber\_insurance\_premiums$ – валові премії страхування кібер-ризиків;

$Population\_cover$ – покриття населення мобільним зв'язком;

$Cyber\_damage$ – втрати від кібератак.

Для підтвердження запропонованої гіпотези здійснюємо перевірку моделі за допомогою статистичних тестів.

Р-значення для всіх показників моделі є меншим за прийнятий рівень значущості 0,05 (5%), відповідно це свідчить про їх значущість для моделі, тобто наявний вплив покриття населення мобільним зв'язком та втрат від кібератак на обсяг валових премій страхування кібер-ризиків. Отже, приймаємо гіпотезу Н1 про значущість даних показників.

Адекватність моделі, тобто відповідність моделі фактичним даним процесу, відображає Р-значення (F), що менше за прийнятий рівень значущості 0,05 (5%). За підсумками тестування Р-значення (F)=6,86e-0, це свідчить про те, що побудована модель є адекватною, тому приймаємо гіпотезу Н1 про адекватність побудованої моделі.

Для перевірки існування залежності між випадковими значеннями проводимо тест на автокореляцію. У запропонованій моделі автокореляція відсутня, оскільки р-значення більше за прийнятий рівень значущості 0,05 (Тестова статистика: р-значення=0,582; Ljung-Box: р-значення=0,459), тому приймаємо Н0 про відсутність автокореляції (Таблиця 2.4).

Таблиця 2.4

Результати перевірки математичної моделі досліджуваної модифікованої гіпотези на автокореляцію

Показник	Коефіцієнт	Статистична похибка	t-статистика	р-значення
const	0,864790	6,37849	0,1356	0,8966
Cyber_damage_bn	0,0324482	0,139009	0,2334	0,8232
Population_cover	−0,000126041	0,000901287	−0,1398	0,8934
uhat_1	0,263284	0,452317	0,5821	0,5817
Невиправлений R-квадрат = 0,053451				
Тестова статистика: LMF = 0,338817, р-значення = P(F(1,6) > 0,338817) = 0,582				
Альтернативна статистика: TR^2 = 0,534512, р-значення = P(Хі-квадрат(1) > 0,534512) = 0,465				
Ljung-Box Q' = 0,549544, р-значення = P(Хі-квадрат(1) > 0,549544) = 0,459				

Джерело: розрахунки автора на основі Таблиці 2.1

Далі потрібно протестувати модель на наявність гетероскедастичності, що означає несталість умовної дисперсії випадкових відхилень при побудові моделі. Досліджувана модель має p-значення більше від прийнятого рівня 0,05 (Тест Вайта: p-значення=0,804274; Тест Бріша-Пегана: p-значення=0,855731), відповідно приймаємо H0 про відсутність гетероскедастичності, тому модель є гомоскедастичною (Таблиця 2.5).

Таблиця 2.5

Результати перевірки математичної моделі досліджуваної модифікованої гіпотези на гетероскедастичність за тестами Вайта та Бріша-Пегана

Тест Вайта				
Показник	Коефіцієнт	Статистична похибка	t-статистика	p-значення
const	−155,626	184,619	−0,8430	0,4467
Cyber_damage_bn	−14,8618	346,672	−0,4287	0,6902
Population_cover	0,0449869	0,0540289	0,8326	0,4519
sq_Cyber_damage	−0,102991	0,215898	−0,4770	0,6582
X2_X3	0,00203293	0,00469009	0,4335	0,6870
sq_Population_cover	−3,23531e-06	3.93E-01	−0,8225	0,4570
Невиправлений R-квадрат = 0,231355				
Тестова статистика: TR^2 = 2,313553, p-значення = P(Хі-квадрат(5) > 2,313553) = 0,804274				
Тест Бріша-Пегана				
Показник	Коефіцієнт	Статистична похибка	t-статистика	p-значення
const	0,514665	12,9052	0,03988	0,9693
Cyber_damage_bn	−0,121638	0,264931	−0,4591	0,6601
Population_cover	0,000100436	0,00182018	0,05518	0,9575
Пояснена сума квадратів = 0,623198				
Тестова статистика: LM = 0,311599, p-значення = P(Хі-квадрат(2) > 0,311599) = 0,855731				

Джерело: розрахунки автора на основі Таблиці 2.1

Наступним кроком є перевірка якості отриманого регресійного рівняння моделі. Запропонована модель має нормальний розподіл залишків, оскільки різниця між розрахунковими та фактичними значеннями залежної змінної відповідає очікуваним значенням нормальних залишків (Таблиця 2.6). На основі отриманих результатів перевірки приймаємо гіпотезу H0 про нормальність розподілу залишків (p-значення >0,05).

Таблиця 2.6

Результати перевірки математичної моделі досліджуваної модифікованої гіпотези на нормальність залишків

Розподіл частот, спостереження 1-10				
Кількість стовпців = 5, середня = 5,50671e-015, ст. відх. = 0,548517				
Інтервал	Середина	Частота	Відн.	Інтерв.
< -0,65256	-0,84466	1	10%	10%
-0,65256 - -0,26834	-0,46045	1	10%	20%
-0,26834 - 0,11587	-0,076236	3	30%	50%
0,11587 - 0,50008	0,30798	4	40%	90%
>= 0,50008	0,69219	1	10%	100%
Нульова гіпотеза - нормальний розподіл:				
Хі-квадрат(2) = 0,335 p-значення 0,84561				

Джерело: розрахунки автора на основі Таблиці 2.1

Гістограма розподілу залишків моделі досліджуваної модифікованої гіпотези, що показує розподіл різниць між фактичними та розрахунковими значеннями, відображена на рис. 2.7.

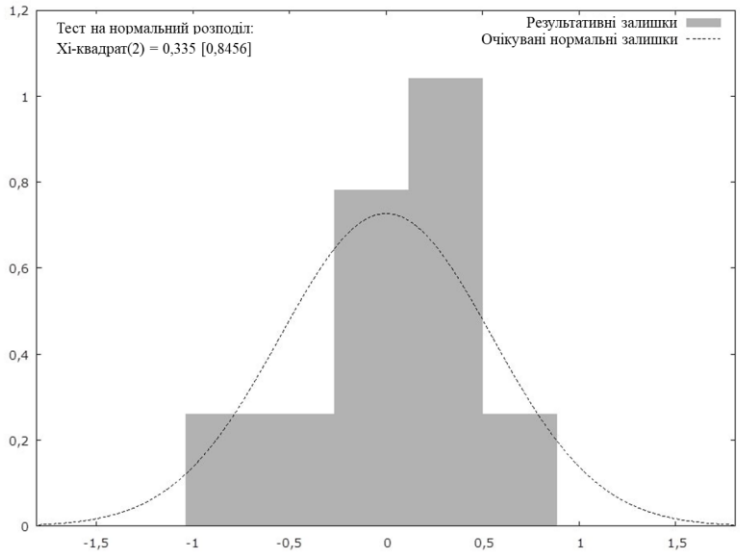


Рисунок 2.7. Гістограма розподілу залишків моделі досліджуваної модифікованої гіпотези

Джерело: розраховано автором на основі Таблиці 2.1

Для доведення коректності обрання функціональної моделі проводимо перевірку на наявність помилок специфікації моделі. Дана перевірка здійснюється за допомогою критерію Рамсея (RESET). Оскільки p-значення більше прийнятого рівня 0,05 (Квадрати та куби: 0,17; Тільки квадрати: 0,0841; Тільки куби: 0,134), приймаємо гіпотезу H0 про правильність специфікації моделі (Таблиця 2.7).

Таблиця 2.7

Результати перевірки математичної моделі досліджуваної модифікованої гіпотези на коректність обраної функціональної форми за тестом Рамсея (RESET)

Тест Рамсея (RESET)		
Квадрати та куби	Тільки квадрати	Тільки куби
Тестова статистика: F = 2,579945, p-значення = =P(F(2,5) > 2,57995) = 0,17	Тестова статистика: F = 4,277149, p-значення = = P(F(1,6) > 4,27715) = 0,0841	Тестова статистика: F = 2,997427, p-значення = =P(F(1,6) > 2,99743) = 0,134

Джерело: розрахунки автора на основі Таблиці 2.1

Унаслідок проведених тестувань було доведено відповідність моделі ключовим метрикам, що визначають можливість її використання. Додатково це підтверджується графічним зображенням різниці між спостережними (фактичними) та розрахунковими значеннями моделі (рис. 2.8).

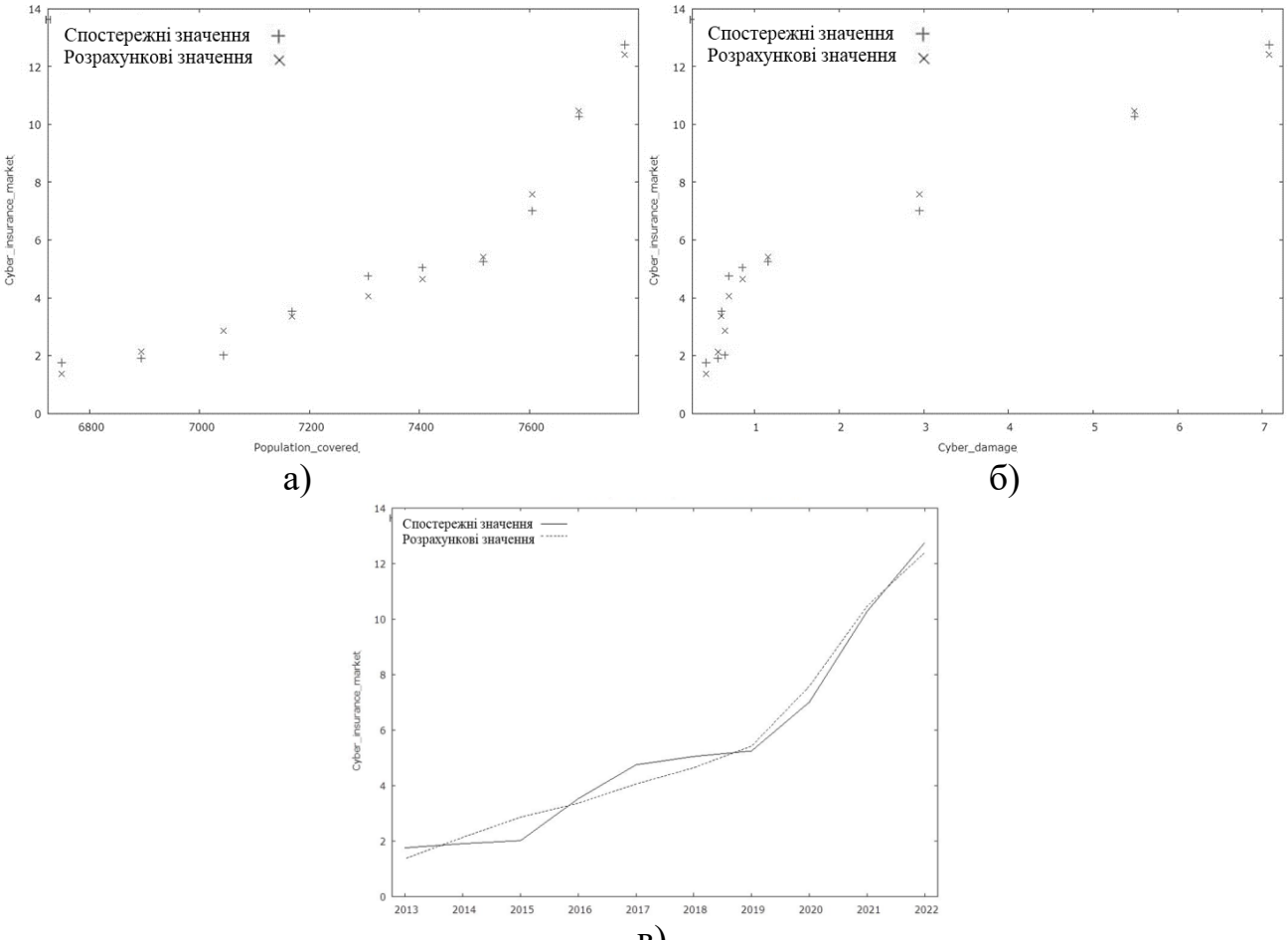


Рисунок 2.8. Графік фактичних та розрахункових значень моделі залежно від: а) покриття населення мобільним зв'язком; б) втрат від кібератак; в) від усіх факторів моделі.

Джерело: розраховано автором на основі Таблиці 2.1

Таким чином, маючи підтвердження взаємозв'язку показників цифрової трансформації та обсягу валових премій страхування кібер-ризиків, можемо систематизувати отримані результати у вигляді хронологічного порядку розвитку страхування кібер-ризиків (рис. 2.9).

Підготовчий етап	Етап зародження	Етап створення самостійних продуктів страхування кібер-ризиків	Етап зростання обізнаності про кібер-ризики	Етап популяризації	Сучасний етап активного розвитку
1950-1989 рр.	**1990-2005 рр.**	**2006-2012 рр.**	**2013-2015 рр.**	**2016-2019 рр.**	**2020 р.- сьогодення**
ГЛОБАЛЬНА ЦИФРОВІЗАЦІЯ					
- Зародження технологій та систем; - створення мережі «Інтернет»; - випуск перших мобільних телефонів та персональних комп'ютерів; - популяризація цифрових камер.	- Розвиток мережевих технологій; - розширення функціоналу мобільних телефонів та персональних комп'ютерів; - перші продажі продуктів страхування кібер-ризиків як додаткового покриття.	- Ріст користувачів мережі «Інтернет» до ~2,9 млрд осіб; - поширення нових технологій та обладнання; - стрімкий ріст розмаїття ПЗ; - початок продажу окремих продуктів страхування кібер-ризиків.	- Розробка глобальних стратегій розвитку кібер-безпеки; - нарощення кількості ПК, ПЗ та обсягів даних; - збільшення премій страхування кібер-ризиків, як інструмента управління ними.	- Розвиток технологій IoT, BigData, Cloud; - ріст доступності мережі «Інтернет»; - поступове збільшення премій страхування кібер-ризиків в рамках стратегій підвищення кібербезпеки.	- Перехід на дистанційний формат роботи через COVID-19; - використання технологій в гібридних війнах; - масштабна автоматизація; - значне нарощення премій страхування кібер-ризиків.

Рисунок 2.9. Періодизація становлення та розвитку глобального ринку страхування кібер-ризиків

Джерело: складено та доповнено автором на основі [100; 190, с.4-6]

Відповідно до запропонованої періодизації, першим періодом становлення та розвитку глобального ринку страхування кібер-ризиків був підготовчий етап, що тривав протягом 1950–1989 рр. Здобутки цього періоду стали передумовою початку цифровізації: винайдено цифрові резистори, мікросхеми; створено доступне мережеве обладнання, що дало змогу масово використовувати мережу «Інтернет»; оптимізовано виробництво персональних комп'ютерів, консолей, це допомогло масштабувати їх використання; поширено використання банкоматів, які мали доступ до даних платіжних карток, інформаційних табло, терміналів; переведено значну частину інформації з паперових носіїв на цифрові; створено блоги та мікроблоги в інтернет-просторі, де користувачі часто залишали вразливу особисту інформацію. Описані фактори стали передумовою розвитку страхування кібер-ризиків, оскільки інноваційні технології розширили спектр можливих кібер-ризиків, а також недостатня обізнаність користувачів інтернету стала однією з головних причин активізації зловмисників.

Другий етап розвитку страхування кібер-ризиків охопив 1990–2005 рр. та став періодом фактичного зародження вказаного виду страхування. Упродовж цього періоду відбулось підвищення продуктивності та можливостей персональних комп'ютерів, поширилось використання мобільних технологій, відповідно збільшивши обсяги передачі даних через онлайн-канали. З метою викрадення інформації зловмисники при передачі даних почали використовувати віруси, що блокували чи порушували стабільність роботи систем, комп'ютерів і телефонів. Незважаючи на протидію таким зловмисним діям за допомогою антивірусів, повністю уникнути кібер-ризиків було неможливо. Науковці відзначають, що в цей період 1997 року фактично був створений перший поліс, який включав покриття відповідальності за безпеку в мережі «Інтернет» [164]. Однак більшість компаній обирала створення власних резервів на випадок настання кіберінциденту, оскільки страхування кібер-ризиків надавало фрагментарне покриття, при цьому маючи високу вартість.

Третій етап розвитку: з 2006 р. по 2012 р. – відзначився формуванням самостійних продуктів страхування кібер-ризиків. У цей період частка користувачів мережі «Інтернет» серед населення світу становила більш ніж 33% завдяки збільшенню кількості мобільних девайсів, які спростили доступ користувачам до онлайн-сервісів із будь-якої точки світу. Найпопулярнішими сервісами в цей період були соціальні мережі, онлайн-ігри, платформи онлайн-оголошень, а також інтеграції платіжних систем на вказані сервіси. Для зловмисників кіберпростору все це значно розширювало можливості компрометації та викрадення даних, оскільки необов'язковим було використання протоколів безпеки на веб-сайтах, а відрізнити справжню платіжну систему від фейкової було майже неможливо без спеціальної кваліфікації. Відповідно, вже були сформовані групи кібер-ризиків, дію яких необхідно було обмежити. Таким чином, поліси страхування кібер-ризиків на даному етапі відокремились від полісів майнового страхування і страхування відповідальності та перейшли в самостійний вид страхування.

Протягом четвертого етапу розвитку страхування кібер-ризиків у 2013–2015 рр. відбулось зростання обізнаності про кібер-ризики, відповідно збільшився попит на страхові послуги даного виду страхування. Ключовими драйверами зростання обізнаності стали розробка та запровадження стратегій покращення кібербезпеки в країнах Європейського Союзу та Сполучених Штатах Америки [140; 171]. Додатково стимулювало розвиток страхування кібер-ризиків масове збільшення кількості та доступності смартфонів, комп'ютерів, інших девайсів, які мали постійний доступ до мережі «Інтернет», генеруючи при цьому великі обсяги даних. Водночас зростала кількість програм та додатків у вільному доступі без необхідного ліцензування. Більшість такого програмного забезпечення була створена зловмисниками з метою отримання доступу до внутрішніх систем та інформації індивідів, що їх встановлять. Для страховиків даний етап розвитку розширив можливості зростання, оскільки в багатьох регіонах ринкова ніша страхування кібер-ризиків була не заповнена.

П'ятий етап розвитку (2016–2019 рр.) відзначився активним насиченням усіх сфер життя новітніми технологіями: IoT, BigData, Cloud, що поступово зменшували участь людини в багатьох процесах. Упродовж цього періоду використання мережі «Інтернет» стало невід'ємною частиною бізнес-діяльності, а тому кібер-ризики стали перманентними. Відповідно страхування кібер-ризиків на даному етапі переросло з інструмента, який мінімізує наслідки настання кіберінциденту, у засіб зниження ймовірності його настання. Також у цей період почали розгортатися партнерські програми співпраці між страховиками та спеціалістами у сфері кібербезпеки, оскільки різноманітність кібер-ризиків постійно зростала, проте у страхових компаній не вистачало експертизи за даним напрямком.

Останній, шостий етап розвитку страхування кібер-ризиків, який розпочався 2020 р. одночасно з масштабним переходом діяльності на віддалений формат через обмеження, спричинені глобальною пандемією COVID-19, триває й досі. На даному етапі відбулась вимушена автоматизація виробництва, сфери обслуговування, послуг; проте приріст покриття населення мережею «Інтернет»

сповільнився, оскільки наблизився до граничного значення. В цей час спостерігався значний приріст втрат від кіберінцидентів, що стимулювало розвиток страхування як інструмента захисту від ризиків такого виду. Додатково варто відзначити, що пріоритетність питання кібербезпеки значно зросла з початком гібридної війни, яку веде Російська Федерація проти України та її партнерів. Так, жертвами контрольованих російським урядом хакерських угрупувань протягом 2021–2023 рр. ставали не лише об'єкти військового та державного значення, а й приватні організації та їх ІТ-інфраструктура. Відповідно використання послуг страхування кібер-ризиків бізнесом є одним із варіантів ефективного управління загрозами у кіберпросторі.

Таким чином, на основі проведеного економетричного моделювання, що підтвердило вплив показників цифровізації на розвиток страхування кібер-ризиків та віднайдених особливостей розвитку технологій, систем і способів управління даними, ми виділяємо шість етапів становлення та розвитку глобального ринку страхування кібер-ризиків, а саме: підготовчий етап; етап зародження; етап створення самостійних продуктів страхування кібер-ризиків; етап зростання обізнаності про кібер-ризики; етап популяризації; сучасний етап активного розвитку.

2.2. Оцінка потенціалу страхування кібер-ризиків як інструмента забезпечення цілей сталого розвитку

На Саміті Організації Об'єднаних Націй (ООН) зі сталого розвитку 2015 року було ухвалено резолюцію «Перетворення нашого світу: Порядок денний в галузі сталого розвитку на період до 2030 року», що окреслила головні вектори зростання і трансформації глобальних сфер життя та діяльності на наступні 15 років [228]. У даному документі було окреслено 17 цілей сталого розвитку, кінцевою метою яких є подолання бідності, захист планети та забезпечення якісних умов життя для стабільності поступу людства.

Проаналізувавши специфіку зазначених у резолюції цілей, ми визначили низку кібер-ризиків, які можуть стати перешкодою для досягнення запланованої мети. Одним із інструментів, що має потенціал подолання вказаних перепон, є страхування кібер-ризиків. Відповідно, аналіз особливостей та можливостей розвитку глобального ринку страхування кібер-ризиків сприятиме вдосконаленню заходів, спрямованих на досягнення Цілей сталого розвитку.

Дев'ята ціль сталого розвитку визначає необхідність оптимізації інфраструктури, проведення інклюзивної індустріалізації за допомогою активного залучення інновацій [93]. Для досягнення даної мети на Саміті ООН було запропоновано: модернізувати інфраструктуру задля підвищення результативності праці через ефективніше використання ресурсів, залучення інновацій та використання екологічно чистих технологій; стимулювати активізацію наукових досліджень у всіх сферах, збільшувати кількість наукових працівників та дослідників завдяки створенню державних і приватних програм підтримки; розширювати та спрощувати доступність до інформаційно-комунікаційних технологій та сприяти розширенню покриття населення мережею «Інтернет».

Оскільки супутнім процесом активного розвитку технологій та інновацій є збільшення видів зловмисних дій у кіберпросторі, тож водночас варто розширювати підходи до управління новітніми ризиками.

Як ми визначили, страхування кібер-ризиків є інструментом запобігання реалізації сучасних кіберзагроз та мінімізації ефектів від наслідків їх настання. Ефективний вплив страхування кібер-ризиків на досягнення Дев'ятої цілі сталого розвитку розкривається через:

- створення механізму моніторингу, управління та нейтралізації кібер-ризиків на інфраструктурі, що була модернізована за допомогою новітніх технологій та автоматизації в рамках превентивних заходів, які проводить страховик та / або його партнери під час страхування кібер-ризиків;
- підвищення рівня цифрової грамотності населення, персоналу організацій, домогосподарств, органів влади завдяки проведенню профілактичних

навчальних програм, залучення наукових працівників до розвитку кібербезпеки на різних рівнях як частини підвищення рівня кібербезпеки потенційного страхувальника на етапі ухвалення рішення щодо доцільності страхування, а також як частини розвитку партнерства страховиків з кваліфікованими фахівцями у сфері кібербезпеки;

- реалізації програм підвищення рівня захищеності, конфіденційності та цілісності особистих даних як складової обов'язків страхувальника щодо використання міжнародних стандартів захисту чутливої інформації.

Шістнадцята ціль сталого розвитку визначає необхідність сприяння розвитку мирних та інклюзивних суспільств, надаючи доступ до правосуддя для всіх і створюючи ефективні, підзвітні та інклюзивні інституції на всіх рівнях [93]. Запропонованими заходами для досягнення вказаної цілі стали: скорочення незаконних фінансових потоків, підвищення ефективності дій, спрямованих на відновлення та повернення викрадених активів; зменшення рівня корупції у всіх сферах; підвищення прозорості та збільшення повноти звітів установ на всіх рівнях.

Середній щоденний обсяг ринку криптовалют, які можуть бути використані як незаконні способи фінансування, відмивання грошей, корупції та шахрайства, перевищував 1,7 трлн дол. у 2023 році, тоді як щоденна кількість фішингових листів, створених для викрадення платіжної інформації, сягала 3,4 млрд [118; 207].

Відсутність єдиних стандартів звітності та належного контролю використання технологічних засобів для передачі, генерації та використання коштів у сучасній цифровій економіці провокує зростання фінансових злочинів у кіберпросторі.

Оскільки частиною процесу страхування кібер-ризиків є створення або оптимізація системи контролю віртуального доступу до фінансових ресурсів організації, використання страхових продуктів даного типу виступає одним із інструментів досягнення Шістнадцятої цілі сталого розвитку:

- забезпечення прозорої звітності страхувальників щодо фінансових операцій у кіберпросторі як умови прийняття на страхування кібер-ризиків, пов'язаних з онлайн-транзакціями та цифровими операціями;

- запобігання корупції, шахрайству та відмиванню коштів у кіберпросторі завдяки розробці індикативних показників безпеки операцій під час проведення превентивних заходів страховиком або його партнерами у сфері кібербезпеки;

- розвиток інституту репутації різних установ та організацій через демонстрацію прозорості їхньої діяльності, а також ефективну стратегію відновлення страхувальника в разі настання страхового випадку, спрямовану на збереження його репутації.

Сімнадцята ціль сталого розвитку описує необхідність поширення партнерств задля підтримання стійкого зростання [93]. З метою досягнення вказаної цілі було запропоновано низку заходів, зокрема: використання сучасних інноваційних екологічно чистих технологій та їх передача на сприятливих умовах; розробка механізму розвитку науково-технічного та інноваційного потенціалу для країн, що розвиваються, з передачею для них наукових знань; поглиблення партнерств на різних рівнях, включаючи регіональний та міжнародний, задля обміну важливими технологіями, що впливають на збереження планети.

Станом на 2023 рік фахівці у сфері кібербезпеки створили систему потужних міжнародних організацій та приватних компаній, що допомагає посилювати захист від загроз кіберпростору. Проте регіональний розподіл таких компаній нерівномірний, оскільки їх більшість розташована та діє в розвинених країнах і країнах, що розвиваються, відповідно обмежуючи доступ для регіонів з малорозвиненою економікою.

Оскільки однією із особливостей страхування кібер-ризиків є створення системи партнерських відносин з експертами у сфері кібербезпеки, страхування даного виду стає ефективним інструментом досягнення Сімнадцятої цілі сталого розвитку завдяки:

- використанню міжнародного досвіду при розробці системи ризик-менеджменту для страхувальників, що означає залучення кваліфікованих спеціалістів на етапі створення нового страхового продукту;

- систематизації інформації про глобальні кібер-ризики та квантифікації їхніх наслідків, створення глобальних агрегованих баз даних, що допоможе надавати кваліфіковану оцінку стану кібербезпеки суб'єктів залежно від їхніх особливостей, що натомість оптимізує підходи до проведення актуарних розрахунків;

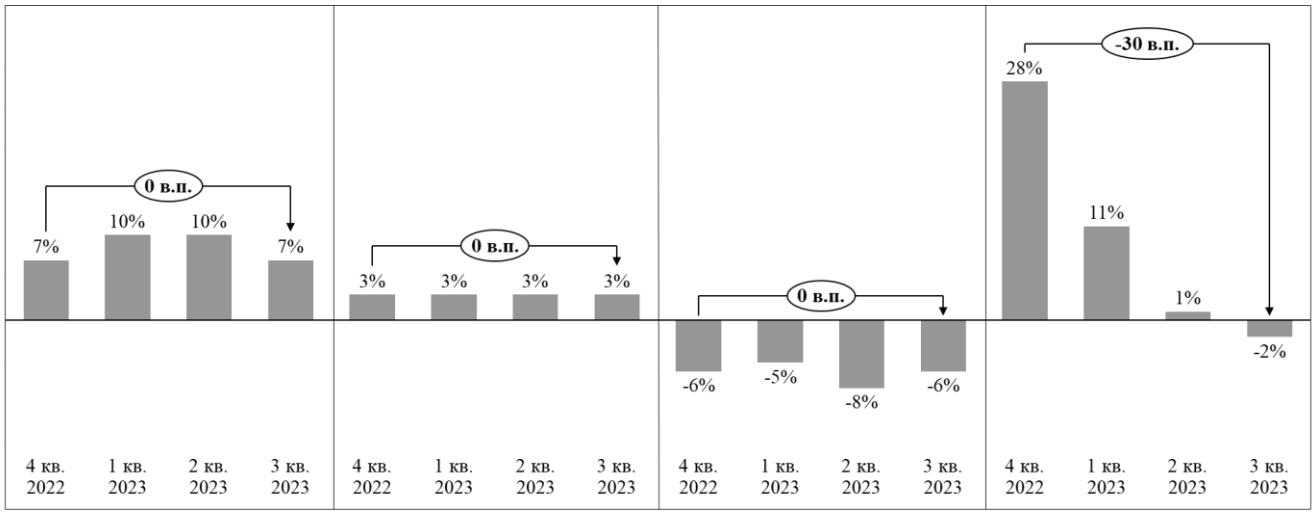
- створенню сприятливого інвестиційного середовища завдяки реалізації міжнародних партнерств, спрямованих на виявлення потенціалу росту в різних технологічних галузях, які відзначатимуть свою надійність та розвиненість завдяки наявності страхування від кібер-ризиків.

У глобальному вимірі страхування кібер-ризиків вже відзначило свою ефективність для досягнення Цілей сталого розвитку, тому світовий ринок вказаного виду страхування постійно зростає. Визначення особливих аспектів становлення даного ринку допоможе оцінити потенціал його розвитку в майбутньому.

У 2023 році міжнародна організація Marsh, що здійснює розробку стратегій управління ризиками, почала відстежувати індекс зміни вартості продуктів страхування кібер-ризиків на квартальній основі [162]. Станом на третій квартал 2023 р. індекс зміни вартості продуктів страхування кібер-ризиків став від'ємним -2% (порівняно з +28% у четвертому кварталі 2022 р.) завдяки активному розвитку даного сегменту страхового ринку, зменшенню кількості та серйозності страхових випадків, що виникають через шкідливе програмне забезпечення, збільшенню кількості страхових компаній, що пропонують страхування кібер-ризиків та розробку технологічних систем контролю кібербезпеки, що зумовило зменшення виплат партнерським організаціям.

Для порівняння, динаміка індексу змін вартості продуктів інших видів страхування була стабільною в третьому кварталі 2023 р. порівняно з четвертим кварталом 2022 р. (рис. 2.10):

- майнового страхування ;
- страхування від нещасних випадків;
- фінансового та професійного страхування.



а) б) в) г)

Рисунок 2.10. Індекс зміни вартості продуктів: а) майнового страхування; б) страхування від нещасних випадків; в) фінансового та професійного страхування; г) страхування кібер-ризиків у 4-му кварталі 2022 р. – 3-му кварталі 2023р.

Джерело: складено автором на основі [162]

Одним із важливих аспектів аналізу перспектив розвитку страхування кібер-ризиків є визначення його актуальності для різних сфер. Міжнародна організація Sophos, що надає послуги в секторі кібербезпеки, провела опитування серед IT-спеціалістів організацій багатьох сфер, які розташовані в різних країнах світу, щодо наявності у компаній полісів страхування кібер-ризиків [121].

За даними опитування, кількість організацій, які користувались послугами страхування кібер-ризиків у 2022 р., зросла в середньому до 92% з усіх опитаних (на 7 в.п. більше порівняно з 2020 р.). Окремо експерти виділяють використання послуг страхування кібер-ризиків, які покривають вимагання за відновлення / розшифрування даних, частка використання яких зросла в середньому до 83% з усіх опитаних (на 17 в.п. більше порівняно з 2020 р.).

Приріст страхування такого типу підтверджує активізацію зловмисних дій з використанням методів фішингу, соціальної інженерії та шпигунства. Також

частина сфер була вперше виведена спеціалістами в окрему категорію, тому результати опитування IT-спеціалістів таких сфер за 2020 р. відображені в категорії інші (вища та середня освіта, логістика і транспорт, місцеве управління та урядові установи, охорона здоров'я) (Таблиця 2.8).

Таблиця 2.8

Використання страхування кібер-ризиків за сферами у 2020–2022рр.

Сфера	Наявність полісів страхування кібер-ризиків, % компаній			Наявність полісів страхування кібер-ризиків, що покривають вимагання за відновлення / розшифрування даних, % компаній		
Рік	2020	2022	Приріст	2020	2022	Приріст
IT, технології та телекомунікації	87	94	7 в.п.	70	85	15 в.п.
Бізнес і професійні послуги	87	94	7 в.п.	68	87	19 в.п.
Будівництво та нерухомість	80	89	9 в.п.	62	76	14 в.п.
Виробництво	83	86	3 в.п.	63	75	12 в.п.
Вища освіта	-	90	-	-	78	-
Логістика і транспорт	-	94	-	-	87	-
Енергетичні і комунальні послуги	88	96	8 в.п.	62	89	27 в.п.
Медіа, дозвілля, розваги	88	94	6 в.п.	66	86	20 в.п.
Місцеве управління	-	88	-	-	80	-
Охорона здоров'я	-	89	-	-	78	-
Роздрібна торгівля	83	96	13 в.п.	62	88	26 в.п.
Середня освіта	-	90	-	-	78	-
Урядові установи	-	92	-	-	79	-
Фінансові послуги	86	93	7 в.п.	72	83	11 в.п.
Інші сфери	83	93	10 в.п.	69	85	16 в.п.
Середнє значення	85	92	7 в.п.	66	83	17 в.п.

Джерело: складено автором на основі [121]

Відповідно до наведених даних, станом на 2022 р. найбільша частка компаній, які користуються послугами страхування кібер-ризиків, функціонує у сферах: IT, технології та телекомунікації, бізнес і професійні послуги, логістика і транспорт, енергетичні і комунальні послуги, медіа, дозвілля, розваги, роздрібна торгівля (наявність полісів більш ніж у 94% компаній). Найнижчий показник наявності полісів страхування кібер-ризиків у виробництва – 86%, що

пояснюється низьким рівнем можливості зловмисного втручання в процеси даної сфери.

У 2022 р. найбільший приріст наявності полісів страхування кібер-ризиків продемонстрували сфера роздрібної торгівлі (+13 в.п. порівняно з 2020 р.) і сфера будівництва та нерухомості (+9 в.п.). Однак динаміка наявності полісів страхування кібер-ризиків, що покривають вимагання за відновлення / розшифрування даних, дещо відрізнялась. Лідером була сфера енергетичних і комунальних послуг (+27 в.п. порівняно з 2020 р.), другу позицію зайняла сфера роздрібної торгівлі (+26 в.п. порівняно з 2020 р.), після яких були сфери медіа, дозвілля, розваг та бізнесу і професійних послуг. Також варто зауважити, що приріст даного показника був більше 10 в.п. в усіх сферах, що свідчить про зростання загроз викрадення та видозміни даних.

Аналізуючи структуру здійснених кібератак у 2022 р. за сферами, бачимо, що найбільшу частку (24,8%) мала сфера виробництва, в якої, за аналогічний період, був найнижчий рівень наявності продуктів страхування кібер-ризиків [160]. Дана тенденція стала відмінною від попередніх періодів, оскільки в 2021 році лідерами за часткою кібератак були сфери освіти, фінансових послуг, урядових органів та охорони здоров’я [199]. Ця зміна свідчить про активний та цільовий пошук зловмисниками вразливих і незахищених систем виробництва, що можуть бути пошкоджені та використані з метою глобальної дестабілізації. Однак наступні позиції в рейтингу частки кібератак за сферами у 2022 р. відповідають тренду минулих років (рис. 2.11).

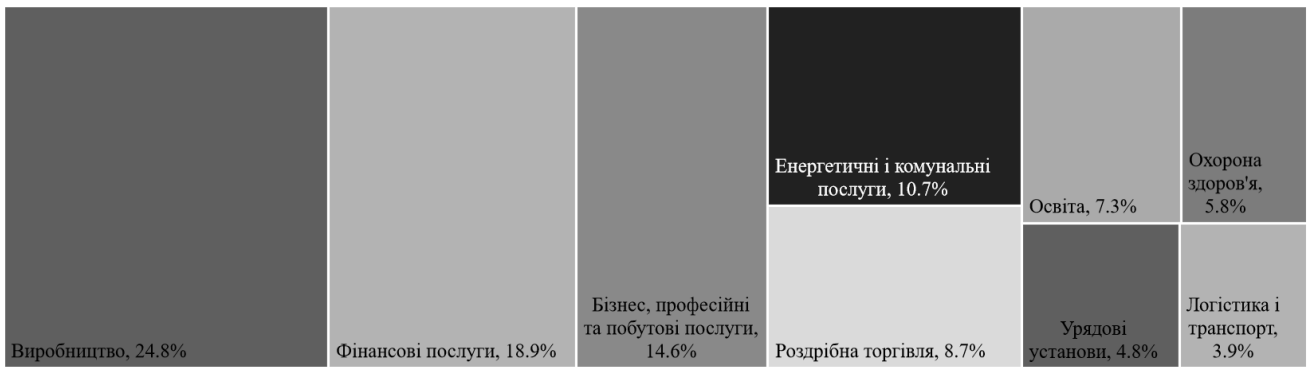


Рисунок 2.11. Розподіл кібератак за сферами у 2022 р.

Джерело: складено автором на основі [160]

Проте, щоб визначити потенційні можливості розвитку ринку страхування кібер-ризиків, варто розглянути характеристики діяльності основного регіону цього ринку – Сполучених Штатів Америки (США) [60].

У 2022 році обсяг валових премій страхування кібер-ризиків у США зріс до 9,66 млрд дол. (76% від глобального обсягу), що на 47,6% більше, ніж у 2021 р., при цьому кількість полісів страхування (не включаючи полісів Alien Surplus Lines) зросла до 3,9 млн, що лише на 4,4% більше, ніж у 2021 р. Така нерівномірність свідчить про збільшення вартості полісів страхування через розширення страхового покриття та зростання рівня збитковості від настання кіберінцидентів [213; 214].

Значне зростання валових премій страхування кібер-ризиків у 2022 р. перевищило темпи росту страхових відшкодувань, що позначилось на падінні рівня збитковості страхової суми до 44,6% (-21,8 в.п. порівняно з 2021 р.). Такий рівень спостерігався 2019 року до глобальної пандемії COVID-19, що свідчить про повернення виплат відшкодувань до органічного докризового рівня (Таблиця 2.9). Також варто відзначити, що ефект зростання розмаїття кібер-ризиків, спричинених COVID-19, позначився на зростанні збитковості страхової суми у 2020–2021 рр., відповідно у 2022 р. страхувальники імпульсивно продовжували нарощувати інвестиції в страхування кібер-ризиків як інструмента, що мінімізує ймовірність негативних втрат від них.

Таблиця 2.9

Основні показники ринку страхування кібер-ризиків США за 2018–2022рр.

Показник	2018	2019	2020	2021	2022
Поліси страхування (без Alien Surplus Lines), млн	3.00	3.31	4.02	3.75	3.91
Приріст рік до року, %	15.5%	10.6%	21.3%	-6.8%	4.4%
Валові премії страхування кібер-ризиків, млрд дол.	3.16	3.36	4.65	6.54	9.66
Приріст рік до року, %	2.2%	6.3%	38.4%	40.6%	47.7%
Збитковість страхової суми, %	35.3%	44.6%	66.9%	66.4%	44.6%

Джерело: складено автором на основі [213; 214]

Ще одним показником, що відображає стан ринку страхування кібер-ризиків США, є розподіл валових страхових премій за видами продукту.

Відповідно у 2022 р. частка валових страхових премій комплексних продуктів становила 2,50 млрд дол. (26%), а частка валових страхових премій самостійних продуктів становила 7,16 млрд дол. (74%). Проте в 2021 р. такий розподіл був дещо іншим: частка валових страхових премій комплексних продуктів становила 2,0 млрд дол. (31%), а частка валових страхових премій самостійних продуктів – 4,54 млрд дол. (69%). Такий розподіл визначає наявність стійкого зростання попиту на самостійні продукти страхування кібер-ризиків, а не бажання отримати комплексні поліси з покриттям інших видів ризиків.

Таким чином, розвиток ринку страхування кібер-ризиків США демонструє важливість даного виду страхування як частини комплексної стратегії покращення рівня кібербезпеки.

Наступним за обсягом валових премій страхування кібер-ризиків є європейський ринок. Однак через відсутність централізованого збору основних показників вказаної страхової діяльності визначення обсягу валових премій страхування здійснюється на основі експертних оцінок. Так, згідно з даними дослідницької агенції Polaris, частка європейських валових премій страхування кібер-ризиків протягом останніх п’яти років оцінювалась у межах від 20% до 25%, однак у майбутньому може зменшуватись через зростання частки азійського ринку даного виду страхування [138].

З метою оцінки потенціалу розвитку страхування кібер-ризиків на території Європейського Союзу Європейське агентство з мережевої та інформаційної безпеки ENISA провело опитування серед менеджменту організації щодо наявного попиту на страхові продукти даного типу [127]. Станом на 2023 р. в середньому 26% опитаних мали поліси страхування кібер-ризиків, з яких найвищий рівень був у опитаних із Західної і Північної Європи (45%), середній – в опитаних із Південної Європи (39%) та найнижчий – в опитаних із Східної Європи (12%). Основними причинами відмови від використання страхування кібер-ризиків як інструмента ризик-менеджменту організації були: висока ціна страхування, невідповідний рівень оцінки страховиком стану потенційного

страхувальника, недостатній обсяг страхового покриття, особливі вимоги страховика, зазначені в умовах страхової угоди.

Однак ті організації, що мають поліс страхування кібер-ризиків, зазначають такі причини його використання: отримання повного відшкодування в разі настання страхового випадку, проведення експертизи стану кібербезпеки страхувальника, широкий постінцидентний супровід страхувальника, вимоги стейкхолдерів або клієнтів.

На основі отриманих результатів опитування ENISA визначила, що близько 50% організацій не користуються послугами страхування кібер-ризиків через відсутність кіберінцидентів у своїй практиці; тоді як до 20% готові отримати поліс страхування кібер-ризиків через широкий набір послуг, які включають залучення експертів у сфері кібербезпеки на різних етапах дії страхової угоди.

Проте варто визначити необхідність розвитку страхування кібер-ризиків у різних регіонах світу, оскільки запровадження вказаного виду страхування є доволі дорогим, а також доцільним для страхувальників із високим рівнем технологічного розвитку. Ґрунтуючись на підсумках проведеного економетричного моделювання, для аналізу регіональної необхідності розвитку страхування кібер-ризиків варто використовувати дані про покриття населення мобільним зв'язком та обсяги втрат від кіберінцидентів.

Використаємо регіональний розподіл країн світу, запропонований World Bank, до якого входять: Північна Америка, Європа і Центральна Азія, Східна Азія та Тихоокеанські країни, Південна Азія, Латинська Америка і Карибський басейн, Субсахарська Африка, Близький Схід і Північна Африка – для аналізу регіональної необхідності розвитку страхування кібер-ризиків [158].

Регіональний розподіл втрат від реалізованих кібер-ризиків 2017 року здійснювала організація McAfee, що створює системи та інструменти захисту від кіберзагроз [186]. Однак через обмеженість фактичної деталізованої інформації про наслідки настання кіберінцидентів обсяг втрат був визначений як частка від ВВП регіону (Додаток Д).

Найбільша середня частка втрат від кіберінцидентів у ВВП 2017 року була в регіону Європа і Центральна Азія (0,84%), на другому місці – Північна Америка зі значенням 0,78%, на третьому місці – Східна Азія та Тихоокеанські країни зі значенням 0,71%, на четвертому місці – Латинська Америка і Карибський басейн зі значенням 0,43%, на п'ятому місці – Південна Азія зі значенням 0,38%, на шостому місці – Субсахарська Африка зі значенням 0,14%, на сьомому місці – Близький Схід і Північна Африка зі значенням 0,11% [186].

Для визначення аналогічного показника у 2022 році використаємо зміну регіонального розподілу ВВП порівняно з 2017 роком, оскільки це дає змогу відобразити оновлений стан економічного розвитку, а тому, відповідно, і обсягу ресурсів, які стають ціллю зловмисників у кіберпросторі (Додаток Д).

Зваживши оновлений регіональний розподіл частки ВВП у 2022 році, отримаємо структуру локальних втрат від кіберзлочинів (рис. 2.12).

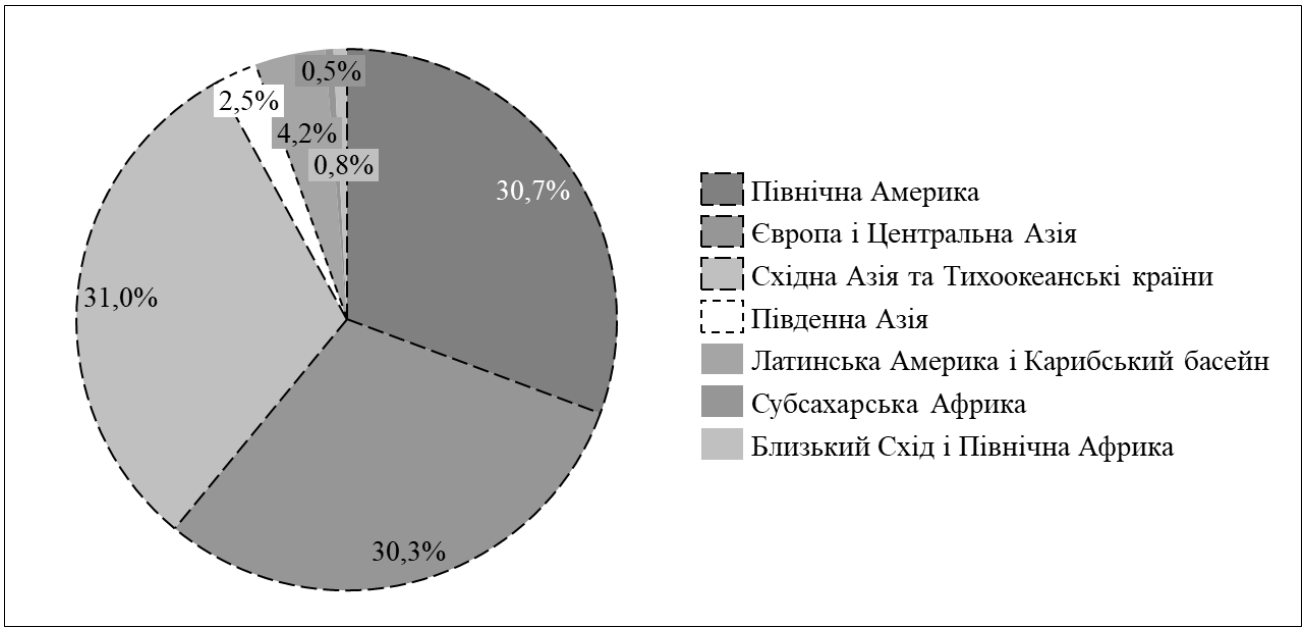


Рисунок 2.12. Регіональний розподіл втрат від кіберзлочинів у 2022 р.

Джерело: розрахунки автора на основі [158; 186]

На першому місці – Східна Азія та Тихоокеанські країни зі значенням 31,05% (+0,72 в.п. порівняно з 2017р.), на другому місці – Північна Америка зі значенням 30,66% (+0,7 в.п. порівняно з 2017р.), на третьому місці – Європа і Центральна Азія зі значенням 30,32% (-2,05 в.п. порівняно з 2017р.), на четвертому місці – Латинська Америка і Карибський басейн зі значенням 4,22% (-

0,06 в.п. порівняно з 2017р.), на п’ятому місці – Південна Азія зі значенням 2,47% (+0,38 в.п. порівняно з 2017р.), на шостому місці – Близький Схід і Північна Африка зі значенням 0,79% (+0,14 в.п. порівняно з 2017р.), на сьомому місці – Субсахарська Африка зі значенням 0,50% (+0,11 в.п. порівняно з 2017р.).

Використовуючи отримані в пункті 2.1 коефіцієнти економетричної моделі модифікованої гіпотези, що відображає фактори впливу на зміну обсягу глобальних валових премій страхування кібер-ризиків, розробимо зведене значення регіональної необхідності розвитку страхування кібер-ризиків. Найбільш доцільним підходом є розробка індексного показника.

Регіональний розподіл покриття населення мобільним зв’язком визначаємо на основі локалізації у World Bank, а обсяг втрат від кіберінцидентів – на основі вищезазначеного розрахунку. Як було виявлено в економетричній моделі, вага коефіцієнтів покриття населення мобільним зв’язком та обсягу втрат від кіберінцидентів становить 0,00435 та 0,99 відповідно.

Для визначення рангової оцінки (від 0 до 7) покриття населення мобільним зв’язком моделі за регіонами, було надано найвищий ранг (7) регіону, значення якого серед інших є найвищим, тоді як ранг решти регіонів був розрахований пропорційно до значення показника регіону, якому було присвоєно найвищий ранг:

$$R_{COV_i} = \frac{C_i * n}{C_{max}}, \tag{2.2}$$

де R_{COV_i} – рангова оцінка покриття населення мобільним зв’язком регіону;

C_i – покриття населення мобільним зв’язком регіону;

C_{max} – максимальне значення покриття населення мобільним зв’язком групи;

n – кількість регіонів.

Аналогічний підхід використаємо для визначення рангової оцінки (від 0 до 7) обсягу втрат від кіберінцидентів моделі за регіонами:

$$R_{DAM_i} = \frac{D_i * n}{D_{max}}, \tag{2.3}$$

де R_{DAM_i} – рангова оцінка обсягу втрат від кіберінцидентів регіону;

D_i – обсяг втрат від кіберінцидентів регіону;

D_{max} – максимальне значення обсягу втрат від кіберінцидентів групи;

n – кількість регіонів.

Відповідно до отриманих результатів, рангова оцінка покриття населення мобільним зв'язком за регіонами очікувано є найвищою в регіоні з найбільшою кількістю населення, тобто в Східній Азії й Тихоокеанських країнах – 7. Наступні за величиною ранги отримали регіон Південна Азія – 3,6; регіон Європа і Центральна Азія – 2,6; регіон Субсахарська Африка – 2,3; регіон Латинська Америка і Карибський басейн – 1,6; регіон Близький Схід і Північна Африка – 1,2; регіон Північна Америка – 0,9.

Дещо іншими є результати рангової оцінки обсягу втрат від кіберінцидентів: регіон Східна Азія і Тихоокеанські країни – 7; регіон Північна Америка – 6,9; регіон Європа і Центральна Азія – 6,8; регіон Латинська Америка і Карибський басейн – 1,0; регіон Південна Азія – 0,6; регіон Близький Схід і Північна Африка – 0,2; регіон Субсахарська Африка – 0,1.

Найвищий ранг за даним показником отримали регіони Східна Азія й Тихоокеанські країни, Північна Америка, Європа і Центральна Азія, оскільки економічний розвиток країн у даних регіонах є вищим та супроводжується значним залученням інноваційних технологій і систем у процеси діяльності, що свідчить про активний процес цифрової трансформації (Таблиця 2.10).

На основі отриманих рангових значень вважаємо за доцільне сформувати інтегральний індекс, що відображає необхідність розвитку страхування кібер-ризиків залежно від особливостей розвитку ключових показників, що впливають на розвиток страхування кібер-ризиків регіону. Для розрахунку варто визначити середнє значення вищезазначених рангових показників:

$$I_{CI_i} = \frac{R_{COV_i} + R_{DAM_i}}{2}, \quad (2.4)$$

де I_{CI_i} – Індекс необхідності розвитку страхування кібер-ризиків регіону;

R_{COV_i} – рангова оцінка покриття населення мобільним зв’язком регіону;

R_{DAM_i} – рангова оцінка обсягу втрат від кіберінцидентів регіону.

Використовуючи запропонований підхід, Індекс необхідності розвитку страхування кібер-ризиків регіону має межі від 0 до 7, де найвище значення Індексу (7) відображає найвищу необхідність розвитку даного виду страхування, а зі зменшенням значення Індексу знижується необхідність розвитку страхування кібер-ризиків.

Таблиця 2.10

Рангові значення показників покриття населення мобільним зв'язком та обсягів втрат від кіберінцидентів за регіонами у 2022 р.

Регіон	Покриття населення мобільним зв'язком, млн осіб			Обсяг втрат від кіберінцидентів, млн дол.		
	Значення показника	**Вага коефіцієнта в економетричній моделі**	**Рангове значення показника**	**Значення показника**	**Вага коефіцієнта в економетричній моделі**	**Рангове значення показника**
Північна Америка	379	0,00435	0,9	2170823	0,99	6,9
Європа і Центральна Азія	1070	0,00435	2,6	2146760	0,99	6,8
Східна Азія і Тихоокеанські країни	2828	0,00435	7,0	2198196	0,99	7,0
Південна Азія	1440	0,00435	3,6	174851	0,99	0,6
Латинська Америка і Карибський басейн	634	0,00435	1,6	298561	0,99	1,0
Субсахарська Африка	919	0,00435	2,3	35054	0,99	0,1
Близький Схід і Північна Африка	503	0,00435	1,2	56047	0,99	0,2

Джерело: розрахунки автора на основі [156; 186; 193]

Відповідно до проведених розрахунків на основі Таблиці 2.10, отримуємо наступні значення Індексу для регіонів:

1. Східна Азія і Тихоокеанські країни – 7;
2. Європа і Центральна Азія – 4,74;
3. Північна Америка – 3,93;
4. Південна Азія – 2,06;
5. Латинська Америка і Карибський басейн – 1,26;
6. Субсахарська Африка – 1,19;
7. Близький Схід і Північна Африка – 0,71.

Найвище значення Індексу отримав регіон Східна Азія і Тихоокеанські країни, оскільки регіон займає основну частку покриття населення мобільним зв'язком (36%) та обсягу втрат від кіберінцидентів (31%). Значне збільшення використання технологій та інформаційних систем як основних джерел виникнення кіберзагроз є додатковим стимулом для розвитку страхування кібер-ризиків у регіоні.

На другому місці за значенням Індексу перебуває регіон Європа і Центральна Азія, незважаючи на те, що частка покриття населення мобільним зв'язком є третьою у світі (14%). Драйвером збільшення необхідності розвитку страхування кібер-ризиків у регіоні є значна частка втрат від кіберінцидентів (30%). Стабільний економічний розвиток країн цього регіону завдяки значній автоматизації усіх сфер життя робить локальну IT-інфраструктуру привабливою мішенню для зловмисників у кіберпросторі.

Третю позицію за значенням Індексу займає регіон Північна Америка. Варто зазначити, що частка покриття населення мобільним зв'язком є невисокою (лише 5%), однак значною є частка втрат від кіберінцидентів (31%). Оскільки даний регіон характеризується високим рівнем залучення новітніх технологій, що об'єднані через мережу «Інтернет», проте є недостатньо захищеними, зловмисники використовують вразливості систем задля отримання фінансових активів постраждалих чи викупу від них.

На четвертій позиції за значенням Індексу міститься регіон Південна Азія, у якого частка покриття населення мобільним зв'язком досить висока (19%), однак частка втрат від кіберінцидентів незначна (2,47%). Більшість країн даного регіону недостатньо розвинуті в цифровому просторі, відповідно канали доступу до їхніх цифрових активів обмежені для зловмисників.

П'яту позицію за значенням Індексу займає регіон Латинська Америка і Карибський басейн. Частка покриття населення мобільним зв'язком регіону середня (8%), аналогічно з часткою втрат від кіберінцидентів (4%). Цифрова трансформація цього регіону перебуває на початковому етапі, відповідно використання новітніх технологій обмежене. Таким чином зловмисники не

можуть використовувати значний обсяг сучасних інструментів для шкідливого впливу на ІТ-інфраструктуру регіону.

Шосте місце за значенням Індексу займає регіон Субсахарська Африка. Попри те, що частка покриття населення мобільним зв'язком там середня (12%), Індекс є одним із найнижчих через незначну частку втрат від кіберінцидентів (0,5%). Оскільки зловмисники у кіберпросторі найчастіше використовують для негативного впливу технологічні канали доступу, даний регіон є умовно захищеним через низький ступінь автоматизації життя, виробництва та якісного стійкого з'єднання з мережею «Інтернет».

Останню, сьому позицію за значенням Індексу, посідає регіон Близький Схід і Північна Африка, оскільки частка покриття населення мобільним зв'язком регіону низька (6%), аналогічною є й частка втрат від кіберінцидентів (0,8%). Даний регіон досі мало насичений цифровими технологіями й характеризується низькою доступністю до мережі «Інтернет», відповідно актуальність страхування кібер-ризиків низька.

На основі отриманих результатів сформуємо графічне зображення географічного розподілу Індексу необхідності розвитку страхування кібер-ризиків у світі (рис. 2.13)

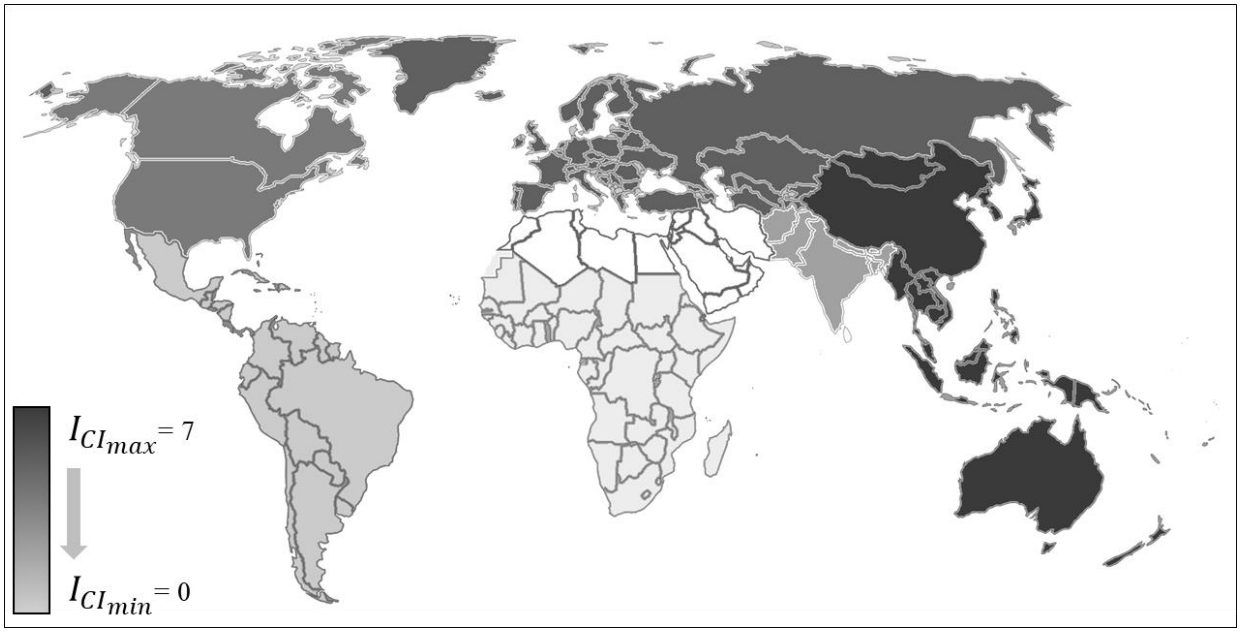


Рисунок 2.13. Регіональний розподіл Індексу необхідності розвитку страхування кібер-ризиків у 2022 р.

Джерело: розробка автора

Відповідно до розрахованого Індексу, запровадження та використання страхування кібер-ризиків як засобу досягнення Цілей сталого розвитку, має відповідати унікальним особливостям та потребам кожного окремого регіону, що відображає різноманітність викликів і можливостей, притаманних різним частинам світу.

Як було визначено, глобальний ринок страхування кібер-ризиків щороку розвивається, збільшуючи обсяги зібраних валових страховий премій. Експерти вважають, що до 2027 року даний сегмент страхового ринку сягатиме від 26,3 млрд дол. до 32,8 млрд дол. [122; 125; 126; 133].

Для визначення власного прогнозного значення використаємо метод експоненційного згладжування, що допомагає виявити зміни в тенденціях досліджуваного показника та визначає точніші розрахункові дані на основі наявної фактичної інформації (рис. 2.14).

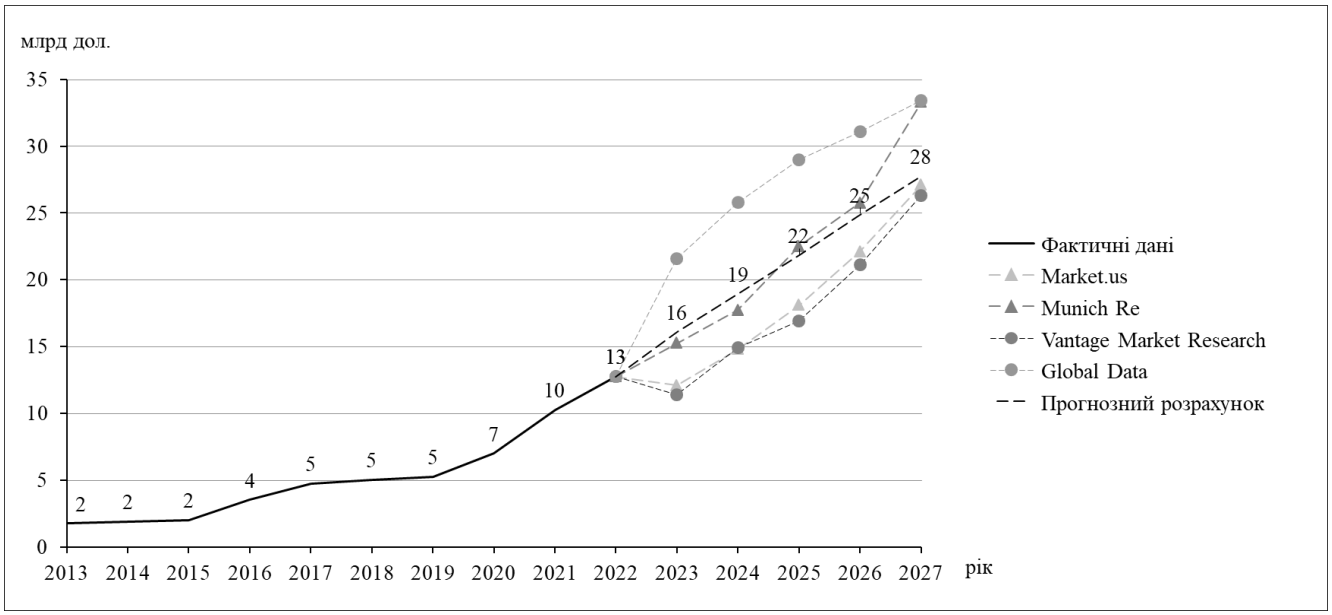


Рисунок 2.14. Прогнозні значення глобальних валових премій страхування кібер-ризиків у 2023–2027 рр.

Джерело: складено та доповнено автором на основі [122; 125; 126; 133]

Відповідно до отриманих результатів прогнозування, за 5 років глобальні валові премії страхування кібер-ризиків зростуть більш ніж удвічі (+117% у 2027р. порівняно з 2022 р.). Утім, міжнародна група Vantage Market Research оцінює приріст ринку страхування кібер-ризиків дещо консервативніше (+106% у

2027 р. порівняно з 2022 р.), аналогічно з агенцією Market.us (+112% у 2027р. порівняно з 2022 р.).

Отримані прогнозні дані протягом 2023–2026 рр. були найбільш наближені до оцінки Munich Re. Однак, на думку спеціалістів Munich Re, інвестиції в страхування кібер-ризиків значно зростуть після 2026 року та досягнуть 33,3 млрд дол., тобто +161% у 2027 р. порівняно з 2022 р.

Також оптимістичний проноз зростання обсягу валових премій страхування кібер-ризиків протягом усього досліджуваного періоду надає організація Global Data з очікуваним приростом у +162% у 2027 р. порівняно з 2022 р.

Доцільно зауважити, що оцінки перелічених експертів щодо прогнозу змін на ринку страхування кібер-ризиків можуть відрізнятися залежно від таких факторів:

- відмінності в оцінках впливу технологічних факторів на розвиток людства, включаючи різні прогнози швидкості масового запровадження інноваційних технологій;
- різні особливості локального регулювання сфери кібербезпеки та страхування, що асимілює прогнози локального розвитку в усіх частинах світу;
- різниця у підходах до визначення перспектив трансформації діяльності зловмисників, тобто зміщення фокусу їхньої діяльності з традиційних сфер у кіберпростір;
- протилежне бачення майбутнього соціального і культурного розвитку, тобто одні експерти вважають, що майбутня діяльність людства буде повністю переміщена в кіберпростір, коли інші вбачають тренд відмови від цифровізації в побутовому житті людини.

Таким чином, використання продуктів страхування кібер-ризиків стане дієвим інструментом для досягнення глобальних Цілей сталого розвитку. Наявні тенденції на світовому страховому ринку свідчать про те, що в період 2023–2027 рр. років очікується активний розвиток страхування кібер-ризиків, що позначиться на зростанні обсягу глобальних валових премій вказаного виду страхування більш ніж удвічі. Відповідно до запропонованого Індексу

необхідності розвитку страхування кібер-ризиків, в регіональному розрізі перспектива розвитку страхування кібер-ризиків різниться: найвищий потенціал наявний у країн Східної Азії й Тихоокеанських країн, Європи і Центральної Азії та Північної Америки; середній потенціал – у країн Південної Азії, Латинської Америки і Карибського басейну; найнижчий – у країн Субсахарської Африки, Близького Сходу і Північної Африки.

2.3. Діагностування стану розвитку страхування кібер-ризиків в Україні

У глобальному вимірі страхування кібер-ризиків демонструє постійний приріст протягом останніх десяти років. При цьому збільшуються не лише доступні види страхового покриття, але й напрямки нейтралізації наслідків кіберінцидентів. Проте на українському страховому ринку пропозиції страхових продуктів даного виду є доволі обмеженими.

Станом на 2023 рік, лише дві компанії на страховому ринку України пропонують послуги страхування кібер-ризиків: Українська акціонерна страхова компанія (АСКА) та Українська пожежно-страхова компанія (UPSK) [35; 86]. Ризики вказаного типу страховики пропонують для юридичних осіб, що використовують, зберігають чи передають конфіденційні дані, користуються електронними інформаційними базами, співпрацюють з іноземними компаніями на аутсорсі або виконують зобов’язання за договорами замовлення ІТ-послуг.

З огляду на особливості діяльності потенційних страхувальників, українські страховики виділяють чотири групи ризиків, що можуть бути застраховані, а саме: обмежений доступ до інформації, яку використовував страхувальник; перерва у виробництві через настання кіберінциденту; витік, викрадення чи знищення (повне або часткове) інформаційної бази страхувальника; порушення конфіденційності даних страхувальника або третіх осіб.

На основі даних груп кібер-ризиків проведено компаративний аналіз страхового покриття у страхових компаній АСКА та UPSK (Таблиця 2.11).

Таблиця 2.11

Компаративний аналіз страхового покриття українських страхових компаній АСКА та UPSK

Група покриття	Характеристика покриття	АСКА	UPSK
Ведення розслідування	Витрати на проведення розслідування щодо здійсненого страхувальником порушення законодавства, порушення безпеки даних чи їх конфіденційності		
	Витрати на здійснення експертизи щодо причин настання страхового випадку		
	Витрати на залучення фахівців у сфері кібербезпеки відразу після настання кіберінциденту		
Порушення цілісності або конфіден-ційності даних	Збитки через знищення (повне або часткове) чи реконструкцію інформаційної бази		
	Збитки через порушення конфіденційності даних страхувальника (критична бізнесінформація)		
	Збитки через порушення конфіденційності даних третіх осіб (чутлива інформація)		
	Витрати на відновлення даних чи інформаційної бази		
	Витрати на відшкодування збитків вимагачам за дешифрування даних страхувальника		
Превентивні заходи	Витрати на розробку систем моніторингу кіберзагроз		
	Витрати на залучення спеціалістів у сфері кібер-безпеки для розробки стратегії покращення стану страхувальника		
Помилкова інформація	Витрати на залагодження ситуацій щодо неналежного використання даних (PR стратегії)		
	Витрати на залагодження ситуацій щодо некоректно опублікованої інформації (PR стратегії)		
Перерва у виробництві	Збитки в межах суми недоотриманого доходу за час простою виробництва		
	Збитки в межах суми недоотриманого доходу за час недоступності IT-систем, що залучені в процес продажу продуктів страхувальника		
Соціальна інженерія	Втрати через фішинг		
	Втрати через картинг		
Інфраструктура та програмне забезпечення	Витрати на відновлення програмного забезпечення		
	Витрати на відновлення фізичного обладнання		
Цільові атаки	Втрати через DDoS-атаки		
	Втрати через ненавмисні внутрішні атаки		
	Втрати через навмисні внутрішні атаки		

Джерело: складено автором на основі [35; 86]

Відповідно, для українського бізнесу сьогодні доступне страхове покриття основних кібер-ризиків сучасності, включаючи витрати на проведення

превентивних заходів щодо запобігання кіберінцидентів та нейтралізації наслідків у разі їх реалізації.

Проте новою актуальною загрозою є кібервійни, жертвою яких все частіше стає цивільна інфраструктура. Зрозуміло, що ризики такого типу можуть бути катастрофічними для страховика, тому варто розвивати ефективне партнерство перестрахування та співстрахування як у межах України, так і за кордоном.

У разі настання страхового випадку, що підпадає під умови договору страхування, компанія UPSK пропонує такий порядок дій страхувальника для отримання страхового відшкодування [191]:

1. Повідомлення страховика про настання страхової події.
2. Повідомлення кіберполіції про настання страхової події.
3. Збереження, за можливості, максимально недоторканними умови, в яких відбувся страховий випадок (незмінні паролі доступу, конфігурація IT-систем, налаштування IT-інфраструктури в цілому) за умови, якщо це не перешкоджає стабілізації кризової ситуації.
4. Подання заяви на отримання страхового відшкодування.
5. Надання повної інформації про настання страхового випадку в рамках взаємодії з партнерами страховиків.
6. Отримання відшкодування.

Страховик натомість здійснює наступні заходи для надання страхувальнику страхового відшкодування [35]:

1. Фіксація звернення страхувальника щодо настання страхового випадку.
2. Звернення до партнерів, які є експертами у сфері кібербезпеки, з метою отримання кваліфікаційного висновку щодо причин настання страхового випадку.
3. Підтвердження факту, що обставини кіберінциденту підпадають під умови договору страхування, який є підставою для здійснення страхової виплати.
4. Здійснення розрахунку завданих втрат (із можливим залученням експертів у сфері кібербезпеки за необхідності).

5. Виплата страхового відшкодування страхувальнику.

Відповідно до описаних кроків порядку здійснення страхового відшкодування, усі суб'єкти страхування кібер-ризиків виконують свої функції на кожному етапі, що свідчить про якісний механізм роботи зі страховими випадками у кіберпросторі вітчизняних страховиків (рис. 2.15).

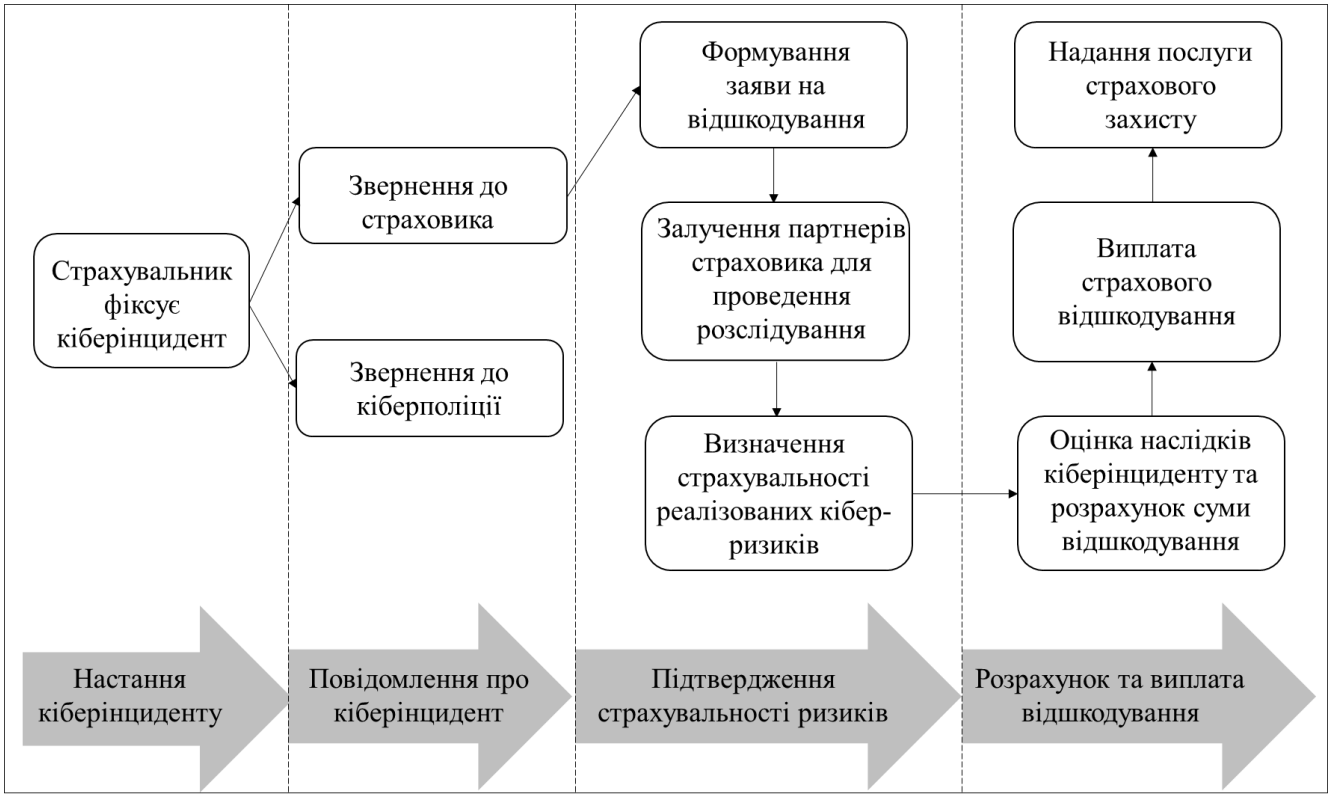


Рисунок 2.15. Механізм взаємодії вітчизняних суб'єктів страхування кібер-ризиків при настанні страхового випадку

Джерело: складено та доповнено автором на основі [35]

Незважаючи на наявність низки кіберзагроз в Україні та доступність продуктів страхування кібер-ризиків, частка страхових компаній, що надають вказані послуги, доволі низька. Станом на кінець третього кварталу 2023 р. ця частка становила 1,6%, що на 0,9 в.п. більше, ніж у 2018р. Однак драйвером збільшення частки стало не розширення кількості компаній, що пропонують страхування кібер-ризиків, а зменшення кількості страховиків через очищення страхового ринку України від недобросовісних страховиків [195, с. 14] (Таблиця 2.12).

Таблиця 2.12

Динаміка страхових компаній України у 2018–2023 рр.

Показник	2018	2019	2020	2021	2022	2023 (9 міс.)
Страхові компанії life, шт.	30	23	20	13	12	12
Страхові компанії non-life, шт.	251	210	190	142	116	111
Всього	281	233	210	155	128	123
Страхові компанії, що надають послуги страхування кібер-ризиків, шт.	2	2	2	2	2	2
Частка від загальної кількості страхових компаній, %	0.7%	0.9%	1.0%	1.3%	1.6%	1.6%
Частка від кількості страхових компаній non-life, %	0.8%	1.0%	1.1%	1.4%	1.7%	1.8%

Джерело: складено автором на основі [35; 52; 80]

Оскільки страхування кібер-ризиків є відносно новим інструментом підвищення кібербезпеки, попит на українському ринку незначний. Перепоною для його розвитку є нерозуміння потенційними страхувальниками можливих втрат від настання кіберінциденту, які, за підсумками проведеного моделювання, впливають на збільшення попиту на дані послуги.

З початком повномасштабного вторгнення Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України регулярно здійснював моніторинг потенційних загроз у кіберпросторі (Таблиця 2.13).

Таблиця 2.13

Статистика моніторингу кіберзагроз України у 2021–2022 рр.

Показник	2022			2023		
	Фактичне значення, шт.	Частка від опрацьованих подій, %	Частка від попереднього рівня, %	Фактичне значення, шт.	Частка від опрацьованих подій, %	Частка від попереднього рівня, %
Опрацьовані події, млрд	58	100%	100%	18	100%	100%
Виявлені підозрілі події, млн	181	0.312069%	0.312%	133	0.738889%	0.739%
Опрацьовано критичних подій, тис.	179	0.000309%	0.099%	148	0.000822%	0.111%
Зареєстровано кібер-інцидентів, шт.	415	0.000001%	0.232%	1105	0.000006%	0.747%

Джерело: розрахунки автора на основі [76; 77]

Станом на 2022 р. було зафіксовано 415 кіберінцидентів, що на 184% більше порівняно з 2021 р. Однак у 2023 р. кількість інцидентів продовжувала зростали та сягнула 1105, що на 166% більше порівняно із зафіксованими інцидентами у 2021 р.

Проте процесу реєстрації кіберінциденту передують процедури опрацювання, ідентифікації та оцінки загроз. Так, із 18 млрд опрацьованих загроз у 2023 році, лише 0,000006% переросли в кіберінциденти.

Як бачимо, ступінь загроз у кіберпросторі зріс у 2023 р., оскільки частка опрацьованих подій, що стали кіберінцидентами, збільшилась порівняно з 2022 р. Однак варто враховувати, що в 2022 році кількість опрацьованих вхідних загроз зросла через активний вплив Російської Федерації на українську ІТ-інфраструктуру перед початком повномасштабного вторгнення.

Основними джерелами кіберінцидентів в українському кіберпросторі у 2023 р. були:

- шкідливе програмне забезпечення (найбільша частка як у 2022 р., так і в 2023 р.);
- порушення конфіденційності, шпигунство, викривлення чи викрадення інформації зловмисниками;
- зловмисне втручання в роботу ІТ-систем;
- вимушена перерва діяльності через загрози доступності ІТ-систем;
- порушення характеристик інформації;
- відомі вразливості ІТ-систем.

За даними Microsoft, в 2022 р. основними сферами, що не стосуються військової діяльності, на які було здійснено найбільше кібератак хакерами, що контролюються Російською Федерацією, були [112]:

1. Урядові організації (19 кібератак).
2. ІТ-організації (7 кібератак).
3. Організації енергетичного сектору (4 кібератаки).
4. Медіа та ЗМІ (4 кібератаки).
5. Телекомунікації (3 кібератаки).

6. Організації, що обслуговують ядерні об’єкти (3 кібератаки).

7. Роздрібна торгівля (2 кібератаки).

8. Організації, що встановлюють та обслуговують підключення до мережі «Інтернет» (2 кібератаки).

Оскільки обсяг кіберзагроз в Україні продовжує зростати у всіх секторах економіки, варто розглянути можливість використання страхування кібер-ризиків як інструмента, що мінімізує ймовірність настання кіберінциденту і надає необхідний захист у разі його настання.

Для визначення потенціалу розвитку страхування кібер-ризиків в Україні розглянемо оцінні значення обсягу втрат від зафіксованих кіберінцидентів.

Одним із підходів для визначення обсягу втрат від кіберінцидентів є визначення кількості зафіксованих кіберінцидентів та їх середньої вартості, оскільки централізований збір агрегованого показника не проводиться уповноваженими органами (Таблиця 2.14).

Таблиця 2.14

Оцінні дані показників втрат від кіберінцидентів України у 2021–2022 рр.

Показник	2021	2022
Кількість кіберінцидентів, шт.	147	415
Середні збитки від кіберінцидентів, млн дол.	4.24	4.35
Втрати від кіберінцидентів, млн дол.	623.28	1805.25
ВВП, млн дол.	199,766	160,503
Частка втрат від кіберінцидентів у ВВП, %	0.3%	1.1%

Джерело: розрахунки автора на основі [76; 77; 157; 209]

Використовуючи дані зі звіту Державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України [76; 77], визначаємо кількість зафіксованих кіберінцидентів у 2021–2022 рр. (оскільки централізований збір верифікованої інформації проводиться з 2021 р.).

Середній обсяг втрат від кіберінциденту приймаємо на рівні зваженого глобального значення, що включає в себе фактично завдані втрати, вплив на економіку через перерву у виробництві, репутаційні втрати, витрати на проведення розслідування і консультацій та надання відшкодувань за порушення конфіденційності даних [209].

Обчислений обсяг втрат від кіберінцидентів в Україні у 2022 році становив 1,8 млрд дол., що на 189,6% більше, ніж у 2021р.

Якщо оцінювати вплив на економічні показники України, то зафіксовані кіберінциденти негативно позначились на ВВП – частка втрат від кіберінцидентів у ВВП в 2022 р. становила 1,1%, що на 0,8 в.п. більше порівняно з 2021 р. Зрозуміло, що на ВВП у 2022 р. негативно вплинуло повномасштабне вторгнення, тому база для вирахування частки впала. Однак, якщо оцінити вплив кіберінцидентів 2022 р. на ВВП України 2021 р., то частка втрат від кіберінцидентів у ВВП становитиме 0,9%, що на 0,6 в.п. більше, ніж попередній органічний рівень.

Збільшення кіберінцидентів призводить до блокування важливих сервісів, критично необхідних населенню України та українському бізнесу в умовах війни. Існує ризик зупинки надання адміністративних, фінансових чи медичних послуг, відсутності покриття чи доступності мобільного зв'язку, блокування послуг мережі «Інтернет», відсутності сповіщення про небезпеку, зупинки транспорту та подачі електроенергії.

Збереження цілісності наявної ІТ-інфраструктури є пріоритетним завданням України для забезпечення стабільності надання критично важливих послуг. Проте в умовах гібридної війни ризики кіберпростору стали особливо непередбачуваними та загрозливими, оскільки підривають безпеку не лише окремих організацій, а й держави в цілому. Зловмисні дії, що їх продовжують здійснювати хакерські угруповання, контрольовані Російською Федерацією, дестабілізують ситуацію в Україні через поширення дезінформації, зупинку діяльності критичної інфраструктури та блокування надання важливих сервісів.

Однак така тактика не є новою, оскільки підривати кібербезпеку України агресор почав задовго до повномасштабного вторгнення. Якщо розглядати хронологію здійснених кібератак, то початок активних дій у кіберпросторі почався ще в 2014 р. Відтоді російськими хакерами неодноразового було атаковано ІТ-інфраструктуру українського уряду, бізнесу та цивільних об'єктів.

Відповідно, необхідність розвитку страхування кібер-ризиків в Україні має високий пріоритет задля підтримки кібербезпеки в умовах нестабільності.

Оскільки частка страхових компаній, що надають послуги страхування кібер-ризиків в Україні, менше 2%, необхідно розглянути потенціал вітчизняних страховиків щодо запровадження даного виду страхування.

Базою для проведення оцінки є показники діяльності страховиків за дев'ять місяців 2022–2023 рр., оскільки такий період відображає стан страхової компанії після початку повномасштабного вторгнення. Забезпечення страховиком покращення результативних показників страхової діяльності в процесі адаптації до нових умов ведення бізнесу після шокового стану є підтвердженням наявності у нього потенціалу не лише до тимчасової стабілізації у кризових ситуаціях, а й до зростання в майбутньому.

Закордонна практика свідчить, що покриття кібер-ризиків сформувалось через трансформацію фінансових та майнових ризиків у кіберпросторі. Відповідно обираємо страховиків, які були лідерами українського страхового ринку за валовими преміями зі страхування фінансових та майнових ризиків в обох періодах.

Під час здійснення оцінки потенціалу доцільно використовувати індексні показники. Тож для визначення можливостей вітчизняних страховиків у запровадженні страхування кібер-ризиків використовуємо такі значення, що будуть проранговані за рейтингом у групі:

- приріст валових страхових премій рік до року. Даний показник вказує на позиції страховика на ринку та рівень попиту на страхові продукти компанії, відповідно, відображає шанси страховика на успішний запуск нового продукту через наявну клієнтську базу;
- обсяг активів страховика. Даний показник вказує на фінансову стабільність компанії та здатність страховика виконувати свої зобов'язання, тому при настанні страхових випадків через кіберінцидент здатний мобілізувати необхідну суму коштів для надання відшкодування;

- загальний рівень виплат. Даний показник відображає ефективність дій страховика на запобігання настанню страхових випадків та його політику щодо відшкодування реально завданих збитків;

- частка валових премій страхування фінансових ризиків у загальних валових преміях. Даний показник вказує на наявний обсяг попиту на продукти страховика у сфері фінансових ризиків, що можуть бути розширені через включення покриття фінансових втрат, спричинених кіберінцидентами;

- частка валових премій страхування майна у загальних валових преміях. Даний показник вказує на наявний обсяг попиту на продукти страховика у сфері майнових ризиків, частина яких під впливом цифровізації трансформується у кібер-ризики.

Для визначення рангової оцінки страхових компаній за кожним із показників використаємо формулу:

$$R_{X_i} = \frac{X_i}{X_{max}}, \tag{2.5}$$

де R_{X_i} – рангова оцінка страховика за показником, що аналізується;

X_i – значення показника, що аналізується, для обраного страховика;

X_{max} – максимальне значення показника, що аналізується, в групі.

Значення рангових показників для обсягу активів страховика, загального рівня виплат, частки валових премій страхування фінансових ризиків у загальних валових преміях та частки валових премій страхування майна у загальних валових преміях можуть варіюватись від 0 до 1. Збільшення значення показника свідчить про кращу позицію страховика у групі.

Проте значення рангових показників для приросту валових страхових премій рік до року можуть бути менше 0 у разі, якщо приріст був від'ємним, та максимум аналогічний до вищевказаних показників, тобто до 1. Зі збільшенням значення показника покращується позиція страховика у групі.

Розраховані за описаним підходом дані, необхідні для оцінки потенціалу вітчизняних страховиків щодо запровадження страхування кібер-ризиків за 2022 р. та 2023 р., відображені у Таблиці 2.15.

Таблиця 2.15

Рангова оцінка страхових компаній за підсумками діяльності за 9 місяців 2022 р. та 2023 р.

Рангове значення / Страхова компанія	Приріст валових страхових премій рік до року (X_1)	Обсяг активів (X_2)	Загальний рівень виплат (X_3)	Частка валових премій страхування фінансових ризиків у загальних валових преміях (X_4)	Частка валових премій страхування майна у загальних валових преміях (X_5)
2022 р.					
ARX	(0,4551)	1,0000	0,7777	0,1335	0,8349
PZU «УКРАЇНА»	(0,6033)	0,5410	0,9076	0,0624	0,2187
«УНІВЕРСАЛЬНА»	0,1399	0,3684	0,4990	0,1276	0,2992
«АРСЕНАЛ СТРАХУВАННЯ»	(0,6096)	0,4522	0,9111	0,0009	0,1777
БРОКБІЗНЕС	0,0063	0,0643	0,5059	0,0183	0,2266
ВУСО	(0,0313)	0,2251	0,6760	0,5716	0,2831
«ГАРДІАН»	0,4843	0,1427	0,3489	0,0005	0,1225
«ЕТАЛОН»	(0,3800)	0,0638	0,7918	1,0000	1,0000
«КРАЇНА»	(0,3946)	0,0790	0,9280	0,0038	0,0159
«ОБЕРІГ»	0,0501	0,0598	0,8000	0,0006	0,0355
«ПЕРША»	(0,1399)	0,1882	0,7930	0,0919	0,1019
«САЛАМАНДРА»	1,0000	0,0409	0,5332	0,2916	0,1137
ТАС СГ	(0,1002)	0,6171	0,7708	0,1564	0,0959
УНІКА	(0,3737)	0,7062	1,0000	0,3111	0,2291
2023 р.					
ARX	0,6364	1,0000	0,7535	0,3898	1,0000
PZU «УКРАЇНА»	0,6515	0,4775	0,7760	0,0002	0,1338
«УНІВЕРСАЛЬНА»	0,8475	0,3780	0,6807	-	0,3286
«АРСЕНАЛ СТРАХУВАННЯ»	0,6570	0,4368	0,9058	0,0002	0,2302
БРОКБІЗНЕС	0,7404	0,0661	0,6582	0,0064	0,2662
ВУСО	1,0000	0,3164	0,7133	0,7982	0,3706
«ГАРДІАН»	0,9392	0,1826	0,5865	0,0011	0,0544
«ЕТАЛОН»	0,5579	0,0645	0,7419	1,0000	0,4646
«КРАЇНА»	(0,4221)	0,0607	1,0000	0,0015	0,0352
«ОБЕРІГ»	0,4766	0,0510	0,9676	0,0006	0,0242
«ПЕРША»	0,7394	0,1699	0,6939	0,1011	0,0954
«САЛАМАНДРА»	0,1051	0,0293	0,7463	0,3206	0,0908
ТАС СГ	0,7415	0,6776	0,7722	0,1126	0,0892
УНІКА	0,3684	0,8354	0,8828	0,2721	0,2747

Джерело: розрахунки автора на основі [52; 80]

Використовуючи отримані рангові оцінки страхових компаній за показниками їхньої діяльності, сформуємо формулу Індексу, що буде враховувати потенціал запровадження страхування кібер-ризиків вітчизняних страховиків:

$$I_i = X_1 + X_2 + X_3 + X_4 + X_5, \quad (2.6)$$

де I_i – Індекс потенціалу запровадження страхування кібер-ризиків страховика;

X_1 – рангове значення приросту валових страхових премій рік до року страховика;

X_2 – рангове значення обсягу активів страховика;

X_3 – рангове значення загального рівня виплат страховика;

X_4 – рангове значення частки валових премій страхування фінансових ризиків у загальних валових преміях страховика;

X_5 – рангове значення частки валових премій страхування майна у загальних валових преміях страховика.

Усі рангові значення показників страхової діяльності вважаємо рівнозначними, оскільки кожне відображає важливі аспекти діяльності страхової компанії, необхідні для визначення потенціалу запровадження страхування кібер-ризиків. Відповідно використання вагових коефіцієнтів для рангових значень при обчисленні Індексу потенціалу запровадження страхування кібер-ризиків страховика є недоцільним.

Оскільки верхня межа рангових значень показників страхової діяльності має значення 1, відповідно максимальне значення Індексу потенціалу запровадження страхування кібер-ризиків має значення 5. Зі збільшенням значення Індексу потенціал запровадження страхування кібер-ризиків зростає.

Додатково варто визначити приріст Індексу рік до року, оскільки у 2023 р. страховий ринок України адаптувався до нових викликів, що виникли після початку повномасштабного вторгнення, та реалізував нові стратегії розвитку. Аналіз приросту Індексу демонструє, наскільки ефективними були дії страховика та чи змінилась його рангова позиція в умовах нової реальності.

Отримані значення Індексу потенціалу запровадження страхування кібер-ризиків вітчизняних страховиків відображені у Таблиці 2.16.

Таблиця 2.16

Індекс потенціалу запровадження страхування кібер-ризиків вітчизняних страховиків у 2022 р. та 2023 р.

Страхова компанія	2022	2023	Приріст
ARX	2,2910	3,7797	1,49
PZU «УКРАЇНА»	1,1263	2,0388	0,91
«УНІВЕРСАЛЬНА»	1,4340	2,2348	0,80
«АРСЕНАЛ СТРАХУВАННЯ»	0,9324	2,2301	1,30
БРОКБІЗНЕС	0,8213	1,7373	0,92
ВУСО	1,7245	3,1985	1,47
«ГАРДІАН»	1,0990	1,7637	0,66
«ЕТАЛОН»	2,4756	2,8289	0,35
«КРАЇНА»	0,6321	0,6754	0,04
«ОБЕРІГ»	0,9461	1,5200	0,57
«ПЕРША»	1,0350	1,7998	0,76
«САЛАМАНДРА»	1,9793	1,2921	(0,69)
ТАС СГ	1,5401	2,3931	0,85
УНІКА	1,8727	2,6335	0,76

Джерело: розрахунки автора на основі [52; 80]

Відповідно до отриманих результатів, найвищий потенціал у 2023 р. має страхова компанія ARX зі значенням 3,78 та позитивним приростом Індексу на 1,49. Основними драйверами росту є нарощення загальних валових премій та валових премій страхування майна.

Другу позицію у 2023 р. займає страхова компанія ВУСО зі значенням 3,20 та позитивним приростом Індексу на 1,47 завдяки покращенню приросту валових премій, рівня виплат та валових премій страхування фінансових ризиків.

На третій позиції у 2023 р. – страхова компанія «ЕТАЛОН» зі значенням 2,83 та позитивним приростом Індексу на 0,35. Основними драйверами росту є підвищення темпів приросту загальних валових премій та рівня виплат.

Четверту позицію у 2023 р. займає страхова компанія УНІКА зі значенням 2,63 та позитивним приростом Індексу на 0,76 завдяки збільшенню обсягу активів та рівня виплат.

На п’ятій позиції у 2023 р. перебуває страхова компанія ТАС СГ зі значенням 2,40 та позитивним приростом Індексу на 0,85. Основними драйверами росту є покращення обсягу активів та рівня виплат.

На шостій-восьмій позиціях у 2023 р. містяться страхові компаній PZU «УКРАЇНА», «УНІВЕРСАЛЬНА» та «АРСЕНАЛ СТРАХУВАННЯ» зі значеннями від 2,04 до 2,25. Незважаючи на те, що Індекс мав позитивний приріст, рангове значення за ключовими показниками діяльності є середнім.

Дев’яту-одинадцяту позиції в 2023 р. займають страхові компанії «ПЕРША», БРОКБІЗНЕС та «ГАРДІАН» зі значеннями від 1,74 до 1,80. Рангові значення за ключовими показниками діяльності вказаних страховиків є нижчі середніх, а Індекс демонстрував помірний темп приросту.

Дванадцяту позицію в 2023 р. посідає страхова компанія «ОБЕРІГ» зі значенням 1,52 та позитивним приростом Індексу на 0,57. Низьке значення Індексу пояснюється незначною часткою валових премій страхування майна та фінансових ризиків.

Тринадцята позиція 2023 року – в страхової компанії «САЛАМАНДРА» зі значенням 1,30 та єдиним негативним значенням падіння Індексу на -0,69 через зменшення темпів приросту валових премій та незначний обсяг активів.

На останній позиції у 2023 р. – страхова компанія «КРАЇНА» зі значенням 0,68 та позитивним приростом Індексу на 0,04. Низьке значення Індексу пояснюється падінням темпів росту валових премій та незначним обсягом активів і валових премій страхування майна та фінансових ризиків.

На основі проведеної кластеризації Індексу потенціалу запровадження страхування кібер-ризиків вітчизняних страховиків можемо сформувати чотири групи страхових компаній, можливість запровадження страхування кібер-ризиків якими перебуває в умовно однакових межах:

- група з оптимальним потенціалом, до якої входять ARX, ВУСО, «ЕТАЛОН», УНІКА і ТАС СГ;
- група з високим потенціалом, до якої входять PZU «УКРАЇНА», «УНІВЕРСАЛЬНА» та «АРСЕНАЛ СТРАХУВАННЯ»;

- група з середнім потенціалом, до якої входять «ПЕРША», БРОКБІЗНЕС та «ГАРДІАН»;

- група з низьким потенціалом, до якої входять «ОБЕРІГ», «САЛАМАНДРА» та «КРАЇНА».

Схематично позиції страхових компаній за отриманим у 2023 р. Індексом можна зобразити за допомогою бульбашкової діаграми на рис. 2.16, де величина бульбашки означає актуальне значення Індексу, вертикальна позиція означає значення Індексу у 2022 р., а горизонтальна позиція означає приріст Індексу у 2023 р. порівняно з 2022 р.

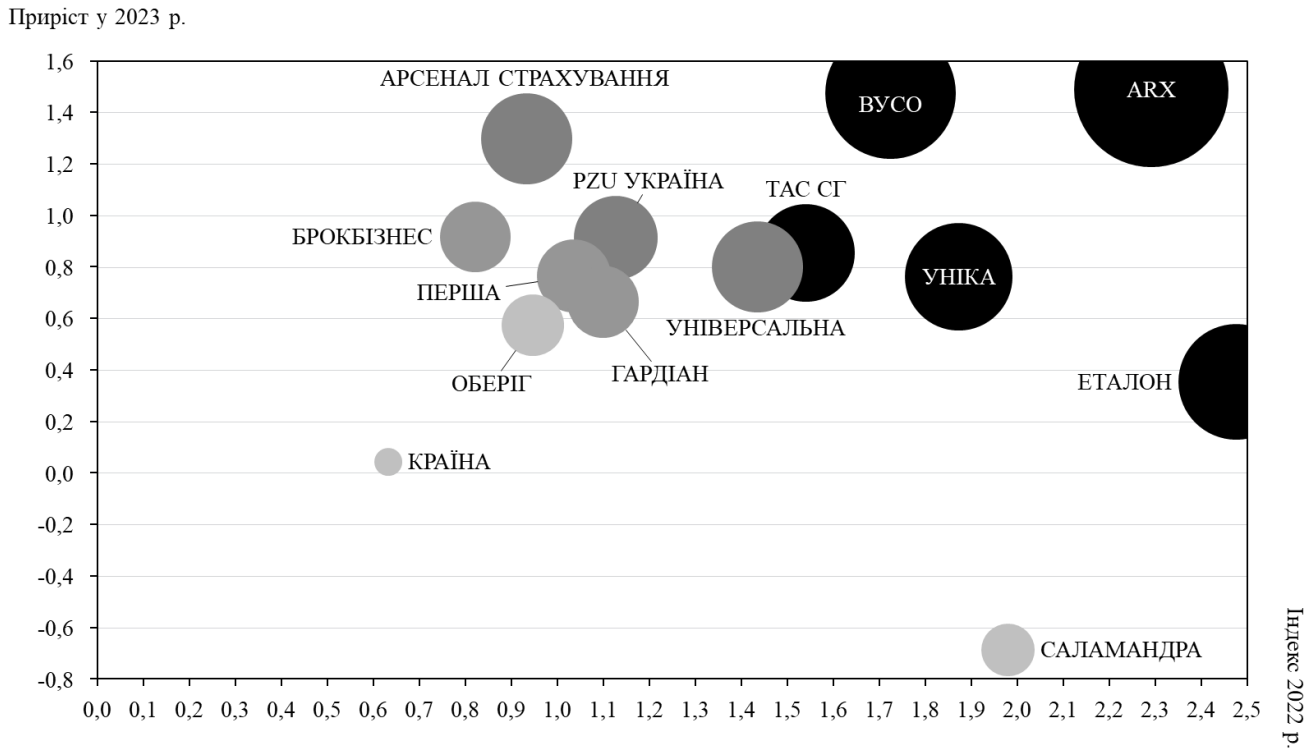


Рисунок 2.16. Діаграма зміни Індексу потенціалу запровадження страхування кібер-ризиків вітчизняними страховиками

Джерело: розрахунки автора на основі [52; 80]

Отримані результати свідчать про наявність страхових компаній з високим потенціалом для запровадження страхування кібер-ризиків, що також матиме позитивний вплив на страховий ринок. Збільшення доступних продуктів страхування стимулюватиме розширення клієнтської бази, забезпечуючи конкурентоздатне середовище та відповідно здорову конкуренцію на ринку.

ВИСНОВКИ ДО РОЗДІЛУ 2

Отримані результати дослідження сучасних тенденцій страхування кібер-ризиків у світі та Україні є основою для наступних висновків:

1. На основі економетричного моделювання виявлено, що драйверами зростання обсягу глобальних валових премій страхування кібер-ризиків, які є індикатором розвитку цього ринку, є збільшення обсягу покриття населення мобільним зв'язком та суми втрат від кіберінцидентів. Отримані результати були використані для визначення етапів періодизації становлення та розвитку глобального ринку страхування кібер-ризиків: підготовчий етап (1950–1989 рр.), протягом якого спостерігався активний розвиток та поширення цифрових технологій, покриття мережею «Інтернет» та поширення використання цифрових платіжних засобів; етап зародження (1990–2005 рр.), під час якого вперше були зафіксовані випадки включення кібер-ризиків до покриття у страхових угодах, оскільки протягом даного періоду доступність персональних комп'ютерів зросла, однак рівень цифрової грамотності був низький; етап створення самостійних продуктів страхування кібер-ризиків (2006–2012 рр.), протягом якого відбулось виділення продукту страхування кібер-ризиків в окремий самостійний продукт, оскільки загрози кіберпростору розширились через активний розвиток соціальних мереж та онлайн-платформ; етап зростання обізнаності про кібер-ризики (2013–2015 рр.), коли було визначено особливість загроз кіберпростору на міжнародному рівні через значну цифровізацію усіх сфер життя та діяльності людини; етап популяризації (2016–2019 рр.), що став періодом активного просування послуг страхування кібер-ризиків як одного з інструментів управління сучасними ризиками; сучасний етап активного розвитку (2020 р. – сьогодення), під час якого зростає частка автоматизованих та оцифрованих сфер діяльності через залучення у всі процеси широкого спектру інноваційних технологій, які замінюють участь людини в них.

2. Обґрунтовано, що страхування кібер-ризиків є важливим інструментом для досягнення глобальних Цілей сталого розвитку. Ефективними

інструментами страхування кібер-ризиків, які необхідно залучати для досягнення мети Дев'ятої цілі сталого розвитку, є: створення механізму моніторингу, управління і нейтралізації відповідних ризиків страхувальника та покращення рівня їх цифрової грамотності. Позитивний ефект на виконання Шістнадцятої цілі сталого розвитку мають елементи страхування кібер-ризиків, оскільки за відповідною страховою угодою страхувальник зобов'язується забезпечувати прозору звітність своєї діяльності, що зменшує рівень корупції, шахрайства та відмивання коштів. Успішність реалізації Сімнадцятої цілі сталого розвитку підсилюють міжнародні партнерські зв'язки страховиків зі спеціалістами у сфері кібербезпеки, що забезпечує обмін важливою інформацією та корисними технологіями між різними регіонами задля підтримання глобального стійкого зростання.

3. Розроблено регіональний Індекс необхідності розвитку страхування кібер-ризиків на основі показників, що впливають на зростання обсягу глобальних валових премій страхування кібер-ризиків, а саме, обсягу покриття населення мобільним зв'язком та суми втрат від кіберінцидентів для визначення доцільності запровадження і вдосконалення вказаного виду страхування для регіонів світу. Базуючись на запропонованому Індексі, визначено рейтинг регіонів за рівнем необхідності розвитку страхування кібер-ризиків на основі їх цифрових особливостей: перше місце посідає Східна Азія і Тихоокеанські країни, друге – Європа і Центральна Азія, третє – Північна Америка, четверте – Південна Азія, п'яте – Латинська Америка і Карибський басейн, шосте – Субсахарська Африка, сьоме – Близький Схід і Північна Африка.

4. Проаналізовано наявну пропозицію продуктів страхування кібер-ризиків на українському страховому ринку та визначено страховиків, які надають вказані послуги. Отримані результати свідчать про низький рівень розвитку даного сегменту страхового ринку в Україні, оскільки кількість страховиків, які пропонують покриття кібер-ризиків, була стабільною протягом 2018–2023 рр. та не перевищувала 2% від загальної кількості страхових компаній.

5. Запропоновано Індекс потенціалу запровадження страхування кібер-ризиків вітчизняними страховиками, що визначає спроможність страхових компаній реалізовувати вказаний вид страхування на основі результативних показників страхової діяльності: приросту валових страхових премій рік до року, обсягу активів, загального рівня виплат, частки валових премій страхування фінансових ризиків у загальних валових преміях та частки валових премій страхування майна у загальних валових преміях. Отриманні значення Індексу виявили чотири групи страхових компаній, що мають різну спроможність запровадження страхування кібер-ризиків: з оптимальним потенціалом, з високим потенціалом, з середнім потенціалом та з низьким потенціалом.

РОЗДІЛ 3. ПЕРСПЕКТИВИ РОЗВИТКУ СТРАХУВАННЯ КІБЕР-РИЗИКІВ В УКРАЇНІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ

3.1. Стимулюючі та стримуючі фактори розвитку страхування кібер-ризиків в Україні

Повномасштабне вторгнення Російської Федерації до України стало початком переоцінки місця кіберзагроз сучасності. Забезпечення належного рівня кіберзахисту держави, суспільства, національних інтересів та критичної інфраструктури закріплене в пункті 1 статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» [72]. Незважаючи на високий пріоритет кібербезпеки України в умовах гібридної війни, у 2023 р. було зафіксовано на 63% більше кіберінцидентів, ніж у 2022 р., що свідчить про значну активізацію зловмисників на кіберфронті [76]. Страхування кібер-ризиків як один з інструментів захисту від кіберзагроз варто розглядати як допоміжний елемент системи забезпечення належного рівня кібербезпеки України.

Аналізуючи перспективи розвитку страхування кібер-ризиків в Україні, варто враховувати унікальні особливості та характеристики локального кіберпростору. Використання досвіду розвитку страхування кібер-ризиків іноземних країн є частиною підготовчого процесу, проте вимагає якісного аналізу доцільності запозичення тих чи інших заходів для українського ринку.

На підготовчому етапі процесу запровадження та розвитку страхування кібер-ризиків необхідно визначити наявні стимулюючі та стримуючі фактори даного напрямку. Проте визначення базових факторів, характерних для українського страхового ринку, ускладнюється умовами війни, яка продовжує трансформовувати всі процеси життя та діяльності.

Відповідно, в умовах нової реальності розвиток нових напрямків потребує інноваційних стратегій, що враховують досвід функціонування в критичних умовах. Тому початок повномасштабного вторгнення в Україну зумовив

видозміну стимулюючих та стримуючих факторів розвитку страхування кібер-ризиків, які варто враховувати для отримання ефективного результату.

Перевагою систематизації та аналізу факторів, що стримують розвиток страхування кібер-ризиків, є не лише створення структурованого огляду інформації, але й можливість розробки конкретного плану заходів, спрямованого на подолання цих факторів. Це дає змогу визначати майбутні завдання та ресурси, необхідні для їх реалізації, і таким чином досягати поставленої мети розвитку даного виду страхування. Окремо варто відзначити, що забезпечення системи повного ефективного управління віднайденими факторами підвищує стартовий потенціал розвитку страхування кібер-ризиків ще до початку їх активного просування.

Стримуючі фактори розвитку страхування кібер-ризиків до та після початку повномасштабного вторгнення наведено на рис. 3.1.

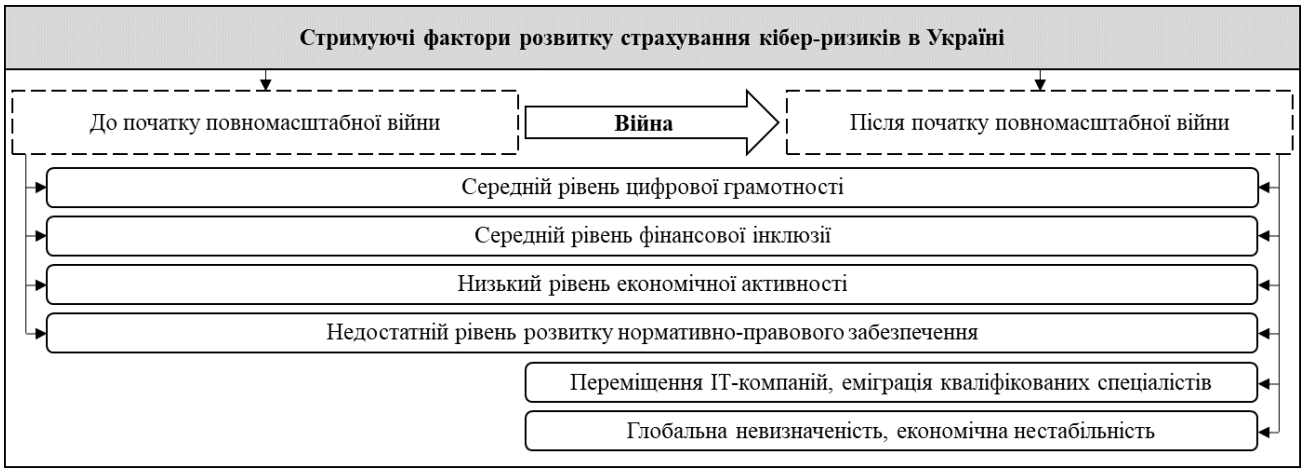


Рисунок 3.1. Стримуючі фактори розвитку страхування кібер-ризиків в Україні до та після початку повномасштабної війни з Російською Федерацією

Джерело: складено та доповнено автором на основі [50; 54]

Загалом виділяємо шість факторів, які стримують розвиток страхування кібер-ризиків в Україні:

1. Середній рівень цифрової грамотності. Наявність високого рівня цифрової грамотності населення є індикатором суспільного прогресу країни в цілому [208, с. 348]. Так, станом на кінець 2023 р. Україна була на 16-му місці з 37 (порівняння з країнами Європейського Союзу) за часткою осіб, які володіють

базовими цифровими навичками [31; 144]. Приріст цього показника в Україні становив +7.4 в.п. порівняно з 2021 р., що є третім за величиною значенням у групі (1-ше місце займає Угорщина +9.8 в.п., 2-ге місце – Чехія +9.4 в.п.). Активне зростання даного показника пояснюється наслідком ефективних дій уряду, міжнародних та приватних організацій, спрямованих на підвищення рівня цифрової грамотності (рис 3.2).

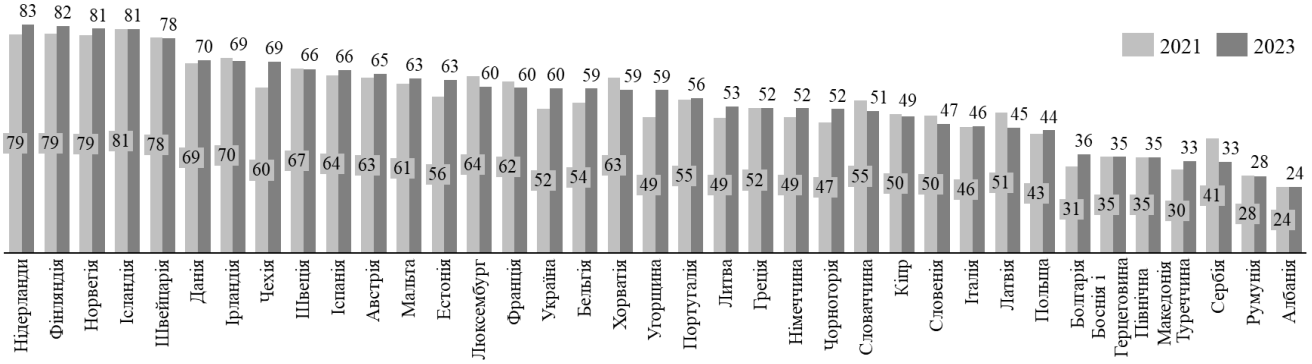


Рисунок 3.2. Частка осіб, які володіють базовими цифровими навичками у країнах ЄС та Україні в 2021 та 2023 роках

Джерело: складено автором на основі [31, 144]

Проте абсолютне значення частки осіб в Україні, які володіють базовими цифровими навичками, становило 60% 2023 року, що на -23 в.п. нижче від максимального значення у групі, проте відповідає середньому рівню розвитку цифрової грамотності країн ЄС. Такий рівень дестимулює розвиток страхування кібер-ризиків в Україні, оскільки свідчить, по-перше, про невисоку обізнаність з наявними кіберзагрозами, а тому й відсутність усвідомлення потреби в захисті від них; по-друге, про недовіру до цифрових технологій, що зменшує доступ потенційних страхувальників до інструментів, які є об'єктами страхування; по-третє, про нестачу спеціалізованих навичок, що зменшує спектр партнерів страховиків, які спеціалізуються на кібербезпеці.

2. Середній рівень фінансової інклюзії. COVID-19 прискорив темпи цифровізації економіки в усьому світі, зріс обсяг онлайн-транзакцій та цифрових фінансових сервісів [204]. При цьому спостерігалась регіональна нерівномірність розвитку фінансової інклюзії в період із 2017 р. по 2021 р. через відсутність цифрових сервісів у країнах, що розвиваються [148]. Україна перебуває в групі

країн із середнім рівнем фінансової інклюзії та має потенціал розвитку у майбутньому завдяки чинній Стратегії цифрового розвитку [74]. Окрім того, науковці зауважують, що недостатній рівень фінансової інклюзії населення призводить до низького рівня фінансової грамотності [22]. Неосвіченість у даній сфері є передумовою для активізації дій зловмисників, які мають негативний вплив на фінансову безпеку, оскільки збільшує спектр актуальних ризиків суб'єктів.

Базовим показником фінансової інклюзії є наявність банківського рахунку, оскільки надання додаткових фінансових послуг можливе лише за його наявності. Світовий банк щорічно подає інформацію про ключові показники фінансової інклюзії окремо за країнами та агрегованими групами, однак останні актуальні дані щодо України є лише станом на 2021 р., так як початок повномасштабної війни ускладнив їх збір та верифікацію [161]. Відповідно частка осіб, які мають банківські рахунки в Україні 2021 року становила 84%, що на 21 в.п. більше, ніж в 2017 р. (рис. 3.3).

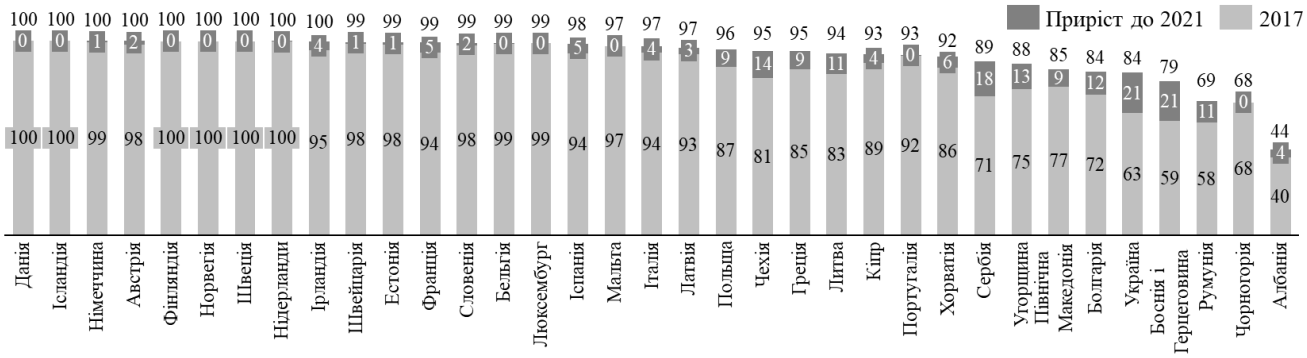


Рисунок 3.3. Частка осіб, які мають банківські рахунки в 2017–2021 рр., %

Джерело: складено автором на основі [161]

Однак максимальні значення даного показника сягають 100% у таких розвинутих країнах, як Данія, Німеччина, Фінляндія, Австрія та інші, що свідчить про можливість повного покриття населення базовими фінансовими послугами. З огляду на це, майбутній вектор розвитку фінансової інклюзії в Україні має бути спрямований на підвищення рівня частки осіб, які мають банківські рахунки, з середнього рівня до максимального в довгостроковій перспективі (до 10 років).

Зростання даного показника дасть змогу розвивати супутні фінансові послуги та якісно покращувати фінансову інклюзію країни в цілому.

Середній рівень фінансової інклюзії є перешкодою для розвитку страхування кібер-ризиків в Україні, оскільки особи з таким рівнем менш зацікавлені в фінансовій безпеці, яка в сучасному цифровому світі може бути реалізована через інструмент страхування; для осіб даної групи рівень доступу до фінансових послуг, зокрема страхових, доволі обмежений; для більшості осіб характерна обмеженість фінансових ресурсів, тому пріоритетність отримання послуг страхування кібер-ризиків стає другорядною.

3. Низький рівень економічної активності. Після наслідків пандемії COVID-19 в 2022 р., для української економіки додатковим фактором навантаження стала війна. Такі умови впливають на діяльність страховиків, оскільки дестимулюють розвиток нових продуктів, провокують низький рівень конкуренції між страховими компаніями та формують високі ціни на страхові послуги [58].

Статистичні дані свідчать про значний спад економічних показників після початку повномасштабної війни у 2022 р. Згідно з даними ДССУ, інфляція в Україні зросла до 26,6% в 2022 р. порівняно з 2021 р., однак сповільнилась до 5,1% у 2023 р. [32]. Розрив між реальним та потенційним ВВП впав до -11% в 2022 р. (-2% в 2021 р.), проте НБУ покращив прогноз на 2023 р. та встановив очікуване значення на рівні -6% [33].

Окрім зазначеного, низьку економічну активність посилюють військові реалії: регуляторні обмеження можливостей підприємництва, інвестування та міжнародної співпраці; фактичне переривання діяльності через знищення фізичного представництва страховиків, повітряні тривоги, потенційні втрати кваліфікованого персоналу, відключення електроенергії; нижчий попит на послуги страхування в цілому, а отже, виведення нової послуги на ринок або просування наявної послуги страхування кібер-ризиків страховики вважають нецільовим та нерентабельним.

4. Недостатній рівень розвитку інституційно-правового забезпечення. Україна використовує об'ємну інституційно-правову базу, що стосується кібербезпеки та стратегії її покращення, утім має потенціал для майбутнього вдосконалення [55]. Загалом використання цифрових технологій у діяльності страховика та страхувальника досі є недостатньо регульованим саме в страховому законодавстві [79]. Стримувальний характер даного фактору виражається через його особливості (рис. 3.4).

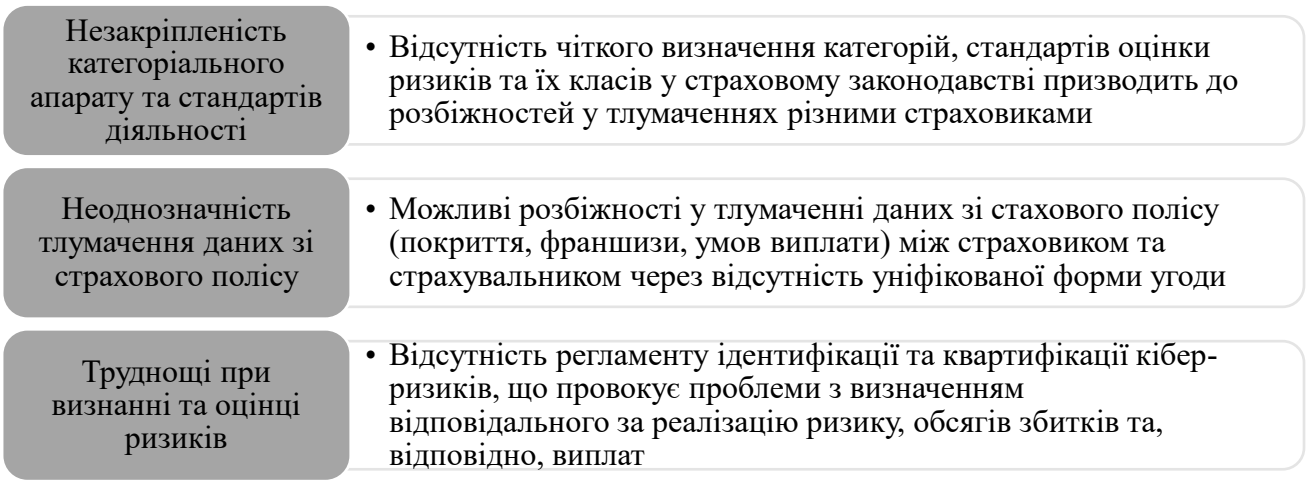


Рисунок 3.4. Особливості розвитку інституційно-правового забезпечення як фактору стримування розвитку страхування кібер-ризиків в Україні

Джерело: складено автором

5. Переміщення IT-компаній та еміграція кваліфікованих спеціалістів. Незважаючи на те, що під час глобальної пандемії COVID-19 виникали проблеми з пошуком кваліфікованих спеціалістів, особливої актуальності даний фактор набув після початку повномасштабної війни в 2022 р. Так, за даними Міністерства цифрової трансформації України, від початку війни 71% IT-компаній були змушені релокуватись, 17% із яких повністю або частково були переміщені за кордон. Ще одним сигналом відтоку фахівців стало зменшення кількості відкритих IT-вакансій на -20% порівняно з 2021 р. [20].

Негативний вплив даного фактору на розвиток страхування кібер-ризиків в Україні полягає у втраті IT-фахівців, які потенційно могли бути залучені до розвитку комплексної співпраці організацій у сфері цифровізації і кібербезпеки зі страховиками; географічному переміщенні локалізації кібер-ризиків, актуальних

для ІТ-спеціалістів та їхніх компаній, що знижує потребу в страхуванні таких ризиків в Україні; зменшення конкуренції між українськими страховиками, що негативно впливає на рівень послуг та їхню цінову політику.

6. Глобальна невизначеність та економічна нестабільність. З початком повномасштабного вторгнення перед страховиками постало питання актуалізації коротко-, середньо- та довгострокових планів розвитку. Дане завдання є базовим кроком результативної діяльності страховика, а тому потребує використання інструментів моделювання з адаптацією продуктів та послуг під воєнний стан [20]. Натомість використання інноваційних інструментів вимагає залучення кваліфікованих спеціалістів, що обмежується попереднім фактором. Загалом процес планування блокується відсутністю інформації про ключові детермінанти, що враховуються під час стратегічного планування, такі як: кількість населення, ВВП, темп інфляції, курс валют та можливі регуляторні вимоги чи обмеження.

Оскільки страхування кібер-ризиків є або повністю, або частково новим продуктом для страховиків в Україні (хоча зацікавленість до тематики кібербезпеки зростає [96, с. 46]), його роль на ринку страхування поки що не є визначальною. Відтак, цей напрямок не є пріоритетним для більшості страховиків, тому їх стратегія зазвичай включає лише просування традиційних страхових послуг. Для страховиків, особливо тих, хто має обмежені ресурси, побудова стратегій розвитку страхування кібер-ризиків або адаптація їхніх послуг до нових реалій відкладається на невизначений термін. Це може бути пов’язано з рядом факторів, включаючи відсутність достатнього розуміння характеристик ризиків та потенційних збитків від них в кіберпросторі, складність оцінки даних ризиків, а також відсутність стандартів, законів та норм щодо страхування кібер-ризиків. У періоди кризи, коли страховики стикаються з викликами та обмеженнями, пріоритетом для них є забезпечення стабільності та виживання. У зв’язку з цим, вони найчастіше віддають перевагу просуванню традиційних страхових послуг, які вже відомі і приносять стабільний дохід, оскільки це не вимагає додаткових витрат ресурсів на просування нових напрямків діяльності та має стабільний рівень попиту серед існуючих та потенційних страхувальників.

На противагу стримуючим факторам війна в Україні розширила перелік актуальних стимулюючих факторів розвитку страхування кібер-ризиків (рис. 3.5).

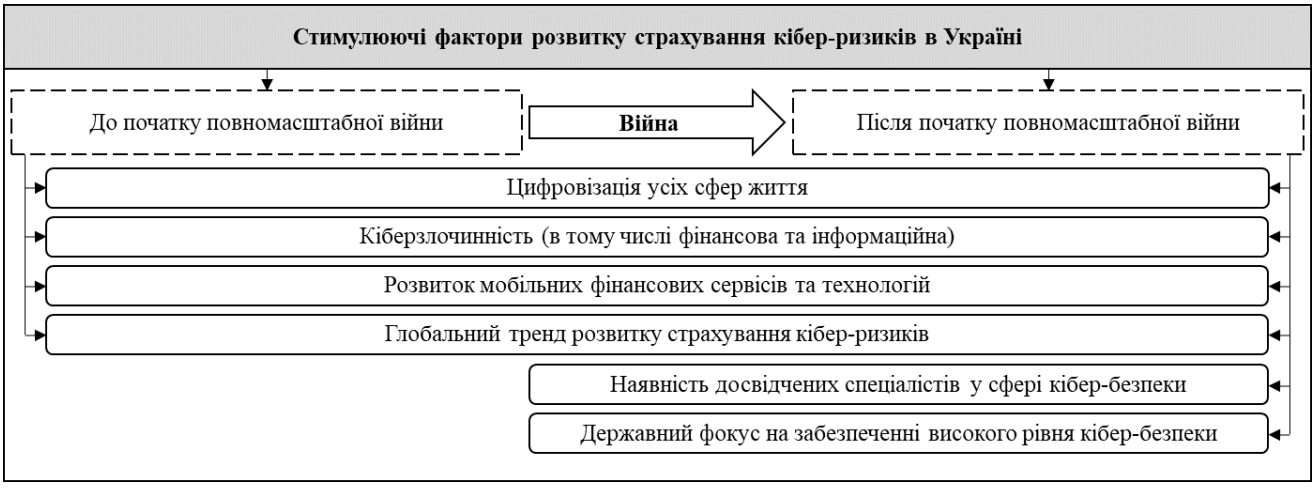


Рисунок 3.5. Стимулюючі фактори розвитку страхування кібер-ризиків в Україні до та після початку повномасштабної війни з Російською Федерацією

Джерело: складено та доповнено автором на основі [14]

До стимулюючих факторів розвитку страхування кібер-ризиків в Україні належать такі:

1. Цифровізація усіх сфер життя. З 2022 р. за ініціативи Міністерства цифрової трансформації було започатковано оцінювання цифрової трансформації України, що включає Індекс цифрової трансформації регіонів, до структури якого входять такі характеристики, як інституційна спроможність, розвиток ЦНАП, візитівка області, розвиток інтернету, цифрова освіта, режим «без паперів», проникнення базових е-послуг, галузева цифрова трансформація [31]. В 2023 р. вказаний Індекс становив 0,632, що на -0.019 менше, ніж у 2022 р. (дані 2022 р. брали на дату до початку повномасштабного вторгнення) [30; 31]. Незначне падіння пов’язане із воєнними діями та періодичними відключеннями електроенергії, що впливає на доступність цифрових послуг.

Масова цифровізація усіх сфер життя та діяльності розширює використання цифрових технологій, які можуть стати джерелом кіберзагроз, а тому вимагають розробки системи захисту від них, елементом якої є страхування. Натомість розширення спектру застосування інноваційних технологій часто має швидші темпи, ніж розвиток обізнаності про них. Тому страхування кібер-ризиків

мінімізує ймовірність настання кіберінциденту для недосвідчених користувачів та забезпечує фінансовий механізм їх відновлення в разі настання страхового випадку.

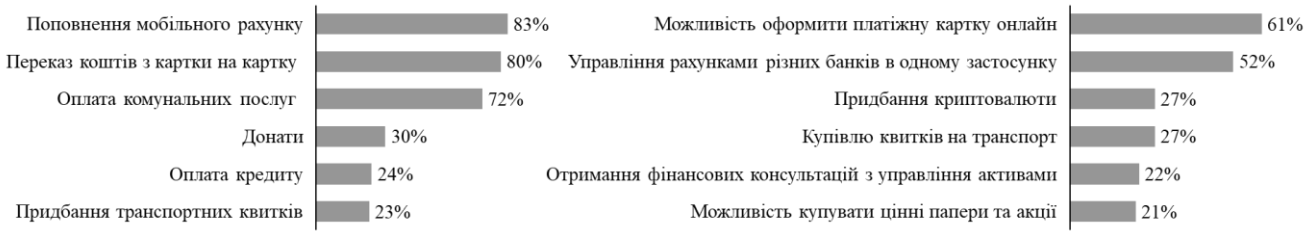
2. Кіберзлочинність. Із початком війни в Україні кількість зареєстрованих злочинів почала зростати. Одним із кроків обмеження даного фактору стало вдосконалення законодавства, що посилило кримінальну відповідальність за здійснення правопорушень у кіберпросторі. Тому в 2022 р. був ухвалений Закон «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану», що також розширило межі діяльності правоохоронних органів у цій сфері [5; 65].

Даний фактор розглядається як такий, що стимулює розвиток страхування кібер-ризиків, оскільки посилює та вдосконалює інституційно-правову базу, яка стосується кібер-злочинів; стає стимулом отримання послуг страхування після понесення збитків внаслідок кіберінциденту для майбутнього унеможливлення повторення таких ситуацій.

3. Розвиток мобільних фінансових сервісів і технологій. Стрімкий розвиток мобільних технологій розпочався під час пандемії COVID-19, коли більшість процесів були переведені в онлайн-режим. За даними опитування Mastercard, яке було проведене 2022 року, 51% українців готові повністю перейти на використання цифрового банкінгу без фізичної карти, окрім того, вже сьогодні активно використовують доступний функціонал мобільних фінансових сервісів без додаткового відвідування банківських відділень [19] (рис. 3.6).

Зважаючи на результати даного дослідження, очевидним стає високий рівень попиту українців на інноваційні мобільні фінансові сервіси та послуги, при цьому опитані виявили інтерес до нових напрямків розширення онлайн-банкінгу. На розвиток страхування даний фактор впливає завдяки розширенню доступності послуг страховика, зокрема, через онлайн-канали продажу та їх оптимізацію під зручний формат замовлення; зростанню кількості об’єктів страхування, оскільки збільшення мобільних технологій призводить до розширення переліку

потенційних ризиків; якісному захисту мобільних сервісів, що знижує вартість страхового полісу завдяки високому рівню кібербезпеки страхувальника.



а) Фактичні б) Потенційно корисні

Рисунок 3.6. Рейтинг фінансових послуг, що використовують та хотіли б використовувати респонденти, %

Джерело: складено автором на основі [19]

4. Глобальний тренд розвитку страхування кібер-ризиків. Про доцільність розвитку страхування кібер-ризиків тривають активні дискусії з початку Четвертої промислової революції, в той час як страховики самостійно активно розвивають даний напрямок. Досвід іноземних компаній, які щороку збільшують зібрані премії кібер-страхування, свідчить про зростання попиту на комплексні та самостійні поліси страхування ризиків такого типу.

Досвід іноземних та міжнародних страхових компаній, що мають свої представництва в Україні, допоможе розвивати страхування кібер-ризиків через залучення кваліфікованих фахівців, використання успішних кейсів просування послуг та аналіз проблем при запуску продуктів на страховому ринку. До того ж, відсутність пропозицій з належним покриттям на локальному рівні змушуватиме потенційних страхувальників шукати такий продукт за кордоном.

5. Наявність досвідчених спеціалістів у сфері кібербезпеки. Незважаючи на часткову еміграцію ІТ-фахівців, з початком гібридної війни кваліфікація спеціалістів з кібербезпеки, які залишились, значно підвищилась. Досвід подолання кіберзагроз, що виникали в Україні протягом 2022–2023 рр., складається з розв’язання проблем на різних рівнях: людина, домогосподарство, суспільство, організація, держава, де кожна ланка є взаємозалежною, адже пошкодження однієї ланки позначається на всіх інших.

Використання даного досвіду дасть змогу страховикам розв’язати методологічні питання кваліфікації та квантифікації ризиків, верифікувати проведення актуарних розрахунків, оптимізувати розрахунки страхових тарифів та обчислення всіх збитків.

6. Державний фокус на забезпеченні високого рівня кібербезпеки. Після початку пандемії COVID-19 за сприяння Міністерства цифрової трансформації України було створено багато освітніх курсів і програм у сфері кібербезпеки. Реалізація такого підходу була спрямована на запобігання кіберінцидентам, підвищення рівнів цифрової грамотності населення та захищеності від загроз цифрового простору. Після початку повномасштабної війни кількість доступних курсів навчання на порталі «Дія», пов’язаних із кібербезпекою, зросла завдяки розширенню можливостей віртуальних освітніх тренажерів [89].

Даний фактор має позитивний вплив на розвиток страхування кібер-ризиків в Україні, оскільки сприяє підвищенню рівня обізнаності із загрозами кіберпростору, відповідно, фізичні та юридичні особи використовують інструменти їх обмеження, одним із яких є страхування. Підвищення усвідомлення необхідності захисту від кіберзагроз, в свою чергу, стане основою для зростання попиту на страхування кібер-ризиків, а тому пожвавлення та трансформації страхового ринку в Україні, що є важливим завданням через війну, що продовжується на кіберфронті.

Зазначені стимулюючі фактори зможуть перекрити стримуючі фактори при зведенні всіх описаних особливостей у відповідну стратегічну матрицю впливу (Таблиця 3.1). Завданням матриці впливу є віднайти варіанти позитивного виправлення існуючих проблем розвитку страхування кібер-ризиків в Україні, через активне використання заходів та інструментів, що були визначені, як стимулюючі фактори. Відповідно, при ефективному управлінні факторами стимулювання розвитку та їхніми інструментами можливо нівелювати або мінімізувати фактори стримування розвитку та їхні наслідки для розширення використання страхування кібер-ризиків в Україні.

Таблиця 3.1

Стратегічна матриця впливу стимулюючих та стримуючих факторів на розвиток страхування кібер-ризиків в Україні

Стримуючі фактори / Стимулюючі фактори	Середній рівень цифрової грамотності	Середній рівень фінансової інклюзії	Низький рівень економічної активності	Недостатній рівень розвитку інституційно-правового забезпечення	Переміщення ІТ-компаній, еміграція кваліфікованих фахівців	Глобальна невизначеність, економічна нестабільність
Цифровізація всіх сфер життя	■	■		■		
Кіберзлочинність	■			■		
Розвиток мобільних фінансових сервісів і технологій		■	■		■	
Глобальний тренд розвитку страхування кібер-ризиків	■			■		■
Наявність досвідчених фахівців у сфері кібербезпеки			■	■		
Державний фокус на забезпеченні високого рівня кібербезпеки	■			■	■	■

Джерело: розробка автора

Відповідно до зазначеної матриці, деталізуємо шляхи подолання стримуючих через розкриття стимулюючих факторів на розвиток страхування кібер-ризиків в Україні.

1. Середній рівень цифрової грамотності можна покращити в першу чергу за допомогою державного фокусу на підвищенні доступності та популяризації навчальних програм, що вчать долати загрози кіберпростору. Оскільки, як було визначено, кількість кіберінцидентів зростає, тому населення України самостійно може вивчати сучасні правила поведінки в цифрових програмах та сервісах, через усвідомлення поточного рівня кіберзлочинності. Даний підхід підсилюється і тим, що рівень цифровізації усіх сфер життя постійно підвищується, незважаючи на війну та економічну нестабільність. Зрозуміло, що загальні світові тренди розвитку страхування кібер-ризиків, вимагають використання даного інструменту захисту від кіберзагроз на вітчизняному

страховому ринку, оскільки в разі відсутності необхідних страхових послуг, потенційні страхувальники можуть звертатись до іноземних страховиків.

2. Для підвищення середнього рівня фінансової інклюзії варто підвищувати пенетрацію мобільних фінансових сервісів і технологій для усіх верств населення, оскільки технологічний потенціал українського ІТ-сектору є доволі високим, однак його діяльність орієнтована на експорт. Створення симбіозу українських фінансових установ та ІТ-компаній дозволить створити доступні цифрові фінансові сервіси і технології, запобігши відтоку ІТ-спеціалістів закордон. Також рівень фінансової інклюзії має потенціал для росту через активну цифровізацію усіх сфер життя, що призводить до міграції типових каналів надання деяких послуг у цифрову сферу, вимагаючи створення споживачами банківських сервісів, що підтримують онлайн-операції.

3. Здолання низького рівня економічної активності – це справжній виклик для всіх економічних суб'єктів в умовах війни. Однак через активний розвиток мобільних фінансових сервісів і технологій, можлива активізація їх розробки українськими ІТ-фахівцями, що розширить кількість робочих місць, підвищить інвестиційну привабливість даного сектору та забезпечить прозорість фінансових потоків. Ще одним допоміжним фактором є наявність досвідчених фахівців у сфері кібербезпеки, що успішно проводили операції у кіберпросторі. Використовуючи їхні знання та можливості, доцільним є створення додаткових робочих місць у цій сфері задля створення навчальних програм по покращенню цифрової грамотності населення.

4. Відповідно до запропонованої матриці, найбільше можливостей для покращення має вітчизняне інституційно-правове забезпечення. Дійсно, сучасний тренд цифровізації усіх сфер життя вимагає адаптацію законодавства під нові реалії або його створення, через виникнення нових сфер, явищ, технологій, професій та ін. Супутнім фактором є розвиток злочинності у кіберпросторі, тому створення правового механізму, що регулює інциденти у даній сфері є важливим завданням. Ще одним підходом, за яким даний стримуючий фактор може бути нівельований, пов'язаний з підняттям пріоритетності питання кібербезпеки для

держави. При реалізації відповідного комплексу заходів, виконання яких контролюється державою, необхідним буде створення супутнього інституційно-правового забезпечення. Гармонізація законодавства, що пов'язана зі страхуванням кібер-ризиків, може базуватись на існуючій світовій практиці, оскільки в глобальному вимірі даний сегмент страхового ринку активно розвивається протягом останніх 10 років. Позитивний ефект на розвиток інституційно-правового забезпечення має наявність досвідчених фахівців у сфері кібербезпеки, оскільки використання практичних кейсів ідентифікації, оцінки, подолання кіберзагроз, може стати ефективною основою для якісних змін у даній сфері. Також експертиза таких спеціалістів є підґрунтям для надання правової оцінки кіберінцидентам, що вже відбулись, проте раніше не були визначені.

5. Переміщення IT-компаній і еміграція кваліфікованих фахівців, що почались під час пандемії COVID-19 та посилились після початку повномасштабного вторгнення, можуть бути врегульованими через реалізацію привабливого середовища для їх розвитку на національному ринку. Для цього варто створювати державні пропозиції та проекти, направлені на розвиток кібербезпеки, трансформації фінансових послуг та інших напрямків, де першочерговими кандидатами на роль виконавців будуть українські IT-компанії, що мають відповідну експертизу. Також, як вже було зазначено, ефективним також буде підхід по створенню партнерств вітчизняних фінансових установ та IT-організацій.

6. Глобальна невизначеність і економічна нестабільність мають безліч зовнішніх факторів впливу, однак в рамках проведеного дослідження частково зменшити їх негативний аспект можливо через існуючий глобальний тренд розвитку страхування кібер-ризиків. Очевидно, що головною метою цього виду страхування є убезпечення страхувальників від поселення негативних фінансових втрат. Також при створенні державою комплексних стратегій кібербезпеки, що місять положення, які направлені на розширення цифрових можливостей громадян, вплив глобальної невизначеності і економічної нестабільності буде зменшуватись.

Відтак, основоположним напрямком, який вимагає найбільш активного вдосконалення для розвитку страхування кібер-ризиків на вітчизняному страховому ринку, є розробка та гармонізація інституційно-правового забезпечення страхування кібер-ризиків в Україні. Даний напрямок є важливим, оскільки ефективне регулювання та наявність якісної законодавчої бази у вказаній галузі є ключовими чинниками для стимулювання розвитку страхового ринку та забезпечення його стійкості у майбутньому. Тому варто визначити вектори удосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні.

3.2. Вектори удосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні

Як уже було визначено, напрямок регулювання страхування кібер-ризиків потребує вдосконалення як на глобальному, так і на національному рівнях. Визначення чітких законодавчих норм, стандартів і процедур забезпечить ефективний механізм співпраці між страховиком, страхувальником, регулятором та іншими суб'єктами страхування, що, як наслідок, матиме позитивний вплив на розвиток кібербезпеки на всіх рівнях. Відповідно, оптимізація чинного інституційно-правового забезпечення є запорукою розвитку страхування кібер-ризиків в Україні.

У 2021 р. Президент України затвердив Стратегію кібербезпеки України, в якій, окрім іншого, вказана Ціль В.2 реалізації національної моделі відносин у сфері кібербезпеки, що включає в себе розвиток системи страхування кібер-ризиків [74]. Однак станом на 2023 р. значних змін на ринку страхування немає, оскільки розвиток основ державного регулювання у вказаній сфері сповільнився через негативні впливи COVID-19 та повномасштабне вторгнення Російської Федерації в Україну.

Незважаючи на наслідки затяжної кризи, спричиненої пандемією COVID-19, що стали причиною падіння іноземних інвестицій, зменшення виробництва та зростання безробіття [149], процес цифрової трансформації української економіки почав прискорюватися завдяки збільшенню частки онлайн-бізнесу та, відповідно, кількості сервісів, що його обслуговують. Також у період пандемії COVID-19 значного розвитку набув ринок криптовалют, який одночасно зі створенням можливостей для трансформації сучасної фінансової системи став основою розширення переліку критичних ризиків [229]. Так, період пандемії став, з одного боку, причиною сповільнення виконання запланованих заходів у сфері кібербезпеки і, зокрема, страхуванні кібер-ризиків, а з іншого, драйвером зростання загроз у кіберпросторі.

Через повномасштабне вторгнення Російської Федерації робота над досягненням цілей, вказаних у Стратегії кібербезпеки України, переорієнтувалась на забезпечення стабільності критичної інфраструктури та об'єктів, що мають важливе значення в умовах війни. Тому заходи, які мали забезпечувати розвиток страхування кібер-ризиків, знову відтермінувались.

Як ми визначили, українські страховики мають потенціал розвитку страхування кібер-ризиків, однак перепоною для зростання вказаного ринку, окрім відсутності фокусу держави з об'єктивних причин, є нерозвинутість інституційно-правової бази, що окреслює ключові напрямки функціонування страхування даного виду. Відповідно варто проаналізувати та систематизувати чинне вітчизняне законодавство, що прямо чи опосередковано може стосуватися страхування кібер-ризиків (Додаток Ж).

Закон України «Про страхування» станом на 1 січня 2024 р. містить визначення поняття «операційний ризик», джерелами якого можуть бути: некоректна організація внутрішніх процесів, дії працівників чи інших осіб, збої у роботі інформаційних систем або вплив зовнішніх факторів [73]. Однак у законі дане поняття використовується не в контексті напрямків діяльності страховика, а в контексті системи управління ризиками самого страховика. Відповідно в

переліку класів страхування прямо не вказується страхування кібер-ризиків або ж цифрових ризиків чи інформаційних.

Однак у Постанові НБУ «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» дефініція «кібер-ризик» визначена як «ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз» [68]. Тому в українському законодавстві уже визначено базове поняття страхування кібер-ризиків, що є основою для майбутнього вдосконалення інституційно-правової бази у цій сфері.

Для вибору оптимального алгоритму вдосконалення чинного законодавства варто розглянути наявні приклади іноземного досвіду трансформації інституційно-правової бази у сфері страхування кібер-ризиків. Оскільки американський ринок цього виду страхування є найбільш розвинутим, варто визначити ключові характеристики їхнього законодавства у вказаній сфері.

Відповідно до нормативного акту 23 NYCRR 500, опублікованого Департаментом фінансових послуг штату Нью-Йорк, США, який поширює свою дію на всіх уповноважених страховиків, у документі був викладений фреймворк розвитку системи страхування кібер-ризиків [124]. Відповідно до запропонованої стратегії розвитку та популяризації даного виду страхування, регулятор та страховики мають реалізувати ефективний механізм співпраці для задоволення потреб страхувальників, кінцевим результатом чого стане посилення національної кібербезпеки. Для досягнення бажаної синергії у фреймворку зазначені наступні кроки:

- створення оптимальної стратегії страхування кібер-ризиків кожним окремим страховиком у межах його можливостей;
- розробка алгоритму виявлення неідентифікованих ризиків страхувальників, що можуть стати причиною настання катастрофічних страхових випадків;

- оцінка системного ризику страхувальників, оскільки частішають випадки перекладання частини виробництва на третіх осіб, покриття ризиків яких не входить до страхової угоди;
- запровадження механізму деталізованої оцінки страхувальних ризиків через отримання повної, прозорої та об'єктивної інформації про страхувальників;
- проведення навчальних програм, спрямованих на обізнаність населення та бізнесу з можливими кібер-ризиками та їх наслідками, а персоналу страховиків з особливостями продуктів страхування кібер-ризиків;
- використання міжнародних стандартів кібербезпеки в своїй діяльності та залучення досвідчених фахівців, які є експертами у вказаній сфері;
- визначення алгоритму взаємодії з поліцією або іншими уповноваженими органами щодо надання інформації про страхові випадки, які є порушенням чинного законодавства.

В оновленій Стратегії кібербезпеки США у 2023 р. одним із завдань вказано розробку федеральної системи страхування кібер-ризиків [198]. Тобто можливі наслідки реалізації кіберзагроз американський уряд оцінює як катастрофічні, що потребують національного контролю. З огляду на це стимулювання розвитку ринку страхування кібер-ризиків є однією з національних цілей США, за якою, при настанні катастрофічних страхових випадків, що загрожуватимуть національній безпеці, Конгрес, Регулятор, Адміністрація Президента та інші стейкхолдери будуть ухвалювати рішення про фінансування страховиків та організацій у сфері кібербезпеки з метою відновлення стабільності постраждалих.

Порівнюючи стратегію кібербезпеки Європейського Союзу з американською стратегією, варто зазначити, що остання є більш широкою та повною [226]. По-перше, європейська стратегія була востаннє оновлена 2020 року на період 2020–2025 рр., тоді як у 2023 р. відбулось чергове вдосконалення американської стратегії з урахуванням нових викликів кіберпростору та можливостей сучасних інструментів кібербезпеки. По-друге, розвиток американської корпоративної сфери кібербезпеки тісно пов'язаний з національною безпекою, оскільки у разі, якщо організація потрапляє в категорію

критично важливих суб’єктів для національних інтересів, то отримує додаткові рівні захисту, що їх надають на національному рівні. По-третє, закріплення інструментів страхування кібер-ризиків в американській стратегії є наслідком розвинутого ринку даного виду страхування, відповідно, досвід використання перевірених практик дає розуміння потенціалу додаткового захисту внаслідок вказаного виду страхування.

Курс України на вступ до Європейського Союзу зумовив посилення активної співпраці між українськими та європейськими організаціями у багатьох сферах. Так, у листопаді 2023 р. була укладена угода між Національним координаційним центром кібербезпеки при РНБО України, Адміністрацією Державної служби спеціального зв'язку та захисту інформації України і Агентством Європейського Союзу з мережевої та інформаційної безпеки (ENISA), спрямована на покращення освіченості у сфері кібербезпеки, обмін досвідом у даній галузі та розбудову інфраструктури сфери кібербезпеки [90].

Одним із пунктів угоди була розробка та вдосконалення законодавства у сфері кібербезпеки на основі Директиви ЄС NIS 2, яка регулює заходи щодо покращення рівня захищеності в кіберпросторі та створення систем звітності про настання кіберінцидентів [150]. Сьогодні дія директиви у Європейському Союзі поширюється на галузі промисловості, для яких зафіксований звичайний або високий рівень критичності (Таблиця 3.2).

Запропонована класифікація критичних галузей промисловості підходить і для України, особливо в умовах військового стану. Використання цієї категоризації дасть змогу визначити пріоритетність розвитку кіберзахисту підприємств української промисловості: з високим рівнем критичності, що мають бути повністю забезпечені державою в партнерстві зі спеціалізованими організаціями; зі звичайним рівнем критичності, управління ризиків яких може бути диверсифіковане, зокрема, за рахунок страхування кібер-ризиків.

Також у 2020 р. агентство ENISA, з яким Україна уклала угоду про співпрацю, опублікувало «Керівництво оцінки національних спроможностей», де

була визначена методологія оцінки локальних стратегій кібербезпеки держав та потенціал їхнього розвитку [197].

Таблиця 3.2

Галузі промисловості зі звичайним та високим рівнем критичності, на які поширюється дія Директиви Європейського Союзу NIS 2

Галузь	Підгалузь / суб'єкти галузі
Галузі промисловості з високим рівнем критичності	
Енергетика	Електроенергетика, міські системи опалення чи охолодження, енергетика (паливо, газ, водень)
Транспорт	Повітряний, залізничний, водний, дорожній
Банківська справа	Банківські установи, що здійснюють послуги кредитування
Складові фінансового ринку	Суб'єкти фінансового сектору, що здійснюють свою діяльність у рамках визначених Директив ЄС
Охорона здоров'я	Виробники медичної та фармацевтичної продукції, дослідницькі центри та лабораторії, надавачі медичних послуг
Питна вода	Постачальники та виробники питної води
Стічні води	Підприємства, що збирають, видаляють або обробляють стічні води
Цифрова інфраструктура	Постачальники та провайдери цифрових послуг і сервісів
Електронні комунікаційні послуги	Постачальники сервісних послуг та послуг безпеки
Державне управління	Органи державного управління всіх рівнів
Космічна сфера	Постачальники чи оператори послуг космічної сфери
Галузі промисловості зі звичайним рівнем критичності	
Поштові та кур'єрські послуги	Постачальники поштових та кур'єрських послуг
Відходи	Підприємства, що здійснюють управління відходами
Хімічне виробництво	Виробники і дистриб'ютори визначених хімічних речовин
Харчове виробництво	Підприємства оптової торгівлі, промислового виробництва та обробки, пов'язані з продуктами харчування
Інше виробництво	Виробництво комп'ютерної техніки, електрообладнання, машин та устаткування тощо
Цифрові провайдери	Провайдери маркетплейсів, пошукових систем, соціальних мереж
Дослідження	Дослідницькі організації

Джерело: складено автором на основі [150]

Додатково в документі було названо сфери, які варто вдосконалювати на національному рівні для підвищення базового рівня кібербезпеки. Одним із запропонованих векторів оптимізації було страхування кібер-ризиків, оскільки на території ЄС воно перебуває на початковому рівні розвитку. Також було визначено, що популяризація даного виду страхування дає такі позитивні ефекти:

- підвищення рівня усвідомленості потенційних загроз кіберпростору організацій та домогосподарств;
- оптимізація системи ризик-менеджменту страхувальників у частині кібербезпеки;
- створення механізмів надання підтримки постраждалим від кіберінцидентів;
- реалізація механізму покриття збитків (у фінансовому, управлінському, консультаційному вигляді) після настання страхового випадку;
- квантифікація впливу кібер-ризиків не тільки для конкретних потенційних страхувальників, а й для галузей промисловості.

Окремо в керівництві ENISA розглядають приклади Естонії та Люксембургу, які підтримують розвиток страхування кібер-ризиків на національному рівні через створення цільових страхових продуктів, що покривають ризики, актуальні для даних регіонів.

Одним із прикладів якісного ефекту синергії державних органів влади, страховиків і спеціалістів у сфері кібербезпеки є Стратегія кібер-безпеки Австралії [99], розроблена у 2023 р., де запропоновано шість цілей, що мають бути реалізовані до 2030 р.:

- сильний захищений бізнес та громадяни;
- безпечні технології, що використовуються в будь-якій сфері країни;
- глобальна мережа обміну корисними даними та знаннями у сфері кібербезпеки, а також інформацією про загрози кіберпростору для їх вчасного блокування;
- захищена критична інфраструктура;
- розробка власних інструментів захисту для збереження суверенності у кіберпросторі;
- стабільність та стійкість до загроз, а також глобальне лідерство у сфері кібербезпеки.

Незважаючи на те, що вказаний комплекс заходів не містить прямої мети розвитку страхування кібер-ризиків, однак сама стратегія була розроблена

робочою групою, що включала представників страхових компаній [211]. Оскільки представники страхової галузі вже мали досвід управління та страхування кіберризиків, представники державного сектору консультувались зі страховиками щодо особливостей ідентифікації та квантифікації сучасних ризиків, а також механізмів для мінімізації ймовірності їх настання. Зокрема, страховики оцінювали доцільність розробки єдиної бази кіберінцидентів, оскільки в такому разі можуть бути порушені стандарти конфіденційності даних.

Загалом Австралія пропонує всеохопну модель підтримки кібербезпеки як для юридичних, так і для фізичних осіб. Усім, кому потрібна допомога у зв'язку з настанням чи підозрою про настання кіберінциденту, доступна цілодобова підтримка через офіційний веб-сайт «The Australian Signals Directorate's Australian Cyber Security Centre» [224]. Проте на вказаному сайті також доступні ресурси для навчання у сфері кібербезпеки, включаючи тренінги для власників бізнесу, їхнього персоналу та звичайних громадян. Таке широке наповнення державних офіційних ресурсів спрямоване на створення повного комплексу урядових засобів кіберзахисту на противагу приватним організаціям.

Оскільки більшість проаналізованих стратегій включають використання міжнародних стандартів кібербезпеки для ефективного управління ризиками, варто розглянути доцільність їх імплементації в українських реаліях.

International Organization for Standardization (ISO) – міжнародна організація, що здійснює розробку та ратифікацію стандартів, які є підґрунтям для діяльності та уніфікації процесів різних сфер. Для страховиків варто визначити стандарти, рекомендовані до запровадження в діяльність страхувальників для покращення стану їхньої кібербезпеки.

Стандарт ISO 22301:2019 надає рекомендації щодо системи управління неперервністю бізнесу [173]. Так, у разі настання критичної події (зокрема, кіберінциденту), при виконанні запропонованих у стандарті заходів, організація швидко відновлює свою стабільну діяльність. Головним завданням даного документа є вказівки щодо запровадження дієвої системи, яка може вчасно визначити загрозу, за можливості її уникнути обмежити реалізацію ризику або

мінімізувати наслідки в разі настання кризового інциденту. Кризовими або катастрофічними ризиками вважаються як природні (катаклізми, погодні катастрофи), так і техногенні явища (технологічні аварії, кіберінциденти).

Під час прийняття ризиків на страхування, страховик або експерти у сфері кібербезпеки можуть пропонувати стратегії покращення процесу діяльності страхувальника на основі стандарту ISO 22301:2019, запровадження якого посилює захищеність суб'єкта, оскільки виконання рекомендацій дає змогу ефективно керувати великими ризиками та забезпечувати безперервну бізнес-діяльність навіть під час реалізації катастрофічних загроз.

Наступна група стандартів ISO/IEC 27000 була розроблена разом з Міжнародною електротехнічною комісією, і в ній надається опис вимог до управління інформаційною безпекою [174-177]. Обсяг стандартів у групі постійно збільшується у зв'язку з наростанням розмаїття інформаційних систем. В цілому стандарти даної групи спрямовані на розвиток механізмів управління інформаційними загрозами, пов'язаними зі зберіганням, передачею та трансформацією даних, а також забезпеченням їх цілісності та конфіденційності. Наслідком запровадження цих стандартів є розбудова IT-інфраструктури, що взаємодіє з інформацією, відповідно до міжнародних стандартів, законодавства чи інших нормативних вимог, що пов'язані з даними.

Використання вказаної групи стандартів є ефективним інструментом для підготовки інформаційних систем страхувальника до прийняття ризиків, що з ними пов'язані, на страхування. Збільшення стійкості страхувальника до кіберзагроз зменшує кількість актуальних для нього ризиків, а це натомість впливає на зниження вартості страхування.

Ще одним важливим стандартом є ISO/IEC 27701:2019, в якому визначено вимоги щодо управління персональними даними [178]. Наслідком запровадження цього стандарту є організація ефективної захищеної системи, в якій передача та обробка персональних даних буде здійснюватись на умовах конфіденційності та цілісності. В цілому стандарт пропонує комплекс заходів, які відповідатимуть вимогам Загального регламенту про захист даних (GDPR) та інших нормативних

актів, що стосуються персональних даних, тобто гармонізує чинні вимоги до обробки персональних даних.

Для страхових компаній, які приймають на страхування кібер-ризики, пов'язані з відповідальністю, даний стандарт є особливо важливим. Оскільки локальні законодавства, що регулюють використання персональних даних, можуть відрізнятися залежно від територіальної ознаки їхньої дії, стандарт ISO/IEC 27701:2019 створює уніфікований підхід до всіх потенційних страхувальників для зменшення їхніх ризиків, що стосуються персональних даних.

На території ЄС діє регламент GDPR, який регулює захист персональних даних [212]. Законодавство визначає принципи збору та обробки персональної інформації, права суб'єктів персональних даних, визначення контролера та оператора даних, виявлення індикаторів порушення безпеки даних, розрахунку штрафів за порушення тощо. Відповідно, всі суб'єкти, що здійснюють свою діяльність на території ЄС, мають дотримуватись описаних у регламенті GDPR принципів.

Під час страхування кібервідповідальності, пов'язаної з кібер-ризиками, використання страхувальником GDPR в країнах ЄС є базовою вимогою для його успішного прийняття на страхування. Тож адаптація даного Регламенту в Україні є важливим етапом для розвитку страхування кібер-ризиків на українському страховому ринку (рис. 3.7).

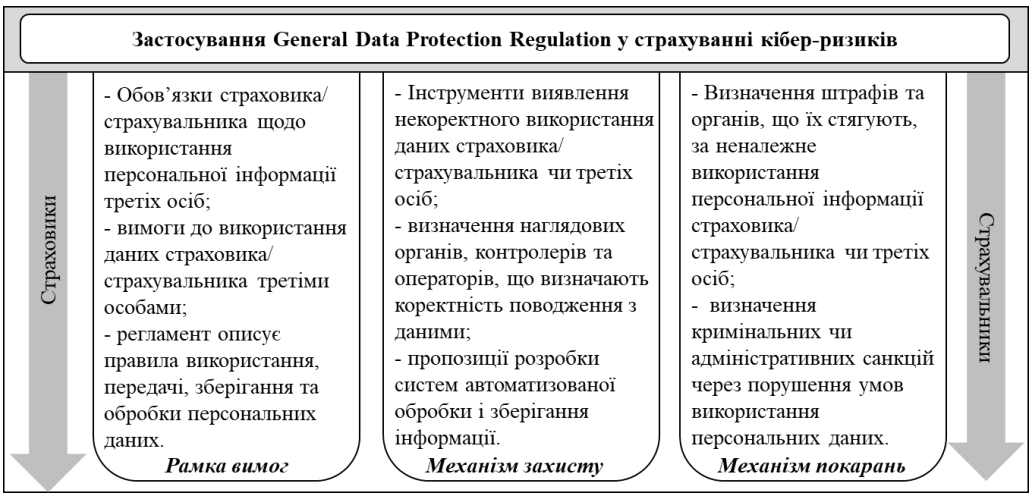


Рисунок 3.7. Переваги використання GDPR при страхуванні кібер-ризиків
Джерело: складено та доповнено автором на основі [212]

Запровадження GDPR важливо розглядати саме в контексті євроінтеграційних процесів, оскільки дія регламенту поширюється на персональні дані, що обробляються суб'єктами, які перебувають у межах ЄС, а також суб'єктами поза межами ЄС, які використовують персональні дані фізичних та юридичних осіб ЄС. Відповідно, Закон України «Про захист персональних даних» та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» потрібно гармонізувати з чинним законодавством ЄС [70; 209].

На думку експертів, до моменту вступу України до ЄС використання повного регламенту GDPR та його імплементація спричинить виникнення низки проблем при зборі та обробці персональних даних, що значно ускладнюється умовами війни [3, с.48].

Тому доцільно говорити про адаптацію чинного Закону України «Про захист персональних даних» у частині теоретико-методичних основ сфери дії закону, визначення прав суб'єктів, контролерів та операторів даних, створення незалежного наглядового органу, проте без фіксації екстериторіальної дії закону.

Однак особливо важливим вектором розвитку українського інституційно-правового забезпечення в сфері страхування кібер-ризиків є окреслення підходів до оцінки кібер-ризиків. Розробка уніфікованого механізму квантифікації кібер-ризиків унеможливить варіанти спекуляції на вартості страхових продуктів та забезпечить здорову конкуренцію на страховому ринку.

Міжнародний валютний фонд у 2018 р. оприлюднив документ «Кібер-ризик фінансового сектору: фреймворк кількісної оцінки», де був запропонований підхід до поетапної ідентифікації та квантифікації кібер-ризиків фінансового сектору [130]. На основі проведених досліджень експерти запропоновували наступну формулу оцінки кібер-ризику в базовому вигляді, що побудована на взаємозалежності характеристик даного ризику:

$$Risk = f(Threat, Vulnerability, Consequences), \quad (3.1)$$

де $Risk$ – кількісна оцінка кібер-ризику;

$Threat$ – загроза, притаманна для аналізованої сфери ризиків;

$Vulnerability$ – вразливість, тобто ймовірність настання кіберінциденту;

$Consequences$ – наслідки, що виникають внаслідок настання кіберінциденту.

Відповідно, для кожного компоненту формули проводиться детальний аналіз кількісних характеристик, залежно від регіону, сфери діяльності, особливостей технології та національної політики кібербезпеки.

Розрахунок вказаних показників для України ускладнюється умовами війни, оскільки теоретична оцінка ймовірності настання кіберінциденту для певного об’єкта може відрізнятися від фактичної у разі, якщо об’єкт буде атакований кіберзлочинцями як важлива ціль під час гібридної війни. Однак робота над відповідним дослідженням та його документацією може бути розпочата в рамках оцінки втрат від розпочатої Російською Федерацією війни задля визначення розміру необхідних відшкодувань у майбутньому.

До робочої групи оцінки фактичних втрат від кібер-ризиків та квантифікації потенційних кібер-ризиків, актуальних для України, можуть бути залучені: представники урядових органів, регулятора (НБУ), вітчизняні та іноземні страховики, вітчизняні та іноземні експерти у сфері кібербезпеки, міжнародні організації у сфері кібербезпеки та захисту персональних даних, іноземні урядові консультанти тощо.

На основі вищезазначеного векторами вдосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні вважаємо:

- розробку стратегії розвитку страхування кібер-ризиків як одного із заходів, вказаних у Цілях Стратегії кібербезпеки України;
- запровадження або гармонізацію регламентів та стандартів, що регулюють діяльність суб’єктів у кіберпросторі з метою посилення їхньої кібербезпеки та збереження конфіденційності і цілісності їхніх персональних даних або інформації, яку вони використовують;
- створення моделі квантифікації кібер-ризиків на основі їхніх характеристик, актуальних у сучасних українських реаліях, за прикладом формул у пункті 1.3, які враховують дані про кіберінциденти не лише від Державного центру кіберзахисту, а й безпосередньо від потенційних страхувальників, залежно

від сфери їхньої діяльності (через застосування запропонованого скринінгу в Додатку Г).

Відповідно до проаналізованих стратегій кібербезпеки різних регіонів, сукупність запропонованих заходів розвитку страхування кібер-ризиків має будуватись на основі клієнтоцентричної моделі, за якої посилення безпеки найменшого суб'єкта веде до підвищення національної кібербезпеки (рис. 3.8).

У такому разі страхування кібер-ризиків впливатиме на посилення кібербезпеки страхувальника, що зі свого боку впливатиме на кібербезпеку галузі чи сфери, яка натомість підвищуватиме національну кібербезпеку.

Рисунок 3.8. Ефект використання клієнтоцентричної моделі під час запровадження та розвитку страхування кібер-ризиків

Джерело: складено автором на основі [99; 198; 226]

На думку Т. Мудлей та К. К. Говендер, реалізація клієнтоцентричного підходу під час страхування відбувається через використання таких принципів [194, с.68-74]:

1. Врахування потреб конкретного страхувальника, тобто створення індивідуального наповнення страхового продукту, що задовольняє його потреби в захисті об'єктів.

2. Врахування відгуків наявних клієнтів про страхові продукти, досвід їх отримання та використання. Даний принцип відображає постійну оптимізацію продукту на основі отриманих рекомендацій чи зауважень.

3. Використання інтернет-каналів продажу страхових продуктів з просуванням через соціальні мережі, оскільки в сучасному світі персоналізований контакт між страховиком та потенційним клієнтом може бути встановлений без фізичного спілкування, достатнім буде листування в чаті соцмережі чи на сайті.

4. Створення адекватної цінової пропозиції, що враховує особливі характеристики потенційного страхувальника, усуваючи можливість спекуляції тарифами.

5. Забезпечення широкої системи зворотного зв'язку для створення різних каналів спілкування зі страхувальником, в яких він зможе швидко отримати необхідну йому інформацію в рамках дії страхової угоди.

Задля розвитку ефективної системи страхування кібер-ризиків в Україні варто використовувати вказані принципи клієнтоцентричної моделі страхування з метою формування пропозиції страхових продуктів, що відповідатимуть попиту на них.

Відповідно до описаних підходів, вектори вдосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні мають втілюватись на основі синергії всіх зацікавлених стейкхолдерів з урахуванням конкретних потреб страхувальників (рис. 3.9).

Для розробки стратегії розвитку страхування кібер-ризиків пропонується реалізувати такі заходи: аналіз закордонного досвіду розвитку страхування кібер-ризиків; визначення потенціалу вітчизняних страховиків щодо запровадження та розвитку страхування кібер-ризиків; розробка цільових показників запровадження та розвитку страхування кібер-ризиків; визначення наглядових органів / рад над процесом виконання стратегії, запровадження стимулів для страховиків; виявлення прогалин в інституційно-правовій базі щодо регулювання страхування кібер-ризиків.

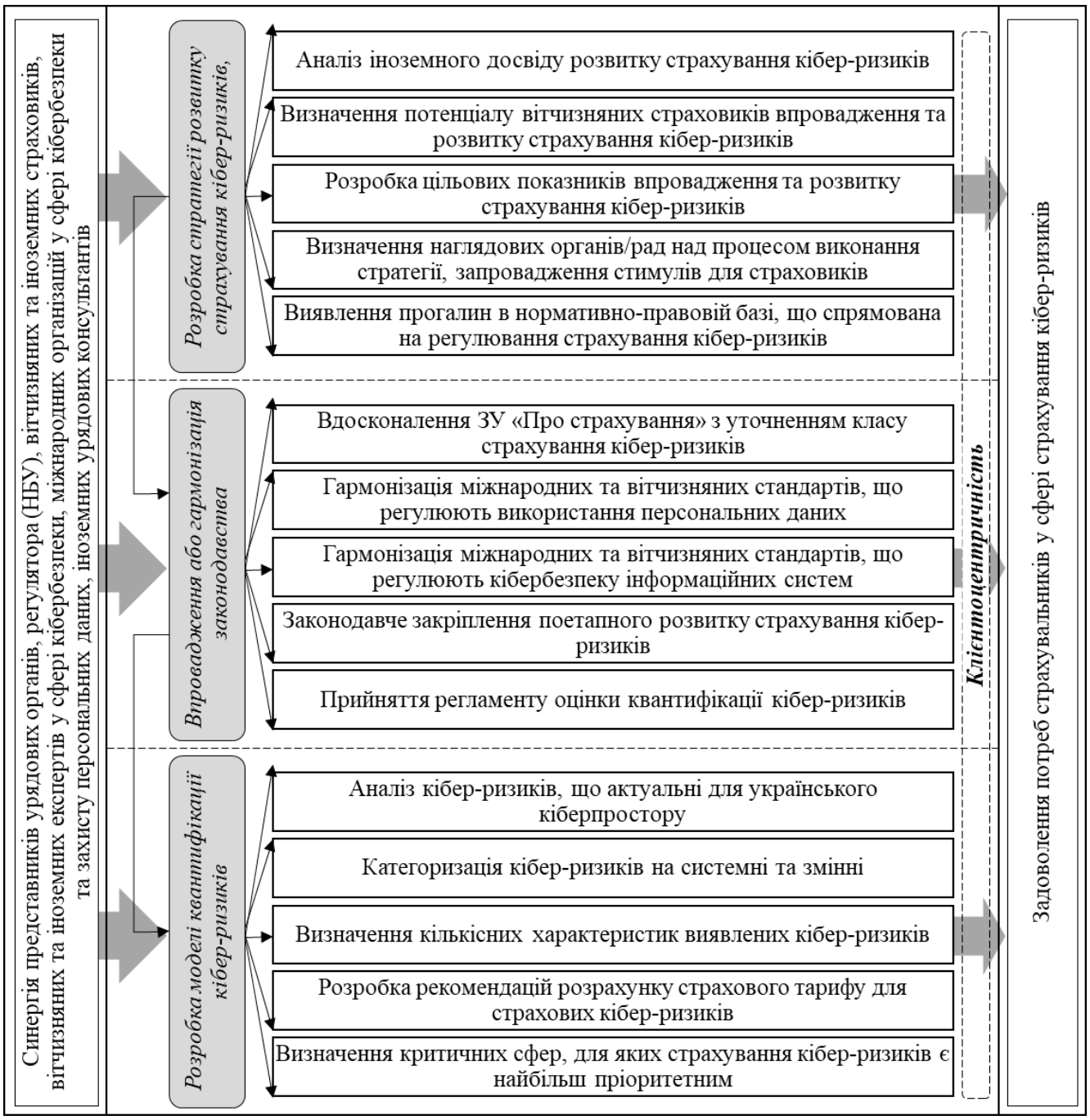


Рисунок 3.9. Вектори вдосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні

Джерело: розробка автора

Для запровадження або гармонізації законодавства доцільно вжити таких заходів: вдосконалення Закону України «Про страхування» з уточненням класу страхування кібер-ризиків; гармонізація міжнародних та вітчизняних стандартів, що регулюють використання персональних даних; гармонізація міжнародних та вітчизняних стандартів, що регулюють кібербезпеку інформаційних систем;

законодавче закріплення поетапного розвитку страхування кібер-ризиків; прийняття регламенту оцінки квантифікації кібер-ризиків.

З метою розробки моделі квантифікації кібер-ризиків варто здійснити такі заходи: аналіз кібер-ризиків, актуальних для українського кіберпростору; категоризація кібер-ризиків, актуальних для українського кіберпростору, на системні та змінні; визначення кількісних характеристик виявлених кібер-ризиків, включаючи ймовірність настання, можливі наслідки та особливі характеристики даних ризиків, які варто враховувати при їх прийнятті на страхування; розробка рекомендацій розрахунку страхового тарифу для страхових кібер-ризиків; визначення критичних сфер, для яких страхування кібер-ризиків є пріоритетним.

Таким чином, результатом запровадження пропонованих змін має стати вдосконалення інституційно-правової бази, пов'язаної зі страхуванням кібер-ризиків, її гармонізація з європейським законодавством у рамках вступу до ЄС, створення ефективних механізмів взаємодії між учасниками страхових відносин та підняття рівня національної кібербезпеки завдяки дієвому алгоритму управління ризиками кіберпростору України.

3.3. Дорожня карта впровадження та розвитку страхування кібер-ризиків в Україні

Світова пандемія COVID-19 стала основою глобального тренду цифровізації усіх сфер життя та діяльності людства. Проте для України цифровізація набула особливого значення з початком російського повномасштабного вторгнення в Україну. Драйверами підвищення пріоритетності даного напрямку стали внутрішня та зовнішня міграція населення, релокація та реорієнтація бізнесу, зміна стратегічних планів розвитку сфер держави в рамках подання заяви на вступ до ЄС, а також збільшення кількості масштабних кібератак.

Задля створення стратегії розширення сфер використання цифрових технологій та інновацій 22 грудня 2023 року Колегія Міністерства освіти і науки України опублікувала Дорожню карту використання науки, технологій та інновацій (НТІ) для досягнення Цілей сталого розвитку[18]. В даному документі описані положення про запровадження наукових результатів досліджень та розробок, можливих ризиків і проблем та індикаторів контролю їх виконання в ключових сферах цифрового розвитку держави. Вектор удосконалення кожної сфери сформований у відповідних місіях:

- цифровізація суспільства;
- ресурсоефективна економіка та альтернативна енергетика;
- раціональне природокористування та циркулярна економіка;
- здоров'я нації;
- нові речовини, матеріали, індустріальні технології;
- безпечне харчування.

Важливою особливістю даного документа є узагальнення вже наявних стратегій та дорожніх карт усіх сфер розвитку України, що потенційно спрощує процес їх цифровізації та збільшує спектр доступних інновацій, які можуть бути залучені в них. Відповідно, положення Дорожньої карти НТІ підтверджують намір розширити використання цифрового інструментарію українськими державними та приватними закладами, що зумовлює майбутнє підвищення кількості та розмаїття кіберзагроз, притаманних вказаним сферам.

Як було визначено, страхування кібер-ризиків є інструментом мінімізації потенційних наслідків від наявних та нових кіберзагроз. Однак в Україні даний вид страхування поки що набув фрагментарного поширення, тому потребує якісно нового підходу до розвитку. Іноземна практика поширення страхування кібер-ризиків є аналогічною – в той час, коли експерти на науковці продовжують досліджувати його актуальність, багато компаній вже включили цей вид страхування до портфоліо, тим самим підтвердивши його необхідність [142].

Загальноприйнятим інструментом поетапного планування розвитку певного нового напрямку є розробка дорожньої карти. Особливістю кібер-ризиків є

постійне збільшення типів кіберзагроз та захисту від них, що водночас означає їх тимчасовий характер. Тому дорожня карта запровадження та розвитку страхування кібер-ризиків має охоплювати короткостроковий період (до року) з обов'язковим оновленням після закінчення вказаного терміну, що включатиме аудит і оцінку проведених етапів та актуалізацію наступних завдань.

Таблиця 3.3

Дорожня карта запровадження та розвитку страхування кібер-ризиків в Україні

Етап та його учасники	**Місяць** / **Заходи**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Підготовчий: СК, вітчизняні та міжнародні експертні організації, регулятор, іноземні СК, урядові комітети	Вивчення іноземної практики розвитку страхування кібер-ризиків; досвіду та кейсів просування даних послуг іноземними СК	■	■										
	Дослідження інституційно-правової бази, яка пов'язана зі страхуванням кібер-ризиків, Стратегій цифрового розвитку та кібербезпеки іноземних країн	■	■	■									
	Адаптація іноземного / міжнародного законодавства під українські реалії, визначення місця кібер-ризиків у системі страхування, внесення змін до законодавства		■	■	■	■							
	Розробка страхового продукту та маркетингової стратегії просування страхування від кібер-ризиків	■	■	■	■	■	■	■	■				
Організаційний: СК, експертні організації, консультанти у сфері кібербезпеки, регулятор	Співпраця СК із фахівцями у сфері кібербезпеки та регулятором з метою розробки уніфікованої моделі оцінки втрат від кібератак			■	■	■							
	Розробка алгоритму взаємодії СК з експертними організаціями в оцінці стану потенційних страхувальників та їх прийнятті на страхування			■	■	■	■	■					
	Створення моделі підбору рекомендацій для покращення кібербезпеки страхувальників				■	■	■	■	■				
Реалізаційний: СК, експертні організації, регулятор, страхувальники	Включення послуг страхування кібер-ризиків до портфоліо зацікавлених СК			■	■	■	■	■	■				
	Запуск маркетингових активностей та інформування населення									■	■	■	■
	Початок продажу послуг										■	■	■

Джерело: складено автором

На основі проведеного аналізу закордонного досвіду розвитку страхування кібер-ризиків та наявних факторів стимулювання і стримування розвитку вказаного сектору вітчизняного страхового ринку, запропонована Дорожня карта запровадження та розвитку страхування кібер-ризиків в Україні (далі Дорожня карта), відображена в Таблиці 3.3.

Ключовими етапами запропонованої Дорожньої карти є:

- підготовчий, що включає аналіз наявної світової практики, розгляд міжнародного та іноземного інституційно-правового забезпечення і його адаптація до українського страхового ринку, підготовка маркетингового плану просування продукції в Україні;
- організаційний, що охоплює створення моделі взаємодії учасників страхових відносин, розробку алгоритмів та механізмів оцінки потенційних страхувальників, покращення стану їхньої кібербезпеки;
- реалізаційний, що описує інформативні заходи роботи з фізичними та юридичними особами, включення нових послуг в портфоліо страховиків, маркетингові активності просування послуг, фактичний початок продажу нових продуктів страхування кібер-ризиків.

Відповідно до запропонованої Дорожньої карти, підготовчий етап запровадження та розвитку страхування кібер-ризиків в Україні включає такі заходи:

1. Вивчення закордонної практики розвитку страхування кібер-ризиків, що передбачає залучення іноземних страховиків з метою вивчення наявних підходів, кейсів та особливостей у розробці, просуванні та управлінні відповідними страховими продуктами на різних ринках. Вітчизняні страховики, регулятор та урядові комітети мають визначити найкращі практики розвитку страхування кібер-ризиків, які доцільно застосовувати на українському страховому ринку.

Аналітична робота, здійснена в межах даних заходів, спрямована на формування проєкту завдань, цілей та інструментів, необхідних для досягнення мети розвитку страхування кібер-ризиків в Україні.

2. Дослідження інституційно-правової бази, пов’язаної зі страхуванням кібер-ризиків, та Стратегій цифрового розвитку або кібербезпеки іноземних країн, тобто виявлення характерних особливостей регулювання даної сфери, а також визначення закріпленості мети страхування кібер-ризиків в іноземних стратегічних планах.

3. Адаптація закордонного / міжнародного законодавства під українські реалії, визначення місця кібер-ризиків в системі страхування, внесення змін до законодавства, що означає гармонізацію та вдосконалення української інституційно-правової бази у сфері страхування кібер-ризиків.

Задля виконання заходів 1–3 доцільно реалізувати вектори вдосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні, запропоновані в пункті 3.1.

4. Розробка страхового продукту та маркетингової стратегії просування страхування від кібер-ризиків кожним страховиком, що передбачає комплексний процес, який має наступні складові: аналіз цільової аудиторії, тобто визначення потреб потенційних страхувальників, особливостей їхньої діяльності в кіберпросторі, рівень їх захищеності на основі проведених ринкових замірів чи опитувань; створення страхового продукту, що задовольнятиме попит потенційних страхувальників; вибір каналів продажу, тобто визначення найбільш ефективних та актуальних каналів взаємодії з потенційними страхувальниками; дослідження та розробка стратегії впізнаваності продукту і бренду, тобто створення PR-кампанії, що буде забезпечувати обізнаність про новий продукт страховика, його особливості та переваги.

До організаційного етапу Дорожньої карти відносимо такі заходи:

1. Співпраця страховиків з фахівцями у сфері кібербезпеки та регулятором з метою розробки уніфікованої моделі оцінки втрат від кібератак, спрямованої на уніфікацію підходу до визначення втрат від кіберінцидентів з метою подальших розрахунків страхових тарифів та інших похідних значень. У межах цього заходу також варто враховувати закордонну практику оцінки втрат

від кібер-ризиків, що передбачає залучення іноземних страховиків та міжнародних експертів у сфері кібербезпеки.

2. Розробка алгоритму взаємодії страховиків з експертними організаціями в оцінці стану потенційних страхувальників та їх прийнятті на страхування, що означає створення ефективного механізму визначення доцільності прийняття на страхування кібер-ризиків потенційних страхувальників.

Використання запропонованих у пункті 1.3 пропозицій щодо оцінки втрат від реалізованих кібер-ризиків та алгоритму взаємодії страховиків з експертними організаціями є доцільним кроком для виконання заходів 1 та 2 даного етапу;

3. Створення моделі підбору рекомендацій для покращення кібербезпеки страхувальників, що означає визначення місця та функцій експертів у сфері кібербезпеки при процесі страхування кібер-ризиків.

Реалізаційний етап Дорожньої карти передбачає проведення таких заходів:

1. Включення послуг страхування кібер-ризиків до портфоліо зацікавлених страховиків передбачає інтеграцію нових страхових продуктів у стратегію продажу страхових компаній.

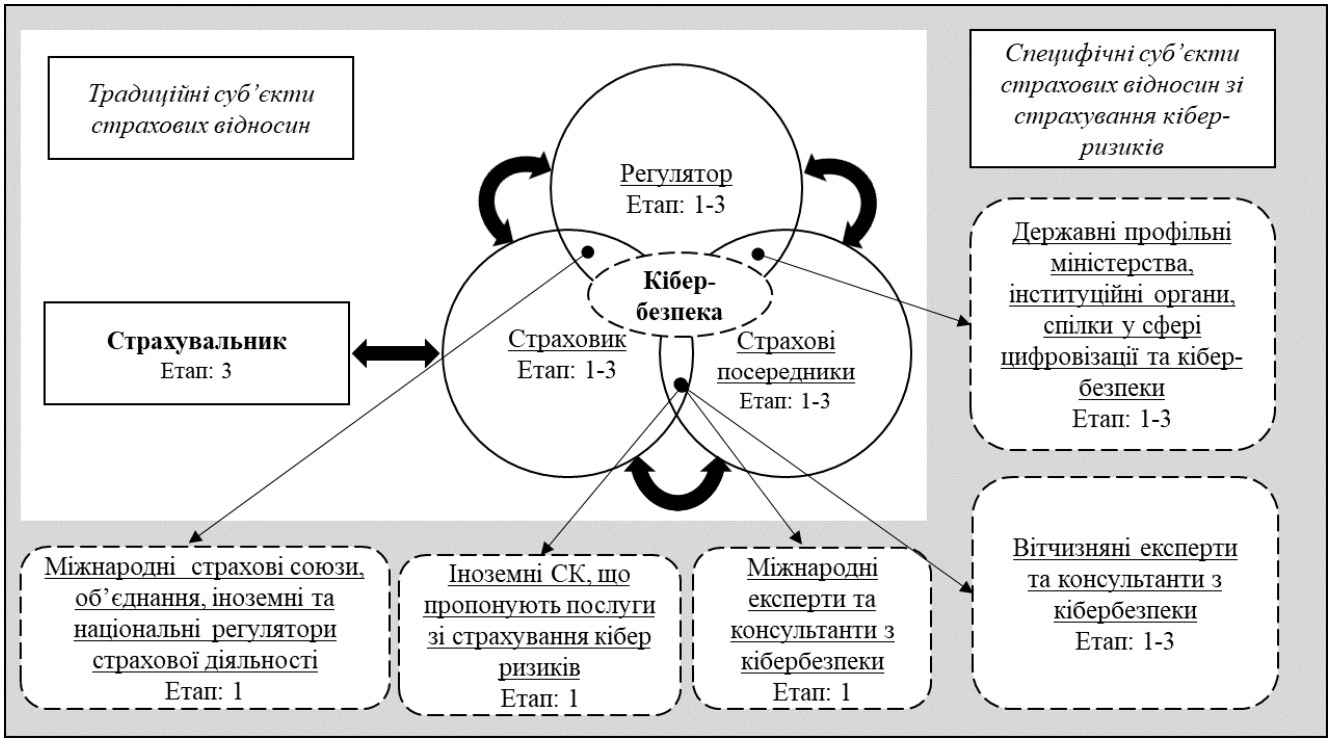
2. Запуск маркетингових активностей та інформування населення означає реалізацію розробленої маркетингової стратегії на запланованих умовах;

3. Початок продажу послуг страхування кібер-ризиків, тобто повноцінний результат реалізації запропонованої Дорожньої карти.

Варто зауважити, що описаний комплекс заходів Дорожньої карти запровадження та розвитку страхування кібер-ризиків в Україні побудований на основі клієнтоцентричного підходу.

Відповідно до класифікації EY, найбільш відповідною роллю страховика в страхуванні кібер-ризиків буде «оркестратор», тобто страхувальник зможе отримати консультаційну та спеціалізовану допомогу у сфері кібербезпеки, інформацію про наявні та актуальні для нього кіберзагрози й персоналізовану послугу зі страхування кібер-ризиків безпосередньо від страховика [171].

З огляду на запропонований календар, бачимо, що всі учасники страхових відносин залучені на етапах до фактичного початку продажу послуг зі страхування кібер-ризиків. На перетині інтересів традиційних учасників виникають специфічні суб'єкти, які мають експертизу у сфері кібербезпеки або досвід розвитку страхування кібер-ризиків (рис. 3.10).



Примітка. Етапи Дорожньої карти запровадження та розвитку страхування кібер-ризиків в Україні: 1 – підготовчий, 2 – організаційний, 3 – реалізаційний.

Рисунок 3.10. Клієнтоценрична система взаємодії суб'єктів страхування кібер-ризиків при запровадженні та розвитку страхування кібер-ризиків в Україні

Джерело: складено автором

Для аналізу успішності виконання завдань Дорожньої карти необхідно проводити індикативне оцінювання після закінчення 12-місячного терміну її дії. Оцінні показники формуються на основі мети створення Дорожньої карти, що полягає у запровадженні та розвитку страхування кібер-ризиків в Україні, покращенні рівня кібербезпеки фізичних і юридичних осіб та підвищенні рівня їх інформованості про наявні кіберзагрози. До переліку оцінних індикаторів відносимо:

1. Індикатор 1. Приріст рівня обізнаності населення щодо кіберзагроз. Для його визначення спочатку потрібно з'ясувати рівень обізнаності населення щодо кіберзагроз. Даний показник визначає ступінь розуміння респондентів актуальних кіберзагроз сучасності, можливих наслідків та варіантів їх уникнення чи мінімізації. Для відстеження тренду коливань оптимально проводити щомісячні заміри даного показника, однак в умовах невизначеності та обмеженості ресурсів заміри мають бути проведені мінімум 3 рази: перед початком інформування населення (6-й місяць), на другий місяць після початку інформування (10-й місяць), після закінчення терміну дії Дорожньої карти (після 12-го місяця). Така періодичність дасть змогу простежити органічний рівень обізнаності, його зміну на початку інформування та після завершення всіх завдань. Заміри відбуваються через опитування у вигляді розгорнутих тестувань за темою кібербезпеки. Відповіді оцінюються в 0 (некоректна відповідь) або 1 бали (коректна відповідь). Розрахунок рівня обізнаності населення щодо кіберзагроз обчислюється як :

$$K = \frac{\bar{C}}{N}, \tag{3.2}$$

де K – рівень обізнаності населення щодо кіберзагроз;

$\bar{C}$ – середнє значення кількості коректних відповідей на тестові запитання усіх респондентів;

N– кількість тестових запитань опитування.

Відповідно, приріст рівня обізнаності населення щодо кіберзагроз відображає зміну показника за обраний період. У межах Дорожньої карти необхідно порівнювати значення рівня обізнаності перед початком інформування населення про кіберзагрози та після закінчення всіх запланованих завдань:

$$\Delta K = K_E - K_S, \tag{3.3}$$

де ΔK – приріст рівня обізнаності населення щодо кіберзагроз;

K_E – рівень обізнаності населення щодо кіберзагроз на кінець періоду;

K_S – рівень обізнаності населення щодо кіберзагроз на початок періоду.

Відповідно до даних Eurostat у країнах Європейського Союзу на початку роботи програм із цифровізації бізнесу та суспільства у 2015−2019 роках щорічний темп приросту цифрової грамотності населення становив від 0,3 в.п. до 2,4 в.п., а середньозважене значення становило 1,8 в.п. [143]. Спираючись на дане значення, приймаємо річний приріст 1,8 в.п. та піврічний приріст 0,9 в.п. як базу для порівняння, оскільки розвиток напрямку кібербезпеки в Україні відповідає рівню розвитку цифровізації в ЄС у 2015 році.

2. Індикатор 2. Частка страховиків, які пропонують послуги страхування кібер-ризиків. Вказаний індикатор визначає фактичну частку страховиків, що мають продукти страхування кібер-ризиків у своєму портфоліо після закінчення терміну дії Дорожньої карти (після 12 місяця), в кількості страховиків, які планували запровадити даний продукт на початковому етапі дії Дорожньої карти:

$$IC_T = \frac{IC_A}{IC_P} * 100\%, \quad (3.4)$$

де IC_T – частка страховиків, які пропонують послуги страхування кібер-ризиків;

IC_A – фактична кількість страховиків, які пропонують послуги страхування кібер-ризиків;

IC_P– планова кількість страховиків, які пропонують послуги страхування кібер-ризиків.

Планове значення кількості страховиків, які пропонують послуги страхування кібер-ризиків, формується на етапі співпраці страховиків із регулятором і урядовими комісіями, коли зіставляються національні цілі з можливостями страхових компаній у даній сфері. Прийнятним рівнем виконання Індикатора 2 є значення >=95%, оскільки в Дорожній карті використовується короткотермінове планування, для якого допустимим є відхилення в межах 5%.

3. Індикатор 3. Загальна частка покриття кібер-ризиків. Даний індикатор відображає рівень страхового захисту від актуальних для України кібер-ризиків враховуючи доступні пропозиції всіх українських страховиків:

$$C_T = \frac{R_U}{R_T} * 100\%, \quad (3.5)$$

де C_T – загальна частка покриття кібер-ризиків;

R_U – кількість унікальних кібер-ризиків, страхування яких пропонують страховики;

R_T– загальна кількість унікальних кібер-ризиків, що актуальні для України.

Оптимальним значенням є покриття всіх кібер-ризиків, які існують в українському просторі. Однак через новизну даного виду страхування близько 10−15% ризиків можуть не ввійти в покриття на початковому етапі розвитку, проте будуть додані до портфоліо в майбутньому [221].

4. Індикатор 4. Індивідуальна частка покриття кібер-ризиків. На відміну від Індикатора 3, даний індикатор відображає середній рівень страхового захисту від актуальних для України кібер-ризиків окремих страховиків:

$$C_I = \frac{\overline{R_U}}{R_T} * 100\%, \tag{3.6}$$

де C_I – індивідуальна частка покриття кібер-ризиків;

$\overline{R_U}$ – середня кількість унікальних кібер-ризиків, страхування яких пропонують окремі страховики;

R_T– загальна кількість унікальних кібер-ризиків, що актуальні для України.

Порогове значення очікується на нижчому рівні, ніж Індикатор 3, оскільки страховики обирають різні стратегії розширення послуг, пов'язаних з кібер-ризиками, як то: моно-продажі, мульти-продажі, крос-продажі в класичних чи цифрових каналах просування послуг [66]. Тому через нерівномірність пропозицій страховиків, опираючись на досвід європейських страховиків, оптимальне значення Індикатора 4 відповідає рівню більше 65%.

5. Індикатор 5. Відношення фактичного обсягу валових премій зі страхування кібер-ризиків до запланованого обсягу валових премій зі страхування кібер-ризиків. Даний показник відображає загальний рівень виконання плану реалізації вказаних послуг:

$$P_T = \frac{P_A}{P_P} * 100\%, \tag{3.7}$$

де P_T – відношення фактичного обсягу валових премій зі страхування кібер-ризиків до запланованого обсягу валових премій зі страхування кібер-ризиків;

P_A – фактичне значення валових премій страхування кібер-ризиків;

P_P – планове значення валових премій страхування кібер-ризиків.

Планове значення валових премій страхування кібер-ризиків формується на основі індивідуальних очікувань страховиків щодо обсягу продажів, так як цінова та продуктова політика може бути різною. Тому на організаційному етапі Дорожньої карти робоча група формує загальний плановий показник, що складається з суми планів страховиків (P_P), та після завершення терміну дії Дорожньої карти за аналогічним підходом формує загальний фактичний показник (P_A).

Ознакою ефективності комплексного підходу до розвитку страхування кібер-ризиків є значення Індикатора 5 >=95%, оскільки при короткотерміновому плануванні показників інноваційних напрямків допустимі відхилення в межах 5%.

6. Індикатор 6. Приріст частки валових страхових премій страхування кібер-ризиків у загальних валових преміях. Даний показник допоможе нівелювати ефект коливань страхового ринку через зовнішні ефекти:

$$\Delta P = \frac{P_{A2}}{P_{I2}} - \frac{P_{A1}}{P_{I1}}, \quad (3.8)$$

де ΔP – приріст частки валових страхових премій страхування кібер-ризиків у загальних валових преміях;

P_{Ai} – фактичне значення валових премій страхування кібер-ризиків (i: 1- на початок періоду, 2 – на кінець періоду);

P_{Ii} – фактичне значення валових премій страхування (i: 1- на початок періоду, 2 – на кінець періоду).

Проте через невисоку частку премій зі страхування кібер-ризиків на початковому етапі та короткий термін для відстежування трендів достатнім буде закладення позитивного приросту в цей період, тобто >0.

7. Індикатор 7. Зростання кількості випадків кібершахрайства. Даний показник відображає зміну стійкості населення до методів соціальної інженерії, наслідками якого можуть бути крадіжка паролів, акаунтів, вимагання коштів та

блокування технічного обладнання. Розрахунок показника відображає порівняння кількості випадків кібершахрайства на кінець та на початок періоду:

$$G_T = \frac{G_2}{G_1} * 100\%, \quad (3.9)$$

де G_T – зростання кількості випадків кібершахрайства;

G_i – кількість випадків кібершахрайства (і: 1 – на початок періоду, 2 – на кінець періоду).

Станом на жовтень 2021 року, згідно з даними опитування щодо інформованості цільових аудиторій про основні аспекти кібербезпеки, 41% респондентів стикався з випадками кібершахрайства [26]. Однак у травні 2023 року лише крадіжка облікових записів у соціальних мережах траплялась уже в 57% опитаних [27], що свідчить про поглиблення проблем, пов'язаних з ризиками кібершахрайства.

Тому зменшення кількості випадків кібершахрайства має стати ефективним результатом виконання завдань Дорожньої карти, що відповідає значенню Індикатора 7<100%.

8. Індикатор 8. Зростання кількості кібератак, зареєстрованих в Україні. Означений у Дорожній карті комплекс заходів спрямований не просто на запровадження та розвиток страхування кібер-ризиків, а й на підвищення рівня кібербезпеки фізичних та юридичних осіб у цілому через заходи інформування про кіберзагрози та посилення кіберзахищеності. Тому даний показник відображає зміну кількості кібератак, спрямованих на об'єкти в Україні:

$$A_T = \frac{A_2}{A_1} * 100\%, \quad (3.10)$$

де A_T – зростання кількості кібератак, зареєстрованих в Україні;

A_i – кількість кібератак, зареєстрованих в Україні (і: 1- на початок періоду, 2 – на кінець періоду).

Офіційну інформацію про зареєстровані кібератаки регулярно публікує Державна служба спеціального зв'язку та захисту інформації України, тому для уніфікації підходу при обчисленні Індикатора 8 варто використовувати дане

джерело [36]. Ефективним значенням Індикатора 8 буде зростання <100%, оскільки це означитиме зменшення реалізованих кібератак в Україні.

Таким чином, ознакою ефективності заходів Дорожньої карти запровадження та розвитку страхування кібер-ризиків в Україні буде виконання або перевиконання всіх вищезазначених цільових індикативних показників, залежно від особливостей розрахунку (висхідний чи низхідний вектор досягнення цільового значення) кожного окремого Індикатора (Таблиця 3.4).

Таблиця 3.4

Індикатори та їх цільові значення Дорожньої карти запровадження та розвитку страхування кібер-ризиків в Україні

Індикатор	**Назва**	**Цільове значення**	**Вектор досягнення цільового значення**
Індикатор 1	Приріст рівня обізнаності населення щодо кіберзагроз	>=0,9	Висхідний
Індикатор 2	Частка страховиків, які пропонують послуги страхування кібер-ризиків	>=95%	Висхідний
Індикатор 3	Загальна частка покриття кібер-ризиків	>=85%	Висхідний
Індикатор 4	Індивідуальна частка покриття кібер-ризиків	>=65%	Висхідний
Індикатор 5	Відношення фактичного обсягу валових страхових премій зі страхування кібер-ризиків до запланованого обсягу валових страхових премій зі страхування кібер-ризиків	>=95%	Висхідний
Індикатор 6	Приріст частки валових страхових премій страхування кібер-ризиків у загальних валових преміях	>0	Висхідний
Індикатор 7	Зростання кількості випадків кібершахрайства	<100%	Низхідний
Індикатор 8	Зростання кількості кібератак, зареєстрованих в Україні	<100%	Низхідний

Джерело: складено автором

Виконання цільових значень індикаторів може бути оцінене в 0, 1 або 2 бали. Невиконання будь-якого з індикаторів оцінюється в 0 балів. Оскільки метою Дорожньої карти є популяризація послуг страхування кібер-ризиків та підвищення рівня кібербезпеки в Україні, приймаємо Індикатор 3 (загальна частка покриття кібер-ризиків) та Індикатор 6 (приріст частки валових страхових премій

страхування кібер-ризиків у загальних валових преміях) як більш значущі, тобто їх виконання оцінюється в 2 бали. Виконання Індикаторів 1–2, 4–5, 7–8 оцінюється в 1 бал.

Отримані результати підрахунку робоча група, визначена на початковому етапі створення Дорожньої карти, вносить в оцінну форму виконання цільових значень індикаторів після завершення відведеного терміну дії усіх завдань Дорожньої карти (Додаток И).

Відповідно значення суми індикаторів може бути в межах [0; 10] балів. Отримане значення відповідатиме оцінному рівню виконання мети Дорожньої карти:

- критичний, що відповідає значенням [0; 5], тобто виконання<=50% завдань. Даний рівень відображає наявність проблем в обраній стратегії запровадження та розвитку страхування кібер-ризиків, співпраці між суб'єктами страхових відносин та діалозі з потенційними страхувальниками;
- середній, що відповідає значенням [6; 7], означає відставання значень кількох індикаторів та сигналізує про проблеми, пов'язані зі сферами, на розвиток яких варто спрямувати більше ресурсів, ніж було заплановано в першому варіанті Дорожньої карти;
- високий [8; 9], що відображає виконання більшості завдань Дорожньої карти, однак підкреслює наявність певних перешкод розвитку страхування кібер-ризиків (тобто невиконання одного значущого або двох простих індикаторів), виправлення яких дасть змогу успішно розвивати обраний напрямок;
- оптимальний рівень [10], що свідчить про коректність та ефективність вибору стратегії заходів у Дорожній карті, їх правильне позиціонування та просування. Такий рівень буде свідчити про достатній попит на дані послуги страхування та наявність страховиків, що можуть його задовольнити.

Отже, задля ефективного розвитку страхування кібер-ризиків в Україні варто враховувати наявні фактори стримування та стимулювання. Так, ефективним інструментом є розробка Дорожньої карти запровадження та розвитку вказаного виду страхування, що передбачає поетапне проведення

підготовчих, організаційних та реалізаційних заходів, результатом яких є забезпечення потреб страхувальників у захисті від загроз кіберпростору за допомогою страхових продуктів. Оскільки Дорожня карта пропонує комплексний підхід розвитку страхування кібер-ризиків в Україні, оцінку її ефективності доцільно проводити на основі запропонованих індикаторів, що відображають цільові значення результативних показників даного виду страхування та інших супутніх аспектів.

ВИСНОВКИ ДО РОЗДІЛУ 3

На основі проведеного аналізу перспектив розвитку страхування кібер-ризиків в Україні було зроблено наступні висновки:

1. Виявлено, що інституційно-правове забезпечення страхування кібер-ризиків в Україні потребує покращення, оскільки через вплив пандемії COVID-19 та повномасштабного вторгнення Російської Федерації до України процес розвитку даної сфери сповільнився. На основі іноземного досвіду розвитку інституційно-правової бази страхування кібер-ризиків визначено, що найбільш ефективним підходом до розвитку вказаного напрямку є використання клієнтоцентричної моделі, за якою на основі синергії вітчизняних та іноземних представників урядових органів, регуляторів, страховиків, міжнародних організацій та експертів у сфері кібербезпеки і захисту персональних даних відбувається задоволення потреб страхувальників щодо безпеки в кіберпросторі. Тому запропоновано три основних вектори вдосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні, а саме: розробка стратегії розвитку страхування кібер-ризиків; запровадження або гармонізація законодавства; розробка клієнтоцентричної моделі квантифікації кібер-ризиків.

2. Визначено фактори стримування розвитку страхування кібер-ризиків в Україні, що включають: середній рівень цифрової грамотності; середній рівень фінансової інклюзії; низький рівень економічної активності; недостатній рівень розвитку інституційно-правового забезпечення; переміщення IT-компаній за кордон або в межах України, еміграція кваліфікованих фахівців; глобальна невизначеність, економічна нестабільність.

3. Виявлено фактори стимулювання розвитку страхування кібер-ризиків в Україні, що полягають у цифровізації усіх сфер життя; посиленні кіберзлочинності, включаючи фінансову та інформаційну; розвитку мобільних фінансових сервісів і технологій; глобальному тренді розвитку страхування кібер-ризиків; наявності досвідчених спеціалістів у сфері кібербезпеки; державному фокусі на забезпеченні високого рівня кібербезпеки.

4. Розроблено Дорожню карту запровадження та розвитку страхування кібер-ризиків в Україні, що включає проведення трьох етапів досягнення Цілі Стратегії кібербезпеки України: підготовчий етап, що передбачає аналіз практики розвитку даного виду страхування страховиками за кордоном, огляд міжнародних та іноземних інституційно-правових актів, їх адаптацію до умов українського страхового ринку, а також розробку маркетингової стратегії для популяризації відповідних страхових продуктів; організаційний етап, що передбачає створення алгоритму взаємодії між учасниками страхових відносин, розробку механізмів оцінки кібер-ризиків потенційних страхувальників та типових шляхів покращення рівня захищеності від загроз кіберпростору страхувальників за допомогою використання інструментів експертів у сфері кібербезпеки; реалізаційний етап, що передбачає включення продуктів страхування кібер-ризиків до портфоліо страхових компаній, проведення маркетингових заходів для просування вказаних послуг, а також фактичний запуск продажу нових продуктів страхування кібер-ризиків.

5. Запропоновано Індикатори ефективності Дорожньої карти запровадження та розвитку страхування кібер-ризиків в Україні та їх цільові значення, що відображають зміну стану даного сегменту страхового ринку та дотичних показників у сфері кібербезпеки після реалізації запланованого у Дорожній карті комплексу заходів. Індикатори відображають широкий спектр даних про зміни у наступних напрямках, що пов’язані зі страхуванням кібер-ризиків: кількісні та якісні зміни на страховому ринку зі страхування кібер-ризиків; зміна обсягу покриття кібер-ризиків; зміна обізнаності населення про кіберзагрози; зміна кількості кіберінцидентів.

ВИСНОВКИ

У дисертаційній роботі поглиблено теоретико-методологічні основи страхування кібер-ризиків в умовах цифрової економіки, розроблено методичні підходи та практичні рекомендації запровадження та розвитку вказаного виду страхування в Україні з метою забезпечення захисту економічних суб'єктів від загроз кіберпростору. Проведене дослідження стало фундаментом для формулювання наступних висновків, які відображають виконання поставлених завдань дисертації.

1. Розкрито економічну природу кібер-ризиків в умовах цифрової економіки на основі зіставлення процесу становлення поняття «цифрова економіка» і трансформації ризиків під впливом цифровізації та виявлено спіральну модель еволюції дефініції «кібер-ризик», яка акцентує увагу на тісному взаємозв'язку проникнення цифрових технологій в економічну діяльність суб'єктів і характер загроз, що вони становлять. Унаслідок дослідження наведено вдосконалене визначення поняття «кібер-ризику» як константи глобальних процесів цифровізації економіки (з урахуванням джерел виникнення загроз та характеру прояву наслідків їх реалізації). Узагальнено і систематизовано класифікацію кібер-ризиків на основі фасетного підходу за локалізацією, видимістю, характером наслідків, формою прояву, розміром і ймовірністю настання та доповнено такими ознаками, як: рівень економіки, страхувальність, сектор реалізації, що також включає розширений перелік кібер-ризиків оборонного сектору, які сформувались під впливом гібридної війни в Україні.

2. Визначено сутність поняття «страхування кібер-ризиків» на основі компаративного аналізу компонентів трактувань дефініцій «кіберстрахування» та «страхування кібер-ризиків» з доведенням їх тотожності. Виявлено детермінанти функціонування страхування кібер-ризиків, що відображають вплив цифровізаційних процесів на економічних суб'єктів і їхню діяльність, до яких входять: мета, об'єкти, суб'єкти, особливості, принципи, позитивні та негативні аспекти запровадження даного виду страхування, що дало змогу розширити та

вдосконалити визначення поняття «страхування кібер-ризиків». Завдяки використанню багатоступеневої структури безпеки економічних суб'єктів обґрунтовано позитивну роль застосування страхування кібер-ризиків як інструмента управління ризиком, що впливає на посилення фінансової безпеки страхувальників, оскільки наслідком реалізованого кібер-ризику є прямі або непрямі втрати, що в кінцевому вигляді набувають вияву втраченої економічної вигоди.

3. Виявлено характерні особливості страхових послуг у сфері страхування кібер-ризиків через застосування декомпозиції процесу реалізації послуги страхування кібер-ризиків та запропоновано: поетапний фреймворк розробки продукту страхування кібер-ризиків, що відображає імплементацію методологічних основ функціонування вказаного виду страхування у фактичний страховий продукт; алгоритм співпраці страховика та потенційного страхувальника при ухваленні рішення про укладання договору страхування кібер-ризиків, що враховує оптимальний метод прийняття кібер-ризиків на страхування з максимізацією користі для всіх суб'єктів страхових відносин задля гарантування прийнятного рівня їхньої фінансової безпеки; класифікацію груп кібер-ризиків для формування страхового покриття з визначенням доцільної форми страхового продукту (самостійного або комплексного). Використовуючи підсумки проведеного аналізу, розрізнено поняття «послуга страхування кібер-ризиків» та «продукт страхування кібер-ризиків», відповідно визначено, що послуга є вираженням комплексу визначених дій страховика, що вказані в зафіксованих умовах продукту.

4. Здійснено періодизацію становлення та розвитку глобального ринку страхування кібер-ризиків: підготовчий етап, етап зародження, етап створення самостійних продуктів страхування кібер-ризиків, етап зростання обізнаності про кібер-ризики, етап популяризації, сучасний етап активного розвитку. Зі свого боку виявлення специфічних особливостей кожного етапу розвиту ринку страхування кібер-ризиків є основою для проведення аналізу потенціалу росту даного сегменту страхового ринку в середньостроковій перспективі, оскільки

дозволяє вчасно відзначати його перехід на новий етап розвитку через розширення наявних унікальних характеристик. Виділено драйвери зростання обсягу глобальних валових премій страхування кібер-ризиків, які є індикатором розвитку ринку страхування кібер-ризиків, а саме: збільшення обсягу покриття населення мобільним зв'язком та суми втрат від кіберінцидентів на основі проведеного економетричного моделювання.

5. Встановлено, що використання економічними суб'єктами страхування кібер-ризиків є одним із ефективних інструментів комплексу заходів, спрямованих на досягнення глобальних Цілей сталого розвитку завдяки розвитку системи моніторингу ризиків страхувальників, підвищенню рівня їхньої цифрової грамотності, зниження рівня корупції, шахрайства та відмивання коштів, а також посиленню міжнародних партнерських зв'язків страховиків з фахівцями у сфері кібербезпеки. На основі виявлених локальних показників, що впливають на розвиток ринку страхування кібер-ризиків, а саме, покриття населення мобільним зв'язком та суми втрат від кіберінцидентів, запропоновано регіональний Індекс необхідності розвитку страхування кібер-ризиків, за яким отримано відповідний рейтинг доцільності розвитку вказаного виду страхування, що відображений наступним низхідним порядком: Східна Азія й Тихоокеанські країни, Європа і Центральна Азія, Північна Америка, Південна Азія, Латинська Америка і Карибський басейн, Субсахарська Африка, Близький Схід і Північна Африка.

6. Проведено діагностування сучасного стану вітчизняного ринку страхування кібер-ризиків, результати якого свідчать про низький рівень розвитку даного сегменту страхового ринку в Україні, оскільки пенетрація страховиків, які пропонують покриття кібер-ризиків, не перевищує 2% у 2023 р. Використовуючи запропонований Індекс потенціалу запровадження страхування кібер-ризиків вітчизняними страховиками, що формується на основі результативних показників страхової діяльності, а саме: приросту валових страхових премій рік до року, обсягу активів, загального рівня виплат, частки валових премій страхування фінансових ризиків у загальних валових преміях та частки валових премій страхування майна у загальних валових преміях, на основі кластерного аналізу

було визначено чотири групи українських страхових компаній, що мають різну спроможність запровадження страхування кібер-ризиків – з оптимальним потенціалом, з високим потенціалом, з середнім потенціалом та з низьким потенціалом. Наявність позитивних результатів потенціалу запровадження страхування кібер-ризиків з одночасним низьким рівнем розвитку даного виду страхування на національному рівні свідчить про існування перепон для його розвитку на вітчизняному страховому ринку.

7. Обґрунтовано наявність та охарактеризовано стимулюючі та стримуючі фактори розвитку страхування кібер-ризиків в Україні, що виникли в умовах нової реальності функціонування цифрової економіки під впливом наслідків глобальної COVID-19 та повномасштабного вторгнення Російської Федерації в Україну. Розглянуті особливості стали основою формування стратегічної матриці впливу, яка забезпечує подолання стримуючих (недостатній рівень розвитку інституційно-правового забезпечення, середній рівень цифрової грамотності та фінансової інклюзії, низький рівень економічної активності, переміщення IT-компаній, еміграція кваліфікованих фахівців, глобальна невизначеність та економічна нестабільність) завдяки активізації стимулюючих факторів, а саме: державний фокус на забезпеченні високого рівня кібербезпеки, глобальний тренд розвитку страхування кібер-ризиків, наявність вітчизняних досвідчених фахівців у сфері кібербезпеки, розвиток мобільних фінансових сервісів і технологій, цифровізація усіх сфер життя.

8. Розроблено комплекс заходів, які доцільно запровадити для вдосконалення інституційно-правового забезпечення страхування кібер-ризиків в Україні, що включає: розробку стратегії розвитку страхування кібер-ризиків на вітчизняному ринку, запровадження або гармонізацію українського законодавства відповідно до міжнародних вимог у рамках початих 2023 року переговорів щодо вступу України до Європейського Союзу; розробку моделі квантифікації кібер-ризиків. Завдяки синергетичному ефекту розвитку вказаних векторів інституційно-правового забезпечення страхування кібер-ризиків в Україні доцільно реалізувати на основі клієнтоцентричної моделі страхування, що

передбачає отримання страхувальником того рівня безпеки (включаючи фінансову та кібербезпеку), яка була зафіксована в умовах страхової угоди між страховими суб'єктами.

9. Наслідком поглибленого дослідження теоретичних та практичних аспектів страхування кібер-ризиків у глобальному та вітчизняному контексті є авторська пропозиція запровадження та розвитку вказаного виду страхування в Україні, представлена у вигляді дорожньої карти терміном на рік. Ключовими етапами запропонованої дорожньої карти є підготовчий, організаційний, та реалізаційний етапи, ефективність втілення яких визначається на основі розрахунку оцінних індикаторів, що відображають широкий спектр даних про зміни у напрямках, пов'язаних зі страхуванням кібер-ризиків, а саме: кількісні та якісні зміни на страховому ринку зі страхування кібер-ризиків; зміна обсягу покриття кібер-ризиків; зміна обізнаності населення з кіберзагрозами; зміна кількості кіберінцидентів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамова А. С. Трансформаційна природа операційних ризиків комерційних банків. *Проблеми сучасних трансформацій. Серія: економіка та управління.* 2022. № 3. URL: https://doi.org/10.54929/2786-5738-2022-3-08-01.

2. Актуарні розрахунки : підручник / за заг. ред. І.М. Копич. К. : Новий Світ – 2000, 2020. 214 с.

3. Аналіз законодавства про захист персональних даних України. АО «Саєнко Харенко», 2020. 55 с. URL: https://ecpl.com.ua/wp-content/uploads/2020/09/UKR_09142020_CEP_Finalnyy-zvit.pdf.

4. Батракова Т. І., Линовецька В. Ю. Особливості та принципи цифрової економіки в Україні. *Науково-практичний журнал. Економічні студії.* 2018. № 2 (20). С. 94–96.

5. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського національного університету.* 2023. Т. 2, № 75. С. 83–87. URL: https://doi.org/10.24144/2307-3322.2022.75.2.13

6. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки.* 2015. № 9. С. 421–427.

7. Варналій З. С., Мехед А. М. Фінансова безпека суб'єктів підприємництва в умовах цифрової економіки. *Financial and credit activity problems of theory and practice.* 2022. Т. 4, № 45. С. 267–275. URL: https://doi.org/10.55643/fcaptp.4.45.2022.3813.

8. Варналій З. С. Багатоступенева структура безпеки держави (на прикладі економічної та фінансової безпеки). *Економічний вісник університету.* 2022. № 54. С. 87–94. URL: https://doi.org/10.31470/2306-546x-2022-54-87-94.

9. Варналій З. С., Мехед А. М. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник Університету банківської справи.* 2021. № 3(42). С. 55–61. URL: https://doi.org/10.18371/2221-755x3(42)2021253524.

10. Вітлінський В. В., Маханець Л. Л. Ризик цифрової економіки у зовнішньоекономічній діяльності. *Стратегії та політика розвитку територій: міжнародні, національні, регіональні та локальні виклики :* Матеріали Міжнар. науковопракт. конф., м. Чернівці-Сучава, 10 трав. 2018 р. Чернівці, 2018. С. 79–81.

11. Войнаренко М. П., Скоробогата Л. В. Мережеві інструменти капіталізації інформаційно-інтелектуального потенціалу та інновацій. *Вісник Хмельницького національного університету. Економічні науки.* 2015. № 3 (3). С. 18–24. URL: http://nbuv.gov.ua/UJRN/Vchnu_ekon_2015_3(3)__5.

12. Волосович С. В., Клапків Л. М. Детермінанти виникнення та реалізації кіберризиків. *Зовнішня торгівля: економіка, фінанси, право.* 2018. № 3. С. 101–115.

13. Гражевська Н. І., Чигиринський А. М. Цифрова трансформація економіки в умовах посилення глобальних ризиків і загроз. *Економіка та держава.* 2021. № 8. С. 53–57. URL: https://doi.org/10.32702/2306-6806.2021.8.53.

14. Гудзь О. Є. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. *Економіка. Менеджмент. Бізнес.* 2019. № 3 (29). С. 4–12. URL: https://doi.org/10.31673/2415-8089.2019.030412 (дата звернення: 15.01.2024).

15. Данченко О. Б., Ланських Є. В., Семко О. В. Інформаційні ризики цифрового формату. *Вісник Черкаського державного технологічного університету.* 2020. № 3. С. 58–66. URL: https://doi.org/10.24025/2306-4412.3.2020.200792.

16. Дашко І. М., Михайліченко Л. В. Цифровізація економіки в умовах пандемії COVID-19 як стратегічна платформа розвитку економіки держави. *Економіка та суспільство.* 2023. № 47. URL: https://doi.org/10.32782/2524-0072/2023-47-63.

17. Дергачова Г. М., Колешня Я. О. Цифрова трансформація бізнесу: сутність, ознаки, вимоги та технології. *Економічний вісник Національного технічного університету України «Київський політехнічний інститут».* 2020. Т. 1, № 17. URL: https://doi.org/10.20535/2307-5651.17.2020.216367.

18. Дорожня карта використання науки, технологій та інновацій для досягнення цілей сталого розвитку : Дорож. карта від 22.12.2023 р. URL: https://mon.gov.ua/storage/app/media/news/2024/01/03/Dorozhnya.karta.vykoryst.nauky.tekhnolohiy.ta.innovatsiy-03.01.2024-1.1.pdf.

19. Дослідження Mastercard: 51% українців готові користуватися виключно цифровим банкінгом. *Mastercard.* URL: https://www.mastercard.ua/uk-ua.html.

20. Драфт Стратегії розвитку екосистеми інновацій в Україні. М-во цифр. трансформації України, 2023. URL: https://thedigital.gov.ua/news/rozvivaemo-tsifrovu-derzhavu-doluchaytesya-do-obgovorennya-strategii-rozvitku-ekosistemi-innovatsiy-v-ukraini.

21. Дубина М. В., Середюк І. О., Білоус Н. В. Роль кіберстрахування в системі ризик-менеджменту банківських установ. *Проблеми і перспективи економіки та управління.* 2020. № 1(21). С. 183–196. URL: https://doi.org/10.25140/2411-5215-2020-1(21)-183-196.

22. Дубина М. В., Тарасенко А. В., Тарасенко О. О. Напрямки підвищення рівня фінансової грамотності домогосподарств в умовах диджиталізації сфери фінансових послуг. *Економіка та суспільство.* 2023. № 56. URL: https://doi.org/10.32782/2524-0072/2023-56-17.

23. Дубина М. В., Холявко Н. І., Попело О. В. Цифровізація ринку фінансових послуг: переваги та ризики для домогосподарств. *Науковий вісник Полісся.* 2022. № 2(25). С. 160–177. URL: https://doi.org/10.25140/2410-9576-2022-2(25)-160-177.

24. Дубина М., Попело О., Тарасенко О. Інституційні трансформації фінансової системи України в умовах розвитку цифрової економіки. *Проблеми і перспективи економіки та управління.* 2021. № 1(25). URL: https://doi.org/10.25140/2411-5215-2021-1(25)-91-110.

25. Журавка О. С., Бухтіарова А. Г., Пахненко О. М. Страхування : Навч. посіб. Суми : Сум. держ. ун-т, 2020. 350 с.

26. Звіт про базове дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки 2021. *Info Sapiens.* URL: https://www.sapiens.com.ua/publications/socpol-research/196/crdf_baseline_obiznanist-auditorii-pro-kiberbezpeku_ukr.pdf.

27. Звіт про базове дослідження щодо інформованості цільових аудиторій про основні аспекти кібербезпеки 2023. *Національний кластер кібербезпеки.* URL: https://cybersecuritycluster.org.ua/resources/report/.

28. Іванова Т. Г. Перспективи розвитку ринку кіберстрахування в Україні. *Проривні інновації на страховому ринку України :* Зб. матеріалів V Міжнар. науково-практ. інтернет-конф., м. Вроцлав, 27 жовт. 2021 р. Київ, 2021. С. 64–70.

29. Ільчук В. П., Парубець О. М., Сугоняко Д. О. Інноваційні підходи до розвитку ринку кіберстрахування в Україні. *Ефективна економіка.* 2018. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=6295.

30. Індекс цифрової трансформації регіонів України 2022. М-во цифр. трансформації України, 2023. 99 с. URL: https://oda.zht.gov.ua/wp-content/uploads/2023/04/Indeks_tsyfrovoyi_transformatsiyi_regioniv_Ukrayiny.pdf.

31. Індекс цифрової трансформації регіонів України 2023. М-во цифр. трансформації України, 2024. 26 с. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/reports/Індекс_цифрової_трансформації_регіонів_України_2023_compressed.pdf.

32. Індекси споживчих цін (інфляція). *Державна служба статистики України.* URL: https://www.ukrstat.gov.ua/operativ/menu/menu_u/cit.htm (дата звернення: 12.01.2024).

33. Інфляційний звіт жовтень 2023. Нац. банк України, 2023. 43 с. URL: https://bank.gov.ua/admin_uploads/article/IR_2023-Q4.pdf.

34. Карчева Г. Т., Огородня Д. В., Опенько В. А. Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. *Фінансовий простір.* 2017. № 3. С. 13–23.

35. Кібер-захист. *Страхова компанія UPSK.* URL: https://cyber.upsk.com.ua/.

36. Кіберзахист: діяльність та статистика. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://cip.gov.ua/ua/statics/cyber-protection.

37. Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку. *Економічний вісник Дніпровської політехніки.* 2020. № 3 (71). С. 18–26.

38. Ковбатюк М. В., Шевчук В. О. Цифрова економіка в Україні: стан, проблеми та можливості розвитку. *Збірник наукових праць ДУІТ. Економіка і управління.* 2021. № 49. С. 69–77. URL: https://doi.org/10.32703/2664-2964-2021-49-69-77.

39. Ковтонюк К. В. Цифрова трансформація світової економіки. *Вчені записки університету «КРОК». Економіка.* 2017. С. 70–76.

40. Коляденко С. В. Цифрова економіка: передумови та етапи становлення в Україні. *Економіка. Фінанси. Менеджмент: актуальні проблеми науки і практики.* 2016. № 6. С. 105–112.

41. Ксьонжик І. В., Жовта Н. А., Павліна А. А. Страхування ризиків кібербезпеки діяльності суб'єктів господарювання в сучасному інформаційному просторі. *Економіка та суспільство.* 2021. № 34. URL: https://doi.org/10.32782/2524-0072/2021-34-90.

42. Кузнєцова А. Я., Чмерук Г. Г. Теоретичні підходи до визначення цифрової економіки. *Проблеми системного підходу в економіці.* 2019. № 6 (74). С. 34–41. URL: https://doi.org/10.32782/2520-2200/2019-6-5.

43. Ломоносова (Гуменюк) Л. С. Глобальна невизначеність як драйвер переоцінки бізнес-ризиків. *Шевченківська весна 2023. Повоєнне відновлення економіки України: проблеми та перспективи* : матеріали XXI Міжнар. науково-практ. конф. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2023. С. 129.

44. Ломоносова (Гуменюк) Л. С. Глобальні соціокультурні тренди поведінкової економіки та їх вплив на розвиток страхування. *Шевченківська весна 2021. Економіка. На шляху до сталого розвитку* : матеріали XIX Міжнар. науково-практ. конф. Київ : К., Інтерсервіс, 2021. С. 296.

45. Ломоносова (Гуменюк) Л. С. Особливості кібер-страхування в процесі адаптації до умов пандемії COVID-19. *Фінансові інструменти сталого розвитку економіки* : матеріали IV Міжнар. науково-практ. конф., 12 трав. 2022 р. Чернівці : Чернівецький нац. ун-т, 2022. С. 436–438.

46. Ломоносова (Гуменюк) Л. С. Перспективи розвитку кібер-страхування в Україні. *Проривні інновації на страховому ринку України*: матеріали V Міжнар. науково-практ. інтернет-конф., 27 жовт. 2021 р. Київ : К.: КНЕУ, 2021. С. 152–154.

47. Ломоносова (Гуменюк) Л. С. Трансформація продуктів кібер-страхування в умовах глобальної пандемії COVID-19. *Економіка. Фінанси. Бізнес. Управління. Зміни. Адаптація. Нова економіка : Діджиталізація ринку фінансових послуг: нові можливості та подолання бар'єрів* : матеріали II Міжнар. форуму, 28 верес.-1 жовт. 2021 р. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2021. С. 22-24.

48. Ломоносова (Гуменюк) Л. С. Фінансова інклюзія як ключовий фактор у відновленні економічного розвитку України після війни. *Transformation of Ukraine's economy: formation of an inclusive economy system and functionality of financial inclusion.* Рига, 2023. С. 152–169. URL: https://doi.org/10.30525/978-9934-26-321-7-7.

49. Мельник Г. В. Модель оцінювання рівня інформаційних ризиків в корпоративних системах. *Вісник Київського національного університету імені Тараса Шевченка. Економіка.* 2015. №6. С. 48-54. URL: http://nbuv.gov.ua/UJRN/VKNU_Ekon_2015_6_11.

50. Морозова (Селіверстова) Л. С., Друхан Д. А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава.* 2020. № 1. С. 23. URL: https://doi.org/10.32702/2306-6806.2020.1.23

51. Нагайчук Н. Г., Третяк Н. М., Ткаленко О. В. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. *Фінансовий простір.* 2019. № 1(33). С. 98–113. URL: https://doi.org/10.18371/fp.1(33).2019.177102.

52. Наглядова статистика. *Національний банк України.* URL: https://bank.gov.ua/ua/statistic/supervision-statist#6.

53. Обушний С. М., Арабаджи К. В., Костікова К. О. Фінансові технології в Україні: шлях до інновацій та стабільності. *European scientific journal of Economic and Financial innovation.* 2023. № 1 (11). С. 59–72. URL: https://doi.org/10.32750/2023-0105.

54. Партин Г. О., Гребенюк А. В. Перспективи розвитку кібер-страхування в Україні, та перешкоди його становлення. *Модернізація економіки у контексті інноваційного розвитку: напрями та пріоритети* : Матеріали міжнар. науково-практ. конф., м. Дніпро, 17 листоп. 2018 р. Дніпро, 2018. С. 30–33.

55. Пікус Р. В., Бабенко Ю. Л. Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава.* 2022. № 2. С. 134. URL: https://doi.org/10.32702/2306-6806.2022.2.134.

56. Пілінський В. В., Веретюк С. М. Визначення пріоритетних напрямків розвитку цифрової економіки в Україні. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2016. № 2 (42). С. 51–58.

57. Планування в системі фінансового менеджменту страхових компаній в умовах воєнного стану / Петрук О. М. та ін. *Інвестиції практика та досвід*. 2023. № 11. С. 5–8. URL: https://doi.org/10.32702/2306-6814.2023.11.5.

58. Попович Д. В., Бундз Н., Іванків В. Проблеми та перспективи розвитку страхування кіберризиків на національному ринку. *Молодий вчений.* 2023. № 4 (116). С. 168–172. URL: https://doi.org/10.32839/2304-5809/2023-4-116-33.

59. Приказюк Н. В. Необхідність та можливість впровадження нових страхових продуктів у страховій системі (на прикладі кіберстрахування). *Економіка і фінанси*. 2016. № 12. С. 109–117.

60. Приказюк Н. В., Кукурузняк М. В. Прогресивний досвід зарубіжних країн у вирішенні проблем розвитку кіберстрахування. *Вісник Одеського національного університету. Серія: Економіка.* 2016. Т. 21. № 2. С. 164-168.

61. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Дорожня карта впровадження кібер-страхування в Україні. *Innovation and sustainability*. 2021. № 1. С. 64–72. URL: https://doi.org/10.31649/ins.2021.1.64.72.

62. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Забезпечення цифрової грамотності населення як складової національної кібер-безпеки. *Грудневі читання 2022. Стійкість бізнесу і добробут домогосподарств: фінансові та соціальні аспекти* : зб. тез доп. XIV Міжнар. науково-практ. конф., 1-2 груд. 2022 р. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2022. С. 84-85.

63. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Кібербезпека фінансового сектору України: нові загрози та захисти в умовах повномасштабного вторгнення. *Страховий ринок України у світлі євроінтеграції: новітні виклики та тренди* : зб. матеріалів VI Міжнар. науково-практ. конф., 12 берез. 2023 р. Київ : К.: КНЕУ, 2023. С. 119-121.

64. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка.* 2020. № 4. URL: https://doi.org/10.32702/2307-2105-2020.4.6.

65. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Передумови розвитку кібер-страхування. *Інвестиції: практика та досвід.* 2020. № 15-16. С. 28–34. URL: http://dx.doi.org/10.32702/2306-6814.2020.15-16.28.

66. Приказюк Н., Марченко К. Маркетингові стратегії страховиків в умовах діджиталізації: сучасна практика та перспективи розвитку. *Економічний аналіз.* 2022. № 32(1). С. 236–247. URL: https://doi.org/10.35774/econa2022.01.236.

67. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 р. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text.

68. Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки,

кіберзахисту та електронних довірчих послуг : Постанова Нац. банку України від 16.01.2021 р. № 4. URL: https://zakon.rada.gov.ua/laws/show/v0004500-21#Text.

69. Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах : Постанова Нац. банку України від 11.06.2018 р. № 64 : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text.

70. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 31 груд. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

71. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

72. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

73. Про страхування : Закон України від 07.03.1996 р. № 1909-IX-ВР : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/85/96-вр#Text.

74. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації : Розпорядж. Каб. Міністрів України від 17.11.2021 р. № 1467-р : станом на 11 квіт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-р#Text.

75. Пуцентейло П. Р., Гуменюк О. О. Цифрова економіка як новітній вектор реконструкції традиційної економіки. *Інноваційна економіка. 2018*. № 5-6 (75). С. 131–143. URL: http://dspace.wunu.edu.ua/handle/316497/32028.

76. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України, 2024. 12 с. URL: https://scpc.gov.ua/api/files/1b6b58b3-07d7-4223-94f6-4cf116d5fe0f.

77. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України, 2023. 10 с. URL: https://scpc.gov.ua/api/docs/sseb6a10-b7aa-4396-8b04-e0e4b7fca111/sseb6a10-b7aa-4396-8b04-e0e4b7fca111.pdf.

78. Сірко А. В. Реалії цифрової економіки: нові можливості та виклики для суспільства і держави. *Ефективна економіка.* 2020. № 11. С. 1–8. URL: https://doi.org/10.32702/2307-2105-2020.11.15.

79. Сосновська О., Сіренька І. Тенденції інноваційного розвитку страхових компаній в Україні. *Європейський науковий журнал Економічних та Фінансових інновацій.* 2021. Т. 2, № 8. С. 20–30. URL: https://doi.org/10.32750/2021-0202.

80. Статистика страхового ринку України. *Forinsurer.* URL: https://forinsurer.com/stat.

81. Страхова система України: теорія, методологія, практика : монографія / Н. В. Приказюк. К. : Логос, 2017. 611 с.

82. Страхові послуги : навч. посібник / за заг. ред. Д. І. Деми. К. : Алерта, 2013. 484 с.

83. Страхові послуги : підручник / за заг. ред. Т. А. Говорушко. К. : Центр учбової літератури, 2011. 376 с.

84. Страхування : підручник / за заг. ред. В. Д. Базилевича. К. : Знання, 2008. 1019 с.

85. Страхування : підручник / за заг. ред. С.С. Осадця. К. : КНЕУ, 2002. 599с.

86. Страхування кібер-ризиків. *Страхова компанія АСКА.* URL: https://aska.ua/ua/business-insurance/industry/cyber-insurance.

87. Страхування професійної відповідальності. *Страхова Компанія Colonnade.* URL: https://colonnade.com.ua/for_it.

88. Струтинська І. В. Дефініції поняття «цифрова трансформація». *Причорноморські економічні студії.* 2019. № 48. URL: https://doi.org/10.32843/bses.48-47.

89. Тести. *Дія.Освіта*. URL: https://osvita.diia.gov.ua/digigram.

90. Україна посилює співпрацю з ЄС у сфері кібербезпеки: НКЦК підписав Угоду про співпрацю з ENISA. *Рада національної безпеки і оборони України.* URL: https://www.rnbo.gov.ua/ua/Diialnist/6706.html.

91. Ус Г. О., Коваль О. О. Цифрова економіка, її розвиток та економічна характеристика. *Вісник Хмельницького національного університету. Економічні науки.* 2021. Т. 1, № 6. С. 70–72. URL: https://doi.org/10.31891/2307-5740-2021-300-6-12.

92. Фінансові та інші ризики. *InsArt.* URL: https://insart.com.ua/vydy-strakhuvannya/.

93. Цілі сталого розвитку. *UNDP*. URL: https://www.undp.org/uk/ukraine/tsili-staloho-rozvytku.

94. Чмерук Г. Г. Цифрова економіка як окремий сектор національної економіки держави. *Науковий вісник Ужгородського національного університету.* 2019. № 27. URL: https://doi.org/10.32782/2413-9971/2019-27-38.

95. Шолойко А. С. Актуалізація кіберстрахування в умовах цифровізації економіки. *Науковий вісник Одеського національного економічного університету.* 2023. Т. 9, № 310. С. 98–106. URL: https://doi.org/10.32680/2409-9260-2023-9-310-98-106.

96. Шолойко А. С. Кібербезпека як нова ціль сталого розвитку. *Вісник Чернівецького торговельно-економічного Інституту.* 2023. Т. 3, № 91. С. 43–52. URL: https://doi.org/10.34025/2310-8185-2023-3.91.03.

97. Що таке кібератака? *Microsoft – Cloud, Computer, Apps und Gaming.* URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack.

98. Як можна застрахуватися від кібер ризиків? *Polis24.* URL: https://polis24.ua/news/articles/yak-mozhna-zastrahuvatisya-vid-kiber-rizikiv.

99. 2023-2030 Australian Cyber Security Strategy : Strategy of 22.11.2023. URL: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy.

100. A history of cyber insurance. *MarshCommercial.* URL: https://www.marshcommercial.co.uk/articles/history-of-cyber-insurance.

101. Allianz Risk Barometer 2014. *Allianz.* URL: https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/migration/media/press/document/other/Press_release_Allianz_Risk_Barometer_14Jan2014-AGCS-final2-EN.pdf.

102. Allianz Risk Barometer 2017. *Allianz.* URL: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/press-releases/global/AGCS-Press-Risk-Barometer-2017.pdf.

103. Allianz Risk Barometer 2020. *Allianz.* URL: https://www.allianz.bg/content/dam/onemarketing/cee/azbg/press-center-images/allianz-risk-barometer-2020/Allianz_Risk_Barometer_2020_report_final.pdf.

104. Allianz Risk Barometer 2022. *Allianz.* URL: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2023.pdf.

105. Bart V. A. The productivity paradox of the new digital economy. *Global Economics & Management.* 2016. Vol. 31. P. 3–18. URL: https://research.rug.nl/en/publications/the-productivity-paradox-of-the-new-digital-economy.

106. Basic Data from a «Digitalized Economy»: 113 Persons Become New Members of the Academy of Engineering. *Chinese Education & Society.* 2001. Vol. 34, no. 3. P. 10–11. URL: https://doi.org/10.2753/ced1061-1932340310.

107. Between a rock and a hard(ening) place: cyber insurance in the ransomware era / G. Mott et al. *Computers & Security.* 2023. Vol. 128. P. 103162. URL: https://doi.org/10.1016/j.cose.2023.103162.

108. Biener C., Eling M., Wirfs J. H. Insurability of Cyber Risk: An Empirical Analysis. *SSRN Electronic Journal.* 2015. URL: https://doi.org/10.2139/ssrn.2577286.

109. Böhme R., Kataria G. Models and Measures for Correlation in Cyber-Insurance. *Revision 0.3: Workshop on the Economics of Information Security :* Working paper, 1 June 2006.

110. Böhme R., Kataria G. On the Limits of Cyber-Insurance. *Trust and privacy in digital business :* Lecture Notes in Computer Science, 1 January 2006. P. 31–40.

111. C. Rossi M., Perez G. Bibliometric analysis of publications on cyber risks in the services sector. *Revista Ibero-Americana de Estratégia.* 2023. Vol. 22, no. 1. P. 1-28. URL: https://doi.org/10.5585/2023.23846.

112. Cadet Blizzard emerges as a novel and distinct Russian threat actor. *Microsoft Security Blog.* URL: https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/.

113. Camillo M. Cyber risk and the changing role of insurance. *Journal of Cyber Policy.* 2017. Vol. 2, no. 1. P. 53–63. URL: https://doi.org/10.1080/23738871.2017.1296878.

114. Cebula J. J., Popeck M. E., Young L. R. A taxonomy of operational cyber security risks Version 2. Carnegie Mellon University, 2014. 48 p. URL: https://insights.sei.cmu.edu/documents/2273/2014_004_001_91026.pdf.

115. Common exclusions. Cyber Insurance. *ABI.* URL: https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/cyber-insurance/common-exclusions-cyber.

116. Consumer cyber insurance for risk transfer: a coverage analysis / F. Schütz et al. *Procedia Computer Science.* 2023. Vol. 219. P. 521–528. URL: https://doi.org/10.1016/j.procs.2023.01.320.

117. Content analysis of cyber insurance policies: how do carriers price cyber risk? / S. Romanosky et al. *Journal of Cybersecurity.* 2019. Vol. 5, no. 1. URL: https://doi.org/10.1093/cybsec/tyz002.

118. Cryptocurrency Prices By Market Cap. *Forbes.* URL: https://www.forbes.com/digital-assets/crypto-prices/?sh=11ab28682478.

119. Customer Identification. *USLI*. URL: https://customers.usli.com/sites/dapps/Dapp_Professional_cyberliability.pdf.

120. Cyber and Privacy Insurance application form. *Eqgroup*. URL: https://www.eqgroup.com/Pdf/Chubb/CHUBB-Cyber-Privacy-Insurance-Application.pdf.

121. Cyber Insurance 2022: Reality from the Infosec Frontline. *Sophos*. URL: https://www.sophos.com/en-us/resources/cyber-insurance-2022.

122. Cyber Insurance Market Size, Share. *Market*. URL: https://market.us/report/cyber-insurance-market/.

123. Cyber Insurance Market Size. *Fortune Business Insights*. URL: https://www.fortunebusinessinsights.com/cyber-insurance-market-106287.

124. Cyber Insurance Risk Framework 23 NYCRR 500 : Insurance Circular Letter of 04.02.2021 no. 2 (2021). URL: https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02#_edn23.

125. Cyber insurance risks and trends 2023. *Munich Re*. URL: https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html.

126. Cyber Insurance. *GlobalData*. URL: https://www.globaldata.com/store/report/cyber-insurance-theme-analysis/.

127. Cyber Insurance: Fitting the Needs of Operators of Essential Services? *ENISA*. URL: https://www.enisa.europa.eu/news/cyber-insurance-fitting-the-needs-of-operators-of-essential-services.

128. Cyber insurance: the current situation and prospects of development / L. Morozova et al. *Revista Amazonia Investiga*. 2020. Vol. 9, no. 28. P. 65–73. URL: https://doi.org/10.34069/ai/2020.28.04.8.

129. Cyber liability insurance coverage for businesses. *GEICO*. URL: https://www.geico.com/cyber-liability-insurance/.

130. Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment : Working Paper of 22.06.2018 no. 2018/143. URL:

https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.

131. Cyber risk insurance for businesses. *Desjardins*. URL: https://www.desjardins.com/qc/en/business/insurance/property-liability/cyber-risk.html.

132. Cyber risk. *Institute of Risk Management (IRM)*. URL: https://www.theirm.org/what-we-say/thought-leadership/cyber-risk.

133. Cyber Security Market Size. *Vantage Market Research*. URL: https://www.vantagemarketresearch.com/industry-report/cyber-security-market-1487.

134. Cyber Security Statistics Trends & Data. *PurpleSec*. URL: https://purplesec.us/resources/cyber-security-statistics/.

135. Cyber Threats. *ENISA*. URL: https://www.enisa.europa.eu/topics/cyber-threats.

136. Cyber-insurance survey / A. Marotta et al. *Computer Science Review*. 2017. Vol. 24. P. 35–61. URL: https://doi.org/10.1016/j.cosrev.2017.01.001.

137. Cybersecurity and digital economy in Malaysia: trusted law for customer and enterprise protection / B. Mat et al. *International Journal of Innovative Technology and Exploring Engineering*. 2019. No. 8. P. 214–220.

138. Cybersecurity Insurance Market Size Global. *Polaris*. URL: https://www.polarismarketresearch.com/industry-analysis/cybersecurity-insurance-market.

139. Cybersecurity Risk - Glossary. *NIST Computer Security Resource Center*. URL: https://csrc.nist.gov/glossary/term/cybersecurity_risk.

140. Cybersecurity Strategy of the European Union : Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions of 07.02.2013. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

141. Cybersecurity Threats. *Imperva*. URL: https://www.imperva.com/learn/application-security/cyber-security-threats/.

142. Dambra S., Bilge L., Balzarotti D. SoK: cyber insurance – technical challenges and a system security roadmap. *2020 IEEE symposium on security and*

privacy (SP), San Francisco, CA, USA, 18–21 May 2020. URL: https://doi.org/10.1109/sp40000.2020.00019.

143. Database: digital economy and society. *Eurostat.* URL: https://ec.europa.eu/eurostat/web/digital-economy-and-society/overview.

144. Dataset: share of individuals having at least basic digital skills, by sex. *Eurostat.* URL: https://ec.europa.eu/eurostat/databrowser/view/sdg_04_70/default/table?lang=en.

145. Development of 2023-2030 Australian Cyber Security Strategy : Circular Letter of 14.03.2023. URL: https://insurancecouncil.com.au/resource/2023-2030-australian-cyber-security-strategy/.

146. Development of digital economy in the context of information security in Ukraine / L. Sopilnyk et al. *Path of Science.* 2020. Vol. 6, no. 5. P. 2023–2032. URL: https://doi.org/10.22178/pos.58-7.

147. Digital Dashboard Ukraine. *The International Telecommunication Union*. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/DDD/ddd_UKR.pdf.

148. Digital financial inclusion: COVID-19 impacts and opportunities / Dluhopolskyi O. et al. *Sustainability.* 2023. Vol. 15, no. 3. P. 2383. URL: https://doi.org/10.3390/su15032383.

149. Digitization of the economy under the influence of the COVID-19 pandemic / Pikus R. et al. *Postmodern openings.* 2022. Vol. 13, No. 4. P. 127–141. URL: https://doi.org/10.18662/po/13.4/510.

150. Directive on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) : Directive of the European Parliament and of the Council of 14.12.2022 no. 2022/2555. URL: https://eur-lex.europa.eu/eli/dir/2022/2555.

151. Duc A. N., Chirumamilla A. Identifying security risks of digital transformation - an engineering perspective. *Conference on e-Business, e-Services and e-Society :* Conference Paper, 1 August 2019. Online, 2019. P. 677–688. URL: https://doi.org/10.1007/978-3-030-29374-1_55.

152. E&O and Cyber Market Review. *Aon.* URL: https://www.aon.com/cyber-solutions/thinking/errors-and-omissions-and-cyber-market-review-2022/.

153. Eling M., Schnell W. What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance.* 2016. Vol. 17, no. 5. P. 474–491. URL: https://doi.org/10.1108/jrf-09-2016-0122.

154. Enhancing the Role of Insurance in Cyber Risk Management. *OECD Foreword.* 2017. P. 3. URL: https://doi.org/10.1787/9789264282148-1-en.

155. Evolution of digital economy research: a bibliometric analysis / Y. Xia et al. *International Review of Economics & Finance.* 2023. Vol. 88. P. 1151-1172. URL: https://doi.org/10.1016/j.iref.2023.07.051.

156. Franke U. The cyber insurance market in Sweden. *Computers & Security.* 2017. Vol. 68. P. 130–144. URL: https://doi.org/10.1016/j.cose.2017.04.010.

157. GDP Ukraine. *World Bank Open Data.* URL: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=UA.

158. GDP. *World Bank Open Data.* URL: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.

159. Global cybercrime estimated cost. *Statista.* URL: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide.

160. Global distribution of cyber attacks in top industries 2022. *Statista.* URL: https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/.

161. Global financial inclusion. *The World Bank DataBank.* URL: https://databank.worldbank.org/source/global-financial-inclusion.

162. Global Insurance Market Index. *Marsh.* URL: https://www.marsh.com/us/services/international-placement-services/insights/global_insurance_market_index.html.

163. Gordon L. A., Loeb M. P., Sohail T. A framework for using insurance for cyber-risk management. *Communications of the ACM.* 2003. Vol. 46, no. 3. P. 81–85. URL: https://doi.org/10.1145/636772.636774.

164. Granato A., Polacek A. The growth and challenges of cyber insurance. *Chicago Fed Letter*. 2019. No. 426. URL: https://doi.org/10.21033/cfl-2019-426.

165. Guide to getting started with a cybersecurity risk assessment. CISA. *URL:* https://www.cisa.gov/sites/default/files/2023-02/22_1201_safecom_guide_to_cybersecurity_risk_assessment_508-r1.pdf.

166. Gupta B., Dahiya A. Distributed Denial of Service (DDoS) Attacks. Taylor & Francis Group, 2021.

167. High-technology exports. *World Bank Open Data.* URL: https://data.worldbank.org/indicator/TX.VAL.TECH.MF.ZS.

168. How can you be truly customer-centric, rather than simply customer facing? *Ernst & Young Limited.* URL: https://www.ey.com/en_ch/forms/2022/how-can-you-be-truly-customer-centric-rather-than-simply-customer-facing.

169. How should we understand the digital economy in Asia? Critical assessment and research agenda / K. Li et al. *Electronic Commerce Research and Applications.* 2020. Vol. 44. P. 101004. URL: https://doi.org/10.1016/j.elerap.2020.101004.

170. Ignatyuk A., Sholoiko A., Syzenko A. Assessment of infrastructure entities' activity on the insurance market. *Investment Management and Financial Innovations.* 2021. Vol. 18, no. 1. P. 76–89. URL: https://doi.org/10.21511/imfi.18(1).2021.07.

171. Improving Critical Infrastructure Cybersecurity : Executive Order of 12.02.2013. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

172. Insurance for cyber-risk: a Utility model / A. Mukhopadhyay et al. *Decision*. 2005. No. 32. P. 153–169.

173. ISO 22301:2019. *ISO.* URL: https://www.iso.org/standard/75106.html.

174. ISO/IEC 27001. *ISO.* URL: https://www.iso.org/standard/27001.

175. ISO/IEC 27002:2022. *ISO.* URL: https://www.iso.org/standard/75652.html.

176. ISO/IEC 27031:2011. *ISO.* URL: https://www.iso.org/standard/44374.html.

177. ISO/IEC 27032:2023. *ISO*. URL: https://www.iso.org/standard/76070.html.

178. ISO/IEC 27701:2019. *ISO*. URL: https://www.iso.org/standard/71670.html.

179. ISO/TC 150. Implants for surgery. Official edition. URL: https://www.iso.org/committee/53058.html.

180. IT Costs. *Gartner*. URL: https://www.gartner.com/en.

181. ITU Statistics. *The International Telecommunication Union*. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

182. Kanavas A. Cyberinsurance as a Risk Management Tool : extended abstract of Master Thesis. Piraeus, 2023. 92 p.

183. Kshetri N. The evolution of cyber-insurance industry and market: an institutional analysis. *Telecommunications policy*. 2020. Vol. 44, no. 8. P. 102007. URL: https://doi.org/10.1016/j.telpol.2020.102007.

184. Kwak Y.-S., Cho Y.-S. Cyber insurance and distribution channels. *Journal of distribution science*. 2018. Vol. 16, no. 5. P. 61–70. URL: https://doi.org/10.15722/jds.16.5.201805.61.

185. Leahovcenco A. Cybersecurity as a fundamental element of the digital economy. *MEST journal*. 2021. Vol. 9, no. 1. P. 97–105. URL: https://doi.org/10.12709/mest.09.09.01.13.

186. Lewis J. Economic Impact of Cybercrime – No Slowing Down. McAfee, 2018. 28 p. URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

187. Lomonosova (Gumenyuk) L. Cyber insurance: modern requirements. *Economics & Education*. 2021. Vol. 6, No. 4. P. 33–36. URL: https://doi.org/10.30525/2500-946x/2021-4-5.

188. Lomonosova (Gumenyuk) L. Financial inclusion as a key factor in the Ukraine's economic development recovering after the war. *Transformation of Ukraine's economy: formation of an inclusive economy system and functionality of financial*

inclusion. Riga, 2023. P. 152–169. URL: https://doi.org/10.30525/978-9934-26-321-7-7.

189. Lomonosova (Gumenyuk) L. Modern risks: anthropogenic or natural? *Modern Trends in The Development of Science and Technology* : Proceedings of the 3rd international scientific and practical conference, 12-13 December 2022. Innsbruck : LIU, 2022. P. 27-31.

190. Majuca R. P., Yurcik W., Kesan J. P. The evolution of cyberinsurance. 2006. P. 1–16. URL: https://arxiv.org/ftp/cs/papers/0601/0601020.pdf.

191. Mazzoccoli A., Naldi M. Optimal investment in cyber-security under cyber insurance for a multi-branch firm. *Risks.* 2021. Vol. 9, no. 1. P. 24. URL: https://doi.org/10.3390/risks9010024.

192. Miller L. Cybersecurity Insurance: Incentive Alignment Solution to Weak Corporate Data Protection. *SSRN Electronic Journal.* 2018. Vol. 7, no. 2. P. 147-182 URL: https://doi.org/10.2139/ssrn.3113771.

193. Mobile cellular subscriptions. *World Bank Open Data.* URL: https://data.worldbank.org/indicator/IT.CEL.SETS?end=2022&start=2022&view=bar.

194. Moodley T., Govender K. K. Collaborative Leadership and Customer-Centricity: The Case of an Insurance Service Provider. *Journal of Public Value and Administrative Insight.* 2020. Vol. 3, no. 3. P. 66–81. URL: https://doi.org/10.31580/jpvai.v3i3.1487.

195. Morozova (Seliverstova) L., Tkachenko N. Trends in the development of the Ukrainian insurance market. *Investytsiyi: praktyka ta dosvid.* 2020. No. 3. P. 10. URL: https://doi.org/10.32702/2306-6814.2020.3.10.

196. Muravskyi V., Pochynok N., Farion V. Classification of cyber risks in accounting. Herald of economics. 2021. No. 2. P. 129. URL: https://doi.org/10.35774/visnyk2021.02.129.

197. National Capabilities Assessment Framework. 2020. 83 p. URL: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework.

198. National Cybersecurity Strategy : Strategy of 01.03.2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

199. Number Of Cyber Attacks In 2021. *Stealthlabs.* URL: https://www.stealthlabs.com/news/cyberattacks-increase-50-in-2021-peaking-all-time-high-of-925-weekly-attacks-per-organization/.

200. Number of malware attacks per year. *Statista.* URL: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/.

201. O'Leary D. E. Digitization, digitalization, and digital transformation in accounting, electronic commerce, and supply chains. *Intelligent systems in accounting, finance and management.* 2022. URL: https://doi.org/10.1002/isaf.1524.

202. Pal R. Improving network security through cyber-insurance : extended abstract of ProQuest Dissertations Publishing. 2014. 24 p.

203. Patterson R. W. Can behavioral tools improve online student outcomes? Experimental evidence from a massive open online course. *Journal of Economic Behavior & Organization.* 2018. Vol. 153. P. 293–321. URL: https://doi.org/10.1016/j.jebo.2018.06.017.

204. Pavlidis G. Europe in the digital age: regulating digital finance without suffocating innovation. *Law, innovation and technology.* 2021. P. 1–14. URL: https://doi.org/10.1080/17579961.2021.1977222.

205. Pavlík L., Ficek M., Rak J. Dynamic Assessment of Cyber Threats in the Field of Insurance. *Risks.* 2022. Vol. 10, no. 12. P. 222. URL: https://doi.org/10.3390/risks10120222.

206. Pervasiveness in a competitive multi-operator environment:the daidalos project / R. Aguiar et al. *IEEE Communications Magazine.* 2007. Vol. 45, no. 10. P. 22–26. URL: https://doi.org/10.1109/mcom.2007.4342815.

207. Phishing Statistics for 2023. *IT Governance UK Blog.* URL: https://www.itgovernance.co.uk/blog/51-must-know-phishing-statistics-for-2023.

208. Pikus R. et al. Knowledge management trends in the digital economy. *Postmodern openings*. 2022. Vol. 13, No. 3. P. 346–357. URL: https://doi.org/10.18662/po/13.3/493.

209. Ponemon Cost of Insider Risks Global Report. *DTEX Systems Inc.* URL: https://www.dtexsystems.com/resources/.

210. Prykaziuk N., Lomonosova (Gumenyuk) L. Pandemic COVID-19 as a key factor in the development of DDOS-attacks insurance. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2022. № 1 (218). С. 39–44. URL: https://doi.org/10.17721/1728-2667.2022/218-1/6.

211. Rangu C. M., Pană N., Șcheau M. C. Cyber Risk Insurance Framework Considerations. *Economic and Financial Crime, Sustainability and Good Governance.* Cham, 2023. P. 383–401. URL: https://doi.org/10.1007/978-3-031-34082-6_15.

212. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on 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) (Text with EEA relevance) : Regulation of 27.04.2016 no. 2016/679. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504.

213. Report on the Cybersecurity Insurance Market 2021. National Association of Insurance Commissioners, 2022. 7 p.

214. Report on the Cybersecurity Insurance Market 2022. National Association of Insurance Commissioners, 2023. 9 p.

215. Review of the 2015 Recommendation on Digital Security Risk Management. *OECD*. URL: https://survey.oecd.org/upload/surveys/877537/files/SecurityRecOverview.pdf.

216. Ruef M. Cyber insurance – benefits and uses. *SCIP*. URL: https://www.scip.ch/en/?labs.20171123.

217. Schwieger D., Ladwig C. Cyber insurance concepts for the MIS and business curriculum. *Information Systems Education Journal*. 2022. No. 20 (5). P. 54–66. URL: https://files.eric.ed.gov/fulltext/EJ1363425.pdf.

218. Sheldon J. B. Cyberwar, Cybersecurity, Cyberattacks & Defense Strategies. Encyclopedia *Britannica.* URL: https://www.britannica.com/topic/cyberwar.

219. Singh R. K., Singh A., Chavan S. Distribution channels in life and general insurance: a conceptual analysis. *UGC Care Journal.* 2020. Vol. 40, no. 27. P. 590–609.

220. Starostina A., Pikus R., Kravchenko V. Innovative Activities within Ukrainian Insurance Companies. *Marketing and Management of Innovations.* 2020. No. 2. P. 44–55. URL: https://doi.org/10.21272/mmi.2020.2-03.

221. Technology and innovation in the insurance sector. *OECD.* URL: https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf.

222. Teoh C. S., Mahmood A. K. Cybersecurity Workforce Development for Digital Economy. *The Educational Review, USA.* 2018. Vol. 2, no. 1. P. 136-146. URL: https://doi.org/10.26855/er.2018.01.003.

223. The approximation of the laws of the Member States relating to active implantable medical devices : Council Directive of 20.06.1990 no. 90/385/EEC.

224. The Australian Signals Directorate's Australian Cyber Security Centre. *ASD's ACSC.* URL: https://www.cyber.gov.au/about-us.

225. The Digital Europa Thesaurus: «digital». *The official portal for European data.* URL: http://data.europa.eu/cpv/cpvsuppl/CA43.

226. The EU Security Union Strategy : Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions of 24.07.2020 no. COM/2020/605 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605.

227. Toward dynamic virtualized network services in telecom operator networks / I. Cerrato et al. *Computer Networks.* 2015. Vol. 92. P. 380–395. URL: https://doi.org/10.1016/j.comnet.2015.09.028.

228. Transforming our World: The 2030 Agenda for Sustainable Development : Resolution of 25.09.2015. URL: https://sdgs.un.org/publications/transforming-our-world-2030-agenda-sustainable-development-17981.

229. Volosovych S., Sholoiko A., Shevchenko L. Cryptocurrency market transformation during pandemic COVID-19. *Financial and credit activity problems of theory and practice.* 2023. Vol. 1, no. 48. P. 114–126. URL: https://doi.org/10.55643/fcaptp.1.48.2023.3949.

230. What is cyber liability insurance. *Malwarebytes.* URL: https://www.malwarebytes.com/cybersecurity/business/what-is-cyber-liability-insurance.

231. What Is Cyber Risk Insurance? *Trend Micro.* URL: https://www.trendmicro.com/en_ae/what-is/cyber-insurance.html.

232. What is Cybersecurity Risk? A Thorough Definition. *UpGuard.* URL: https://www.upguard.com/blog/cybersecurity-risk.

233. Wrede D., Stegen T., Graf von der Schulenburg J.-M. Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *The Geneva Papers on Risk and Insurance - Issues and Practice.* 2020. Vol. 45, no. 4. P. 657–689. URL: https://doi.org/10.1057/s41288-020-00183-6.

ДОДАТКИ

Додаток А

Таблиця А.1

Систематизація визначень поняття «цифрова економіка» за групами теоретико-методологічних підходів

Автор	Визначення
Цифрова економіка як оптимізована похідна економіки	
Карчева Г. Т., Огородня Д. В., Опенько В. А.	Інноваційна динамічна економіка, яка передбачає активне запровадження інновацій та інформаційно-комунікаційних технологій на всіх етапах соціально-економічної діяльності, що сприяє зростанню ефективності й конкурентоздатності окремих організацій, національних економік та якість життя населення.
Ковтонюк К.В.	Віртуальне економічне середовище, що за допомогою ІКТ здійснює трансформацію традиційних економічних взаємовідносин, які складаються в системі виробництва, розподілу, обміну та споживання.
Кузнєцова А.Я., Чмерук Г.Г.	Економічна діяльність, яка виникла лише завдяки новітнім цифровим технологіям та базується на використанні нових цифрових бізнес-моделей і в якій основними засобами (факторами) виробництва є цифрові (електронні, віртуальні) дані як числові, так і текстові.
Пуцентейло, П.Р., Гуменюк, О.О.	Економіка, заснована на даних, мобільності, хмарних сервісах і новітніх інформаційних технологіях, цифровій освіті з завданням підготовки фахівців якісно нового рівня і цифрова медицина, покликана зменшити витрати на надання послуг і підвищити їх якість.
Сірко А.В.	Особлива стадія економічного розвитку, основними характеристиками якої є масове використання цифрової інформації, повсюдним впровадженням багатосторонніх (мережевих) бізнес-моделей і, взагалі, відкриття нових можливостей для існування людини, суспільства та держави.
Цифрова економіка як доповнення до традиційної економіки	
Li K., Kim D.J., Lang K.R., Kauffman R.J., Naldi M.	Доповнення до традиційної невиробничої діяльності передовими технологіями інформатизації та цифровізації, що створюють додану вартість. Технології можуть включати поєднання Інтернету з продажами, розробку нових продуктів шляхом оптимізації виробництва матеріалів (наприклад, 3D-друком) і маркетинг через соціальні мережі.
Батракова Т.І., Линовецька В.Ю.	Цифрова економіка – це не окрема галузь, а віртуальне середовище, яке доповнює нашу реальність та є економікою віртуальний світів.
Ус Г.О., Коваль О.О.	Є вторинною в економічному механізмі, первинним є процес виробництв; прискорює і пришвидшує існуючі економічні процеси.
Цифрова економіка як ознака зрілості традиційної економіки	
Bart V. A.	Економіка, що збільшує свою ефективність та переходить на якісно новий рівень через залучення інформаційно-комунікативних технологій, збільшуючи при цьому свою продуктивність.

Продовження Таблиці А.1

Xia Y., Lv G., Wang H., Ding L.	Економіка, що більше не обмежується конкретною новою технологією, а є більш ефективною новою економічною формою, яка сприяє глибоким змінам у методах виробництва, способах життя та методах управління, а також більшій уніфікованій справедливості і ефективності.
Цифрова економіка як адаптована економіка, що реалізовує свої функції через використання цифрових технологій	
R. W. Patterson	Економічна діяльність, яка є результатом масового залучення за допомогою онлайн-з'єднань процесів, даних, пристроїв, підприємств і людей.
Коляденко С. В.	Економіка, що базується на виробництві електронних товарів і сервісів високотехнологічними бізнес-структурами і дистрибуції цієї продукції за допомогою електронної комерції.
Ковбатюк М.В., Шевчук В.О.	Основними продуктами цифрової економіки є товари і послуги традиційної економіки, але які надаються за допомогою комп'ютерного обладнання і цифрових систем.
Об'єднання «Digitalized Economy»	Оскільки економіка зосереджена на цифрових технологіях, то вона сприймається як ведення бізнесу на ринку, що використовує Інтернет та технології.
Цифрова економіка як окремий сектор економіки	
Войнаренко М. П.	Передбачає, що всі економічні процеси (за винятком виробництва товару) протікають незалежно від реального світу.
Пілінський В.В., Веретюк С.М.	Є складовою частиною економіки, в якій домінують знання суб'єктів та нематеріальне виробництво – основний показник під час визначення інформаційного суспільства.
Чмерук Г. Г.	Окремий сектор економіки, в якому господарська діяльність здійснюється суб'єктами господарювання шляхом застосування інформаційно-комунікаційних та цифрових технологій, де основними засобами (факторами) виробництва є цифрові (електронні, віртуальні) дані (як числові, так і текстові).

Джерело: складено автором на основі [4, с. 94; 11, с. 19; 34, с. 14; 38, с. 70; 39, с. 73; 40, с. 107; 42, с. 38; 56, с. 4; 75, с. 136; 78, с. 4; 91, с. 71; 94, с. 4; 105, с. 3-5; 106, с. 11; 155; 167, с. 101010; 203, с. 304]

Додаток Б

Таблиця Б.1

Систематизація визначень поняття «кібер-ризик» за групами стейкхолдерів

Автор	Визначення
Група міжнародних організацій	
Institute of risk management	Означає будь-який ризик фінансових втрат, збоїв або шкоди репутації організації через певний збій її систем інформаційних технологій.
Microsoft	Мережі, які вважаються найуразливішими для кібератак.
National Institute of Standards and Technology	Пов'язані з втратою конфіденційності, цілісності або доступності інформації, даних або інформаційних (або контрольних) систем і відображають потенційний несприятливий вплив на діяльність організації.
UpGuard	Ймовірність зупинки діяльності або втрат в результаті кібератаки або витоку даних організації.
Група урядових інституцій	
CISA	Обставина або подія, яка має або вказує на існування потенціалу використання вразливостей і негативного впливу на організаційні операції, активи, окремих осіб, інші організації чи суспільство.
ENISA	Реалізація таких кібер загроз як: програми-вимагачі, зловмисне програмне забезпечення, загрози, пов'язані з електронною поштою, загрози щодо даних, загрози щодо доступності та цілісності, дезінформація, атаки на ланцюги поставок.
НБУ	Ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз.
Група страховиків та страхових брокерів	
Colonnade	Ризики, наслідками яких є збитки через витік даних, витрати на відновлення інформації.
InsArt Insurance Broker	Атаки з боку хакерів, крадіжка корпоративних даних, впровадження вірусів і втручання в роботу програмного забезпечення, що викликає перебої в роботі цифрових систем.
Polis24	Ризики, які пов'язані з використанням інтернету, передачею даних та можливим витоком інформації. Адже компаніям стало важко забезпечити кібер безпеку і бути переконаними у надійності зберігання інформації.
Група науковців	
Абрамова А. С.	Не є по-справжньому «новими», вони еволюціонують і збільшуються у результаті структурних змін у зв'язку з цифровізацією бізнес-моделей.
Волосович С. В., Клапків Л. М.	Це операційний ризик, який полягає в отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі.
Гудзь О. Є.	Ризик, що генерується використанням: телекомунікаційного обладнання, програмного забезпечення, локальних і Інтернет-мереж, розрахунково-платіжних систем, систем інтернет-торгівлі, промислових систем менеджменту, а також це ризик, що пов'язаний з накопиченням, зберіганням, передачею і використанням персональних даних.

Продовження Таблиці Б.1

Дубина М. В., Середюк І. О., Білоус Н. В.	Створення нових загроз у віртуальному просторі, що безпосередньо пов'язаний із розробкою та впровадженням нових технологій, які використовують потенціал мережі Інтернет, сучасних інформаційних продуктів, ... що призвело до вже перманентного виникнення кібератак, які зумовлюють створення нових кіберризиків.
Пікус Р., Бабенко Ю.	Це ймовірність настання подій, які вражають роботу ІТ-систем та кібербезпеку організації через стороннє втручання цифрових та інших електронних технологій, що призводить до отримання збитків, руйнування цифрових активів та можливої втрати репутації організації.

Джерело: складено автором на основі [1, с. 3; 12, с. 103; 14, с. 3; 21, с. 184; 55, с. 103130; 68; 87; 93; 97; 98; 135; 139; 165; 232]

Додаток В

Таблиця В.1

Систематизація визначень понять «кіберстрахування» та «страхування кібер-ризиків»

Автор	Визначення
Поняття «кіберстрахування»	
Böhme R., Kataria G.	Відповідний засіб компенсації фінансових втрат, спричинених порушенням безпеки комп'ютерних систем.
Mott G. et al	Засіб компенсації збитків від фінансових ризиків, спричинених кіберінцидентами.
Schütz F. et al.	Бізнес-модель кіберстрахування пропонує низку послуг для організації, спрямованих на мінімізацію негативних наслідків, що виникають внаслідок кіберінцидентів.
Гудзь О. Є.	Страховий продукт, який захищає економічні суб'єкти від ризиків, що відносяться до інформаційно-комунікаційних технологій, використання Інтернет-мережі, ІКТ-інфраструктури та діяльності у кібер-просторі.
Дубина М. В., Середюк І. О., Білоус Н. В.	Відносини, що виникають між страховиком та страхувальником у процесі передачі на певних умовах страховику фінансових ризиків, які пов'язані з порушенням роботи інформаційних систем або програмного забезпечення страхувальника в результаті зовнішнього втручання в їхню роботу.
Нагайчук Н. Г., Третяк Н. М., Ткаленко О.	Страховий продукт, що захищає компанію від ризиків, пов'язаних з використанням мережі Інтернет, а також із ризиками, що відносяться до інформаційних технологій, ІТ-інфраструктури та діяльності підприємства у кіберпросторі.
Пікус Р. В., Бабенко Ю. Л.	Страховий продукт, який пов'язаний з передачею фінансового ризику третій стороні, тобто страховій компанії для того, щоб допомогти державі, суспільству, суб'єктам господарювання та фізичній особі зменшити вплив ризику шляхом компенсації витрат, пов'язаних із потенційно руйнівними наслідками кіберзлочинів, забезпечити захист від збитків, що виникають внаслідок порушення безпеки та конфіденційності.
Морозова Л. С., Друхан Д. А.	Вид страхування розглядається як метод управління ризиками та захисту від різних загроз, що виникають при здійсненні електронної комерції.
Шолойко А. С.	Інструмент передачі страховику на договірній основі несприятливих фінансових наслідків ризиків, що виникають у кіберпросторі з фізичними та юридичними особами (страхувальниками), задля зміцнення їх фінансової безпеки шляхом виплати страхового відшкодування.
Поняття «страхування кібер ризиків»	
Desjardins	Захист бізнесу від будь-яких збитків, спричинених кібератаками та витоком даних.
Geico	Тип страхового продукту для бізнесу, який забезпечує покриття ризиків, пов'язаних із використанням комп'ютерів і технологій, зокрема зловмисного програмного забезпечення, фішингових атак, витоків даних, програм-вимагачів, викрадених пристроїв тощо.

Продовження Таблиці В.1

Malwarebytes	Інструмент захисту компанії від ризиків порушення конфіденційності, безпеки, здійснення операцій і послуг через технічну кібернебезпеку чи зловмисників.
OECD	Один із механізмів передачі ризиків для покриття фінансових витрат та відновленні стану суб'єктів, що постраждали внаслідок кібератак.
Trendmicro	Послуга, яку підприємства можуть придбати, щоб зменшити ризики, пов'язані з веденням онлайн-бізнесу, що покриває відповідальність організації за більшість порушень даних, спричинених інцидентом кібербезпеки.
Іванова Т. Г.	Можливість знизити ризик негативних наслідків у сфері інформаційної безпеки та мінімізувати наслідки від інцидентів, що вже відбулися.
Ксьонжик І. В., Жовта Н. А., Павліна А. А.	Дозволяє компенсувати втрати від кіберзагрози, якщо її так і не вдалося нейтралізувати.

Джерело: складено автором на основі [14, с.5; 21, с.190; 28, с.65; 41, с.136; 50, с.25; 51, с.102; 55, с.136; 95, с.103; 107, с.2; 110, с.37; 116, с.523; 129; 131; 154; 230; 231]

Додаток Г

Форма поверхневого скринінгу діяльності страхувальника для виявлення типових кібер-ризиків

1. Загальна інформація про потенційного страхувальника.

Місцезнаходження (місто, адреса)_____

_____

Опис діяльності (сфера, результат діяльності)_____

_____

Дохід за останні 12 місяців (з них % отриманого доходу через онлайн-діяльність, якщо застосовується)_____

Середня кількість працівників за останні 12 місяців_____

2. Бажаний вид страхування.

□ Майнове страхування кібер-ризиків

□ Страхування відповідальності, пов'язаної з кібер-ризиками

3. Інформація, яку використовує потенційний страхувальник.

Кількість записів даних, що використовуються чи передаються	Кількість записів за останні 12 місяців	Середня кількість записів за 1 раз
Особисті дані (ПІБ, місце проживання)		
Ідентифікаційні дані (паспорт, посвідчення і тд.)		
Платіжна інформація (картки, банківські рахунки)		
Пошта в поєднанні з паролем		
Медична інформація		
Інше (за необхідності)		

4. Сервіси передачі інформації, які використовує потенційний страхувальник.

□ Хмарні сховища даних (зазначити, які саме)_____

□ Пошта (зазначити, яка саме) _____

□ Месенджери, включаючи корпоративні (зазначити, які саме) _____

□ Спеціалізовані сховища даних (зазначити, які саме) _____

5. Особливості передачі інформації (поставити відмітку у відповідній колонці).

Особливість	Актуальна для страхувальника	Неактуальна для страхувальника
Наявність політики конфіденційності даних		
Здійснення шифрування даних		
Зберігання власної інформації у 3-х сторін		
Зберігання клієнтської інформації у 3-х сторін		

6. Особливості веб-сайту потенційного страхувальника.

□ Наявність веб-сайту (зазначити посилання) _____

□ Наявність політики конфіденційності на веб-сайті

□ Верифікація інформації, опублікованої на веб-сайті

□ Наявність дозволу на публікацію усіх даних, що опубліковані на веб-сайті

7. Ризик-менеджмент кібер-сфери потенційного страхувальника.

□ Наявність антивірусу на всіх пристроях компанії, що мають доступ до мережі Інтернет

□ Наявність фаєрволу

□ Наявність програми-ідентифікатора вторгнень (моніторингові системи)

□ Використання складних паролів(більше 8 символів)

□ Зміна паролів раз у 3 місяці (або частіше)

□ Наявність стрес-тесту кібербезпеки технологічних систем страхувальника

□ Наявність бек-апів систем

□ Наявність бек-апів інформації

 Проведення чек-апів вразливостей системи з усуненням недоліків раз у 6 місяців (або частіше)

 Використання лише ліцензійного програмного забезпечення

 Використання неліцензійного програмного забезпечення (вказати джерело походження/отримання) _____

 Використання програмного забезпечення з відкритим кодом

 Верифікація отримання прав доступу до систем контролю

 Проведення щорічних освітніх програм для персоналу у сфері кібербезпеки

 Наявність внутрішніх стандартів кібербезпеки

 Використання міжнародних стандартів кібербезпеки (зазначити, які саме) _____

Джерело: складено та доповнено автором на основі [119; 120]

Додаток Д

Таблиця Д.1

ВВП по регіонам світу у 2017 році, трлн дол.

Регіон	2017 рік	
	ВВП, трлн дол.	Частка ВВП, %
Північна Америка	20.2	27%
Європа і Центральна Азія	20.3	27%
Східна Азія та Тихоокеанські країни	22.5	30%
Південна Азія	2.9	4%
Латинська Америка і Карибський басейн	5.3	7%
Субсахарська Африка	1.5	2%
Близький Схід і Північна Африка	3.1	4%
Всього	75.8	100%

Джерело: складено автором на основі [186]

Таблиця Д.2

ВВП по регіонам світу у 2022 році, трлн дол.

Регіон	2022 рік	
	ВВП, трлн дол.	Частка ВВП, %
Північна Америка	27.6	27%
Європа і Центральна Азія	25.3	25%
Східна Азія та Тихоокеанські країни	30.7	30%
Південна Азія	4.4	4%
Латинська Америка і Карибський басейн	6.8	7%
Субсахарська Африка	2.1	2%
Близький Схід і Північна Африка	4.4	4%
Всього	101.3	100%

Джерело: складено автором на основі [186]

Таблиця Д.3

Частка втрат від кіберзлочинів у ВВП по регіонам у 2017 році, %

Регіон	Частка втрат від кіберзлочинів у ВВП, %		
	Мінімум	Максимум	Середнє
Північна Америка	0.69%	0.87%	0.78%
Європа і Центральна Азія	0.79%	0.89%	0.84%
Східна Азія та Тихоокеанські країни	0.53%	0.89%	0.71%
Південна Азія	0.24%	0.52%	0.38%
Латинська Америка і Карибський басейн	0.28%	0.57%	0.43%
Субсахарська Африка	0.07%	0.20%	0.14%
Близький Схід і Північна Африка	0.06%	0.16%	0.11%

Джерело: складено автором на основі [186]

Таблиця Д.4

Оцінка частки втрат від кіберзлочинів регіонів в загальній сумі втрат від кіберзлочинів, %

Регіон	Оціночна частка втрат від кіберзлочинів, %	
	2017	2022
Північна Америка	30%	31%
Європа і Центральна Азія	32%	30%
Східна Азія та Тихоокеанські країни	30%	31%
Південна Азія	2%	2%
Латинська Америка і Карибський басейн	4%	4%
Субсахарська Африка	0%	0%
Близький Схід і Північна Африка	1%	1%
Всього	100%	100%

Джерело: розрахунки автора на основі Таблиць Д.1, Д.2, Д.3

Додаток Е

Таблиця Е.1

Основні показники діяльності страхових компаній України за 9 місяців 2022 р.

Страхова компанія	Премії страхування фінансових ризиків, тис грн.	Виплати страхування фінансових ризиків, тис грн.	Премії страхування майна, тис грн.	Виплати страхування майна, тис грн.	Валові премії, тис грн.	Рівень виплат, %	Приріст премій рік до року, %	Активи, тис грн.
ARX	24629	1441	224084	43702	1957337	39,63	-21,8	4595424
PZU УКРАЇНА	5446	52059	27758	45300	925728	46,25	-28,9	2486150
УНІВЕРСАЛЬНА	11371	437	38807	6714	945929	25,43	6,7	1692842
АРСЕНАЛ СТРАХУВАННЯ	94	1394	27386	157	1123766	46,43	-29,2	2078235
БРОКБІЗНЕС	319	0	5753	152	185162	25,78	0,3	295302
ВУСО	65673	16429	47329	9117	1219365	34,45	-1,5	1034588
ГАРДІАН	28	0	10573	991	629279	17,78	23,2	655946
ЕТАЛОН	17939	10	26106	1	190380	40,35	-18,2	293224
КРАЇНА	139	58	842	89	386043	47,29	-18,9	363080
ОБЕРІГ	12	0	1025	5	210426	40,77	2,4	275020
ПЕРША	3514	26	5671	1016	405960	40,41	-6,7	864673
САЛАМАНДРА	3881	0	2203	26	141268	27,17	47,9	187830
ТАС СГ	25359	2294	22627	3238	1720226	39,28	-4,8	2836014
УНІКА	56406	118739	60435	20447	1924087	50,96	-17,9	3245224

Джерело: складено автором на основі [35; 86]

Продовження додатку Е

Таблиця Е.2

Основні показники діяльності страхових компаній України за 9 місяців 2023 р.

Страхова компанія	Премії страхування фінансових ризиків, тис грн.	Виплати страхування фінансових ризиків, тис грн.	Премії страхування майна, тис грн.	Виплати страхування майна, тис грн.	Валові премії, тис грн.	Рівень виплат, %	Приріст премій рік до року, %	Активи, тис грн.
ARX	91462	9538	321128	46668	2759944	35,82	41,01	5454959
PZU УКРАЇНА	18	1189	20455	4132	1314354	36,89	41,98	2604640
УНІВЕРСАЛЬНА	-	-	55924	40383	1462487	32,36	54,61	2062023
АРСЕНАЛ СТРАХУВАННЯ	26	33	42850	1592	1599612	43,06	42,34	2382908
БРОКБІЗНЕС	149	0	8472	394	273501	31,29	47,71	360521
ВУСО	136057	14249	86465	16333	2005184	33,91	64,44	1725937
ГАРДІАН	93	0	6389	359	1010096	27,88	60,52	996250
ЕТАЛОН	22001	7	13991	1227	258813	35,27	35,95	351692
КРАЇНА	37	0	1151	65	281034	47,54	-27,2	331321
ОБЕРІГ	13	0	776	20	275049	46	30,71	278304
ПЕРША	5152	27	6653	31	599401	32,99	47,65	926863
САЛАМАНДРА	4111	0	1594	0	150827	35,48	6,77	159845
ТАС СГ	24328	2516	26390	4169	2542203	36,71	47,78	3696306
УНІКА	55068	34494	76106	3874	2380917	41,97	23,74	4557283

Джерело: складено автором на основі [35; 86]

Додаток Ж

Таблиця Ж.1

Нормативно-правові дефініції, що стосуються сфери страхування кібер-ризиків в Україні

Нормативно-правовий акт	**Визначення**
Визначення понять, що стосуються сфери страхування кібер-ризиків	
Пункт 1 статті 1 ЗУ «Про страхування»	Операційний ризик – ризик виникнення збитків чи додаткових втрат або недоотримання запланованих доходів внаслідок допущення недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників чи інших осіб, збоїв у роботі інформаційних систем або внаслідок впливу зовнішніх факторів.
Стаття 1 ЗУ «Про захист інформації в інформаційно-комунікаційних системах»	Виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.
	Захист інформації в системі – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.
	Інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.
	Інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.
	Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.
	Несанкціоновані дії щодо інформації в системі – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.
	Порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст.
	Технічний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.
Пункт 3 глави 1 Розділу 1 Постанови НБУ «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах»	Операційний ризик – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок недоліків або помилок в організації внутрішніх процесів, навмисних або ненавмисних дій працівників банку або інших осіб, збоїв у роботі систем банку або внаслідок впливу зовнішніх факторів. Операційний ризик уключає юридичний ризик, однак має виключати ризик репутації та стратегічний ризик.
	Ризик інформаційної безпеки (складова операційного ризику) – імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, уключаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик.

	Ризик інформаційно-комунікаційних технологій (далі – ризик ІСТ) (складова операційного ризику) – імовірність виникнення збитків або додаткових втрат або недоотримання запланованих доходів унаслідок несправності або невідповідності інформаційно-комунікаційних технологій бізнес-потребам банку, що може призвести до порушення їх сталого функціонування, або недоліків в організації управління такими технологіями.
Пункт 3 Розділу 1 Постанови НБУ «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг»	Кіберризик – ризик виникнення збитків та/або додаткових втрат унаслідок реалізації кіберзагроз.
Стаття 1 ЗУ «Про основні засади забезпечення кібербезпеки України»	інцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів
	Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.
	Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів.
	Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.
	Кіберзлочин (комп’ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Продовження Таблиці Ж.1

Стаття 1 ЗУ «Про захист персональних даних»	Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»	Ціль В.2. Формування нової моделі відносин у сфері кібербезпеки - Україна запровадить сервісну модель державної участі у заходах з кіберзахисту, за якої держава сприйматиметься не як джерело вимог, а як партнер у розбудові національної системи кібербезпеки. Досягнення цілі В.2. пропонується виконати за рахунок ряду заходів, зокрема: запровадження системи страхування від кіберризиків, зокрема механізму оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування.

Джерело: складено автором на основі [68-74]

Додаток И

Форма оцінки цільових значень Індикаторів Дорожньої карти впровадження та розвитку страхування кібер-ризиків в Україні

Індикатор	**Назва**	**Цільове значення**	**Оцінка (отриманий бал/ максимальний бал)**
Індикатор 1	Приріст рівня обізнаності населення щодо кіберзагроз	>=0,9	_/1
Індикатор 2	Частка страховиків, які пропонують послуги страхування кібер-ризиків	>=95%	_/1
Індикатор 3	Загальна частка покриття кібер-ризиків	>=85%	_/2
Індикатор 4	Індивідуальна частка покриття кібер-ризиків	>=65%	_/1
Індикатор 5	Відношення фактичного обсягу валових страховий премій зі страхування кібер-ризиків до запланованого обсягу валових страховий премій зі страхування кібер-ризиків	>=95%	_/1
Індикатор 6	Приріст частки валових страхових премій страхування кібер-ризиків у загальних валових преміях	>0	_/2
Індикатор 7	Ріст кількості випадків кібер-шахрайства	<100%	_/1
Індикатор 8	Ріст кількості кібератак, зареєстрованих в Україні	<100%	_/1

Загальний результат: _/10

Оціночний рівень виконання: критичний/середній/високий/оптимальний

Рекомендації щодо наступних заходів для розвитку страхування кібер-ризиків в Україні, сформовані на основі отриманого досвіду:_____

_____

_____

_____

_____

_____

_____

_____

Впровадження результатів дисертаційної роботи

Довідка про впровадження 1

МІНІСТЕРСТВО
ОСВІТИ І НАУКИ
УКРАЇНИ

КИЇВСЬКИЙ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

вул. Володимирська, 64/13
м. Київ, 01601, Україна

Тел.: +38 (044) 239-33-33
E-mail: office@knu.ua
Web: https://www.knu.ua

MINISTRY
OF EDUCATION AND SCIENCE
OF UKRAINE

TARAS SHEVCHENKO
NATIONAL UNIVERSITY
OF KYIV

64/13 Volodymyrska St,
Kyiv, 01601, Ukraine

26.01.2024 № 056/0095

На №

ДОВІДКА

про впровадження результатів дисертаційної роботи
аспіранта кафедри страхування, банківської справи та ризик-менеджменту
Київського національного університету імені Тараса Шевченка
Ломоносової Людмили Сергіївни
у навчальний процес

Основні наукові положення, отримані в результаті дисертаційного дослідження Ломоносової Людмили Сергіївни за напрямом: «Розвиток страхування кібер-ризиків в умовах цифрової економіки» на здобуття наукового ступеня доктора філософії за спеціальністю 072 «Фінанси, банківська справа та страхування», мають наукову та практичну цінність, апробовані та використовуються у навчальному процесі на економічному факультеті Київського національного університету імені Тараса Шевченка.

До переліку результатів дисертаційного дослідження, що впроваджені Ломоносовою Л.С. та застосовуються при викладанні лабораторних та семінарських занять з дисциплін «Страхування» та «Ринок страхових послуг», належать, зокрема, наступні: окреслення економічної природи кібер-ризиків в умовах цифрової економіки; визначення призначення, особливостей та механізму функціонування страхування кібер-ризиків; аналіз нормативно-правової бази, в межах якої здійснюється сучасне регулювання ринку страхування кібер-ризиків в Україні; виявлення стимулюючих та стримуючих факторів розвитку страхування кібер-ризиків в Україні; визначення сучасних тенденцій і трендів страхування кібер-ризиків в Україні та світі.

Проректор
з науково-педагогічної роботи **Андрій ГОЖИК**

Довідка про впровадження 2

ІРПІНСЬКА МІСЬКА РАДА
КИЇВСЬКА ОБЛАСТЬ
ВИКОНАВЧИЙ КОМІТЕТ
вул. Шевченка, 2-а, м. Ірпінь, Бучанський район, Київська область, 08205
тел.: 045-97-61-407, факс: 045-97-61-150,
http://www.imr.gov.ua/, e-mail: imform@imr.gov.ua, код згідно з ЄДРПОУ 05408846

від 14.02. 2024 р. № 01-18/691

ДОВІДКА

про впровадження результатів дисертаційної роботи
Ломоносової Людмили Сергіївни
на тему: «Розвиток страхування кібер-ризиків
в умовах цифрової економіки»

Важливість розвитку страхування кібер-ризиків, як одного з механізмів підвищення кібер-безпеки, в умовах цифрової економіки підтверджується наростаючою кількістю та розмаїттям кібер-загроз. Розвиток страхування кібер-ризиків є системним завданням, що включає підвищення цифрової грамотності населення та рівня цифрової інклюзії.

Для повоєнного відновлення української економіки заслуговують на увагу пропозиції Ломоносової Людмили Сергіївни, аспіранта кафедри страхування, банківської справи та ризик-менеджменту Київського національного університету імені Тараса Шевченка, викладені в дисертаційній роботі на тему «Розвиток страхування кібер-ризиків в умовах цифрової економіки» на здобуття наукового ступеня доктора філософії за спеціальністю 072 «фінанси, банківська справа та страхування», у частині застосування стимулюючих факторів розвитку страхування кібер-ризиків задля підвищення рівня обізнаності населення про кібер-загрози в умовах цифрової економіки та шляхи мінімізації рівня їх настання.

Довідка видана для подання до спеціалізованої вченої ради Київського національного університету імені Тараса Шевченка без фінансових зобов'язань перед автором.

Перший заступник міського голови **Андрій КРАВЧУК**

Довідка про впровадження 3

ARX
A FAIRFAX COMPANY

№024/895
від 17.12.2023р.

ДОВІДКА

про впровадження результатів дисертаційної роботи
аспіранта кафедри страхування, банківської справи та ризик-менеджменту
Київського національного університету імені Тараса Шевченка
Ломоносової Людмили Сергіївни

Надані науково-практичні результати дисертаційного дослідження Ломоносової Людмили Сергіївни за спеціальністю 072 «фінанси, банківська справа та страхування», на тему: «Розвиток страхування кібер-ризиків в умовах цифрової економіки» були використані при розробці стратегічного плану розвитку інноваційних продуктів компанії.

Зокрема, використання заходів в межах запропонованої аспірантом «Дорожньої карти впровадження та розвитку страхування кібер-ризиків в Україні» дозволяє вчасно виявляти та ефективно управляти потенційними ризиками напрямку страхування кібер-ризиків. Застосування індикативного інструментарію оцінки ефективності впровадження та розвитку страхування кібер-ризиків дозволяє якісно оцінювати результати діяльності з просування інноваційного виду страхування та підвищувати його ефективність у майбутньому.

м. Київ Україна
№38
ARX
Ідентифікаційний код 20474912

З повагою,
Шуляк Дмитро
Директор Департаменту розвитку
роздрібного бізнесу КРД
Страхова компанія «ARX»
Mob.: +380 96 088 88 44
Dmitriy.Shulyak@arx.com.ua

Додаток Л

Список публікацій здобувача

Статті в наукових фахових виданнях:

1. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка.* 2020. № 4. URL: https://doi.org/10.32702/2307-2105-2020.4.6. (Особистий внесок автора: визначення характерних особливостей страхового покриття кібер-ризиків як інструменту захисту підприємств від загроз кіберпростору).

2. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Передумови розвитку кібер-страхування. *Інвестиції: практика та досвід.* 2020. № 15-16. С. 28–34. URL: http://dx.doi.org/10.32702/2306-6814.2020.15-16.28. (Особистий внесок автора: розроблено та обґрунтовано періодизацію становлення та розвитку глобального ринку страхування кібер-ризиків).

3. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Дорожня карта впровадження кібер-страхування в Україні. *Innovation and sustainability.* 2021. № 1. С. 64–72. URL: https://doi.org/10.31649/ins.2021.1.64.72. (Особистий внесок автора: запропоновано алгоритм проведення підготовчих заходів для впровадження та розвитку страхування кібер-ризиків в Україні).

4. Prykaziuk N., Lomonosova (Gumenyuk) L. Pandemic COVID-19 as a key factor in the development of DDOS-attacks insurance. *Вісник Київського національного університету імені Тараса Шевченка. Економіка.* 2022. № 1 (218). С. 39–44. URL: https://doi.org/10.17721/1728-2667.2022/218-1/6. (Особистий внесок автора: виокремлено ключові детермінанти розвитку страхування DDoS-атак в світі та здійснено компаративний регіональний аналіз полісів страхування кібер-ризиків).

Монографії:

5. Ломоносова (Гуменюк) Л. С. Фінансова інклюзія як ключовий фактор у відновленні економічного розвитку України після війни. *Transformation of Ukraine's economy: formation of an inclusive economy system and functionality of*

financial inclusion. Рига, 2023. С. 152–169. URL: https://doi.org/10.30525/978-9934-26-321-7-7.

Статті в іноземних наукових виданнях:

6. Lomonosova (Gumenyuk) L. Cyber insurance: modern requirements. *Economics & Education.* 2021. Vol. 6, No. 4. P. 33–36. URL: https://doi.org/10.30525/2500-946x/2021-4-5.

Опубліковані праці апробаційного характеру:

1. Ломоносова (Гуменюк) Л. С. Глобальні соціокультурні тренди поведінкової економіки та їх вплив на розвиток страхування. *Шевченківська весна 2021. Економіка. На шляху до сталого розвитку* : матеріали XIX Міжнар. науково-практ. конф. Київ : К., Інтерсервіс, 2021. С. 296.

2. Ломоносова (Гуменюк) Л. С. Трансформація продуктів кібер-страхування в умовах глобальної пандемії COVID-19. *Економіка. Фінанси. Бізнес. Управління. Зміни. Адаптація. Нова економіка : Діджиталізація ринку фінансових послуг: нові можливості та подолання бар'єрів* : матеріали II Міжнар. форуму, 28 верес.-1 жовт. 2021 р. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2021. С. 22-24.

3. Ломоносова (Гуменюк) Л. С. Перспективи розвитку кібер-страхування в Україні. *Проривні інновації на страховому ринку України*: матеріали V Міжнар. науково-практ. інтернет-конф., 27 жовт. 2021 р. Київ : К.: КНЕУ, 2021. С. 152–154.

4. Ломоносова (Гуменюк) Л. С. Особливості кібер-страхування в процесі адаптації до умов пандемії COVID-19. *Фінансові інструменти сталого розвитку економіки* : матеріали IV Міжнар. науково-практ. конф., 12 трав. 2022 р. Чернівці : Чернівецький нац. ун-т, 2022. С. 436–438.

5. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Забезпечення цифрової грамотності населення як складової національної кібер-безпеки. *Грудневі читання 2022. Стійкість бізнесу і добробут домогосподарств: фінансові та соціальні аспекти* : зб. тез доп. XIV Міжнар. науково-практ. конф., 1-2 груд. 2022 р. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2022. С. 84-85.

6. Lomonosova (Gumenyuk) L. Modern risks: anthropogenic or natural? *Modern Trends in The Development of Science and Technology* : Proceedings of the 3rd international scientific and practical conference, 12-13 December 2022. Innsbruck : LIU, 2022. P. 27-31.

7. Ломоносова (Гуменюк) Л. С. Глобальна невизначеність як драйвер переоцінки бізнес-ризиків. *Шевченківська весна 2023. Повоєнне відновлення економіки України: проблеми та перспективи* : матеріали XXI Міжнар. науково-практ. конф. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2023. С. 129.

8. Приказюк Н. В., Ломоносова (Гуменюк) Л. С. Кібербезпека фінансового сектору України: нові загрози та захисти в умовах повномасштабного вторгнення. *Страховий ринок України у світлі євроінтеграції: новітні виклики та тренди* : зб. матеріалів VI Міжнар. науково-практ. конф., 12 берез. 2023 р. Київ : К.: КНЕУ, 2023. С. 119-121.