

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СТРАХУВАННЯ КІБЕРРИЗИКІВ НА НАЦІОНАЛЬНОМУ РИНКУ

Анотація. У статті розкрито сутність поняття «страхування кіберризиків» та розглянуто основні його напрями відповідно до видів кіберризиків. Наведено найбільші кібератаки на державний, енергетичний, медійний, фінансовий, бізнесовий та некомерційний сектори України за останній рік. Визначено, що український ринок страхування кіберризиків представлений незначною кількістю страхових компаній. Окреслено основні перешкоди та проблеми розвитку страхування кіберризиків на національному ринку. Наведено документи Європейського Союзу у сфері регулювання кіберстрахування, які можуть слугувати основою для України в процесі вдосконалення нормативно-правової бази в сфері страхування кіберризиків. Охарактеризовано можливі перспективи розвитку страхування кіберризиків на національному ринку для підвищення рівня захисту підприємств та населення від кібератак та їх наслідків.

Ключові слова: кіберстрахування, кіберризик, кібератака, кібербезпека, страховий ринок.

Popovych Dariya, Bundz Nataliia,
Ivankiv Viktoriia

Lviv Ivan Franko National University

PROBLEMS AND PROSPECTS FOR THE DEVELOPMENT OF CYBER RISKS INSURANCE ON THE NATIONAL MARKET

Summary. The article reveals the essence of the concept of "cyber risk insurance". It has been determined that the main purpose of cyber insurance is to protect users from cyber threats such as hacker attacks, data theft, viruses and other types of cybercrime. The following types of cyber risks are indicated: the risk of hacking of access passwords or loss of information and system failure due to DDoS attacks, the risk of financial losses due to a computer system failure, the risk of financial losses due to recourse in the event of theft, disclosure or use of personal information, the risk of financial losses due to extortion in the case of computer systems blocked by viruses, the risk of financial losses for the restoration of software and (or) information due to the actions of cybercriminals. The largest cyberattacks on the state, energy, media, financial, business and non-commercial sectors of Ukraine over the past year are listed. It was determined that the Ukrainian cyber risk insurance market is represented by a small number of insurance companies. The main obstacles and problems of the development of cyber risk insurance on the national market are outlined, in particular: lack of clear standards and rules regarding cyber risk insurance, insufficient amount of financial resources of the insurance company, low level of competition between insurance companies, low demand for cyber insurance products and others. The documents of the European Union in the field of cyber insurance regulation are given, which can serve as a basis for Ukraine in the process of improving the regulatory framework in the field of cyber risk insurance. Possible prospects for the development of cyber risk insurance on the national market to increase the level of protection of enterprises and the population against cyber attacks and their consequences are characterized, namely: increasing demand for cyber risk insurance services, cooperation of insurance companies with specialized cyber companies, involvement of technology companies that develop software for protection against cyber attack, raising awareness of cyber security among businesses and the public.

Keywords: cyber insurance, cyber risk, cyber attack, cyber security, insurance market.

Постановка проблеми. З поширенням комп'ютерної техніки та розвитком інтернету кіберризик стали однією з найбільш актуальних проблем у сфері безпеки інформаційних технологій. У зв'язку з цим зросла потреба в захисті від кібератак та інших онлайн-загроз, які можуть завдати значних збитків як громадянам, так і бізнесу. Страхування кіберризиків є одним з можливих заходів, які можуть захистити від можливих втрат.

У сучасних умовах, коли світ постав перед складними викликами – криза COVID-19, війна та, як наслідок, значний перехід на дистанційну роботу, ризики для інформаційної безпеки зросли в декілька разів. Напади на підприємства та організації за допомогою кібератак вже не є рідкістю, а стали повсякденністю. Відновлення

збитків від кібератак може коштувати компанії мільйони доларів, тому страхування кіберризиків набуває все більшої актуальності та значення для бізнесу. У зв'язку з цим, дослідження перспектив розвитку страхування кіберризиків на національному ринку є важливим кроком для забезпечення захищеності інформаційних систем і зменшення можливих наслідків кібератак. Важливо визначити проблеми та перспективи розвитку страхування кіберризиків в Україні, а також розглянути правові та регуляторні аспекти цього процесу.

Аналіз останніх досліджень і публікацій. Дослідженню питань страхування кіберризиків в Україні приділяється увага багатьох вітчизняних та зарубіжних науковців, серед яких: Арчі Дж., Базилевич В.Д., Гудзь О.Є.,

¹ ORCID: <https://orcid.org/0000-0001-6158-444x>

Дем'янчук М.А., Заруба А.Д., Ксьонжик І.В., Партин Г.О., Приказюк Н.В., Фінкл Дж., Хейеса К. Незважаючи на чималу кількість досліджень, проблематика страхування кіберризиків на національному ринку залишається недостатньо розкритою та потребує подальшого дослідження, зокрема у напрямку вдосконалення теоретико-методичних основ кіберстрахування в Україні та їх впровадження з урахуванням досвіду розвинених країн світу.

Мета статті. Головною метою статті є висвітлення основних перспектив розвитку кіберстрахування в Україні, а також дослідження проблем та викликів, які виникають перед страховими компаніями, що пропонують послуги зі страхування кіберризиків.

Виклад основного матеріалу дослідження. Кіберстрахування – це вид страхування, який надає захист від ризиків, пов'язаних з кібербезпекою. Основною метою кіберстрахування є захист користувачів від кіберзагроз, таких як хакерські атаки, крадіжка даних, віруси та інші види кіберзлочинності.

Кіберстрахування є дуже важливим для забезпечення безпеки в інтернеті, оскільки злочинні елементи шукають шляхи вторгнення в приватну інформацію та вигідні їм дані. Без належного захисту організації та індивідуальні користувачі можуть стати жертвами кібератак, що може призвести до втрати даних, фінансових збитків та завдати шкоди репутації.

Протягом останніх років загалом значно зростає кількість кіберризиків, які можуть завдати шкоди як підприємствам, так і фізичним особам. Кіберризики – це ймовірність настання подій, які вражають роботу IT-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 [1]. Кіберризики можуть бути різних видів, зокрема:

- ризик зламу паролів доступу або втрати інформації та збою системи через DDoS-атаки;
- ризик фінансових збитків через збій комп'ютерної системи;
- ризик фінансових втрат через регрес у разі крадіжки, розкриття або використання особистої інформації;
- ризик фінансових збитків через вимагання у випадку заблокованих вірусами комп'ютерних систем;
- ризик фінансових втрат на відновлення програмного забезпечення та (або) інформації внаслідок дії кіберзлочинців [2].

У табл. 1 розглянемо основні напрями кіберстрахування відповідно до наведених вище видів кіберризиків.

27 червня 2017 року став днем, що продемонстрував наскільки вразлива економіка країни до кібератак. За даними кіберполіції, близько 2000 компаній зазнали наслідків здійсненого нападу. Серед постраждалих від атаки були такі великі компанії, як ТОВ «Нова Пошта», мережа магазинів «Епіцентр», промислово-будівельна група «Ковальська», основні українські мобільні оператори, такі як ПАТ «Київстар», ПрАТ «Vodafone» і ТОВ «Lifecell» та інші. Загалом Україна доволі часто зазнає значних кібератак, через які страждають державний, енергетичний, медійний, фінансовий, бізнесовий та некомерційний сектори країни.

У 2022 році кількість кібератак зросла у зв'язку з повномасштабним вторгненням РФ на територію України, про що свідчать дані Дослідницької служби Європейського парламенту. Зокрема, зазначається, що з кінця березня кібератаки включають фішингові електронні листи, націлені на уряд і збройні сили та різні організації, а також використання бекдору LoadEdge для встановлення програмного забезпечення для стеження. Кібернапади на сайти Укртелекому та WordPress спричинили перебої зі зв'язком та обмеження доступу до фінансових та урядових сайтів. 30 берез-

Таблиця 1

Види кіберризиків та напрями кіберстрахування

№	Види кіберризиків	Напрямок кіберстрахування
1.	Ризик зламу паролів доступу або втрати інформації та збою системи через DDoS-атаки	Стосується кіберризиків втрати інформації та збою комп'ютерної системи. Кіберстрахування відшкодує витрати на відновлення інформаційних технологій, таких як веб-сайт.
2.	Ризик фінансових збитків через збій комп'ютерної системи	Відповідає ризику втрати переваг офлайн-страхування. Напрямом страхування є захист IT-компаній від збитків, завданих кіберзлочинцями у разі збоїв комп'ютерної системи. Напрямок страхування підходить для захисту інтернет-магазинів, медіа-кінотеатрів, торрент-систем трекерів.
3.	Ризик фінансових втрат через регрес у разі крадіжки, розкриття або використання особистої інформації	Суть полягає в тому, що власники даних можуть втратити регрес, коли кіберзлочинці крадуть, розкривають та використовують їх особисту інформацію. Цей вид страхування компенсує компаніям збитки, завдані зверненням власників персональних даних.
4.	Ризик фінансових збитків через вимагання у випадку заблокованих вірусами комп'ютерних систем	Кібер-вимагання через примусову оплату (наприклад, за допомогою текстового повідомлення) за розблокування інформаційних систем або інформації під час попереднього блокування комп'ютерних програм чи баз даних. Кіберстрахування покриває витрати на розблокування інформаційних систем під час підтвердження витрат застрахованого та документування кіберзлочинів.
5.	Ризик фінансових втрат на відновлення програмного забезпечення та (або) інформації внаслідок дії кіберзлочинців	За сутністю подібне до страхування майна і стосується кіберризиків фінансових втрат через пошкодження програмного забезпечення та/або інформації кіберзлочинцями. Кіберстрахування відшкодує вартість програмного забезпечення та/або відновлення інформації.

Джерело: розроблено авторами за даними [2]

ня 2022 року за допомогою викрадача інформації MarsStealer було отримано доступ до облікових даних українських громадян та організацій.

Подібним способом у квітні хакери «втягнули» конфіденційну інформацію та облікові дані користувачів в українських урядових установах та медіаструктурах. Вони також заволоділи банківськими та платіжними даними громадян за допомогою троянської програми та шахрайського опитування через сторінки в соціальних мережах. Інші кібератаки мали на меті заподіяти шкоду населенню. Одним із прикладів таких атак була спроба перешкодити роботі електростанцій та припинити постачання електроенергії мільйонам людей. У результаті останньої атаки вдалося зупинити роботу української поштової служби під час випуску серії поштових марок, присвячених війні [3].

Після серії масштабних кібератак на український бізнес і державний сектор протягом останнього року, вітчизняні підприємці почали задумуватися про можливість захисту від подібних ризиків. Хоча така практика на вітчизняному страховому ринку ще не є загальноживаною, і далека від світових обсягів, українські страхові компанії підтверджують, що попит на такий продукт на вітчизняному ринку є. Вони зауважують, що перш за все цікавість до кіберстрахування може бути виявлена компаніями, що мають значні бази даних.

Варто зазначити, що у 2018 році було прийнято Закон України «Про основні засади забезпечення кібербезпеки України», який передбачає створення національної системи кібербезпеки та інші механізми захисту від кіберзагроз [4]. Окрім цього, уряд України активно сприяє розвитку кібербезпеки, зокрема, через підтримку кібербезпекових заходів та ініціатив, фінансування проектів з цієї галузі, розробку та впровадження національної стратегії кібербезпеки. Це свідчить про те, що влада та приватний сектор розуміють важливість цієї сфери. Та, незважаючи на це, український ринок страхування кіберризиків представлений невеликою кількістю страхових компаній, серед яких: ПрАТ «UPSK» та ПрАТ «АСКА». Страхова компанія «UPSK» пропонує комплексне страхування, яке покриває всі можливі ризики, тоді як «АСКА» пропонує індивідуальний підхід, дозволяючи клієнтам вибрати тільки необхідні ризики, в залежності від специфіки їх господарської діяльності.

Мала кількість компаній, які надають послуги зі страхування кіберризиків пояснюється низкою проблем, що характерні для даного виду страхування. Однією з головних проблем розвитку страхування кіберризиків в Україні є відсутність чіткої законодавчо-нормативної бази, яка регулює цю сферу. Закон України «Про страхування» [5] не визначає кіберстрахування як окремий вид страхування, що ускладнює його розвиток в Україні.

На сьогодні в Україні відсутні чіткі стандарти та правила стосовно страхування кіберризиків, що може створювати проблеми при встановленні відповідальності за збитки внаслідок кібератак, а також при визначенні вартості страхування. Також відсутність нормативної бази ускладнює здійснення контролю за дотриманням страховиками вимог щодо страхування кіберризиків та захисту персональних даних клієнтів. Тому,

для розвитку кіберстрахування в Україні необхідно створити відповідну законодавчу базу, яка б дозволила страховим компаніям розробляти та запроваджувати продукти, які б зменшували наслідки ризиків кібератак та сприяли розвитку цієї галузі. Крім того, важливо враховувати міжнародний досвід в цій сфері, оскільки багато країн вже розробили свої власні стандарти та законодавчі норми для здійснення кіберстрахування. Наприклад, у 2018 році Європейський Союз прийняв General Data Protection Regulation (GDPR), який захищає основні права та свободи фізичних осіб і, зокрема, їхнє право на захист персональних даних. Також у 2023 році набула чинності Directive NIS2, яка має позитивний вплив на розвиток ринку кіберстрахування, а саме: інформованості щодо потенційних загроз, усвідомлення необхідності удосконалення системи кібербезпеки та забезпечення превентивних заходів через введені штрафи, особливо для тих галузей, які чітко визначені у директиві NIS: 1) інтернет-ринок; 2) пошукова система в Інтернеті; 3) служби хмарних обчислень [1]. На нашу думку, ці документи можуть послужити основою для України в процесі вдосконалення нормативно-правової бази в сфері страхування кіберризиків.

Недостатній обсяг фінансових ресурсів українських страхових компаній також можна вважати проблемою для страхування кіберризиків, оскільки це може призвести до того, що страховики не зможуть виплатити відшкодування збитків своїм клієнтам в разі кібератаки. Крім того, це може призвести до зменшення довіри клієнтів до страхової компанії та загрожувати її репутації.

Наступною вагомою проблемою є низький рівень конкуренції між страховими компаніями, що призводить до обмеження вибору для клієнтів, високих цін на страхування та обмеження доступу до нових технологій та продуктів у цьому сегменті. Конкуренція між страховими компаніями є важливою складовою розвитку будь-якого ринку страхування, оскільки вона стимулює компанії до розвитку нових продуктів, покращення якості обслуговування та зниження цін. Низький рівень конкуренції може призвести до того, що страхові компанії не будуть мотивовані до вдосконалення своїх продуктів та послуг, що в результаті може призвести до зниження рівня якості страхування кіберризиків.

Крім згаданих вище проблем, можна виокремити наступні:

- відсутність досвіду страхових компаній з регулювання ситуацій настання страхових подій, пов'язаних з втручанням в інформаційний простір держави, суб'єктів господарювання і населення;

- небажання клієнтів надавати необхідний для виявлення страхових випадків доступ до своїх інформаційних систем;

- відсутність довіри юридичних і фізичних осіб до діяльності страхових компаній і ринку кіберстрахування;

- відсутність наукового обґрунтування методики визначення показників оцінювання та розрахунку кіберризиків, стандартів оцінки збитків від настання кібератак та суми їх відшкодування страховальниками;

- низький попит на продукти кіберстрахування [6].

Незважаючи на існуючі проблеми в галузі страхування кіберризиків, ми вважаємо, що цей вид страхування буде розвиватися в Україні, оскільки він є важливим інструментом захисту від кібератак та їх наслідків. За даними дослідження IBM Global Average Data Breach, у 2022 році глобальні втрати даних від кібератак становили 4,4 мільйона доларів, порівняно з 4,2 мільйона у 2021 році та 3,9 мільйона доларів у 2020 році [7]. Розвиток ринку кіберстрахування може також позитивно вплинути на інші сфери, зокрема на сферу інформаційної безпеки та кібербезпеки загалом.

Основним напрямком розвитку страхування кіберризиків в Україні є збільшення попиту на ці послуги. Компанії та організації з особливо високими ризиками кібератак будуть шукати способи захисту своїх даних та інформації, а страхування кіберризиків може стати важливим інструментом у зменшенні фінансових втрат в разі кібератак. Важливим є розвиток нових продуктів та пакетів страхування кіберризиків, що будуть враховувати специфіку різних галузей та видів діяльності. Наприклад, страхування кіберризиків може включати страхування від втрати даних, зниження репутації, відшкодування збитків клієнтам та інші опції.

Одним із можливих напрямів розвитку кіберстрахування в Україні може стати співпраця страхових компаній зі спеціалізованими кіберкомпаніями. Це дозволить страховим компаніям отримати необхідний досвід у цій сфері та розробляти більш ефективні стратегії захисту. У додаток до страхування кіберризиків компанії можуть надавати послуги з відновлення даних, допомоги у відновленні репутації компанії після кібератаки, а також консультації з питань кібербезпеки. Такі послуги можуть стати додатковими перевагами для клієнтів та зробити продукти страхування кіберризиків більш привабливими.

Також, страхові компанії можуть залучати до своєї роботи технологічні компанії, які розро-

бляють програмне забезпечення для захисту від кібератак. Це дозволить страховим компаніям отримати доступ до новітніх технологій та інструментів, які можуть допомогти у запобіганні кібератак та зменшенні їх наслідків.

Окрім цього, дуже важливою є освіта та зростання інформованості про кібербезпеку серед бізнесу та населення. Страхові компанії можуть допомогти в цьому, проводячи навчання та конференції з питань кібербезпеки, в яких можуть брати участь як їх клієнти, так і широкий загал.

Узагальнюючи, можна зазначити, що розвиток страхування кіберризиків в Україні є важливим напрямом розвитку страхового ринку. Це дозволить підвищити рівень захисту компаній та населення від кібератак та їх наслідків, а також дасть змогу залучити нових клієнтів страховикам.

Висновки. Таким чином, кіберстрахування є новим та недостатньо дослідженим в Україні, проте стає все більш актуальним у зв'язку з необхідністю захисту українських компаній та організацій від кібератак. Незважаючи на існуючі складнощі, які пов'язані з оцінкою ризиків, формуванням продуктів страхування та розвитком правової бази, кіберстрахування має потенціал для росту на українському ринку. Цей вид страхування може стати ефективним інструментом захисту від кібератак, особливо з урахуванням зростаючих збитків від кіберзлочинності в усьому світі. Крім того, розвиток ринку кіберстрахування може сприяти покращенню інформаційної безпеки та кібербезпеки в цілому.

Загалом можна стверджувати, що розвиток страхування кіберризиків є важливим фактором для забезпечення безпеки та стабільності в інформаційній сфері. Цей процес є динамічним та вимагає постійної уваги та підвищення рівня компетенції страхових компаній та користувачів. Тому, для успішного розвитку страхування кіберризиків на національному ринку необхідно постійно працювати над вирішенням проблем та удосконаленням практики страхування в цій сфері.

Список літератури:

1. Пікус Р.В., Бабенко Ю.Л. Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава*. 2022. № 2. С. 134–140. URL: http://www.economy.in.ua/pdf/2_2022/25.pdf (дата звернення: 18.04.2023).
2. Проблеми розвитку страхування в Україні : наук. студ. зб. / за заг. ред. проф. В.Й. Плиси. Львів, 2022. 174 с.
3. Пшетачник Я., Тарпова С. Війна росії проти України: хронологія кібератак. Дослідницька служба Європейського парламенту. 2022. С. 1–8. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI\(2022\)733549_XL.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf) (дата звернення: 19.04.2023).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 21 червня 2018 р. № 2469-VIII / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 19.04.2023).
5. Про страхування : Закон України від 7 березня 1996 р. № 85/96-ВР / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/85/96-%D0%B2%D1%80#Text> (дата звернення: 19.04.2023).
6. Партин Г.О., Гребенюк А.В. Перспективи розвитку кіберстрахування в Україні, та перешкоди його становлення. *Модернізація економіки у контексті інноваційного розвитку: напрями та пріоритети* : матеріали міжнар. наук.-практ. конф. (Дніпро, 17 листопада 2018 р.). Дніпро, 2018. С. 32–33.
7. Середня вартість збитків від витоку даних від кібератак у світі в 2022 році зросла до \$ 4,4 млн. *Forinsurer*. 2023. URL: <https://forinsurer.com/news/23/02/20/42397> (дата звернення: 20.04.2023).

References:

1. Pikus R., Babenko Y. (2022) Kiberstrakhuvannia: novi mozhlyvosti dlia strakhovoho rynku Ukrainy [Cyber insurance new opportunities for the insurance market of Ukraine]. *Ekonomika ta derzhava – Economy and the state*, no. 2, pp. 134–140. Available at: http://www.economy.in.ua/pdf/2_2022/25.pdf (accessed April 18, 2023).
2. Plysa V. (ed) (2022) *Problemy rozvytku strakhuvannia v Ukraini* [Problems of insurance development in Ukraine]. Lviv: Ivan Franko National University of Lviv.
3. Pshetachnyk J., Tarpova S. (2022) Viina rosiu proty Ukrainy: khronolohiia kiberatak [Russia's war against Ukraine: chronology of cyberattacks]. *Doslidnytska sluzhba Yevropeiskoho parlamentu – Research Service of the*

- European Parliament, pp. 1–8. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI\(2022\)733549_XL.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf) (accessed April 19, 2023).
4. Verkhovna Rada Ukrainy. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [About the main principles of ensuring cyber security of Ukraine]. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (accessed April 19, 2023).
 5. Verkhovna Rada Ukrainy. Pro strakhuvannia [About insurance]. Available at: <https://zakon.rada.gov.ua/laws/show/85/96-%D0%B2%D1%80#Text> (accessed April 19, 2023).
 6. Partyn H., Hrebeniuk A. Perspektyvy rozvytku kiber-strakhuvannia v Ukraini, ta pereshkody yoho stanovlennia [Prospects for the development of cyber insurance in Ukraine, and obstacles to its formation]. *Modernizatsiia ekonomiky u konteksti innovatsiinoho rozvytku: napriamy ta priorytety*: Mizhnarodna naukovo-praktichna konferenciya (Dnipro, November 17, 2018).
 7. Serednia vartist zbytkiv vid vytoku danykh vid kiberatak u sviti v 2022 rotsi zrosla do \$ 4,4 mln. *Forinsurer* [The average cost of losses from data leakage from cyberattacks in the world in 2022 has increased to \$ 4.4 million. Forinsurer]. Available at: <https://forinsurer.com/news/23/02/20/42397> (accessed April 20, 2023).