

Р. В. Пікус,

к. е. н., професор, професор кафедри страхування, банківської справи та ризик-менеджменту, Київський національний університет імені Тараса Шевченка
ORCID ID: 0000-0002-1951-148X

Ю. А. Бабенко,

студентка магістратури, спеціальність "Фінанси, банківська справа та страхування", Київський національний університет імені Тараса Шевченка
ORCID ID: 0000-0001-9244-5880

DOI: 10.32702/2306-6806.2022.2.134

КІБЕРСТРАХУВАННЯ: НОВІ МОЖЛИВОСТІ ДЛЯ СТРАХОВОГО РИНКУ УКРАЇНИ

R. Pikus,

PhD in Economics, Professor, Professor of the Department of Insurance, Banking and Risk Management Taras Shevchenko National University of Kyiv, Kyiv
Y. Babenko,

Master's student of the Department of Finance, banking and risk management, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

CYBER INSURANCE: NEW OPPORTUNITIES FOR THE INSURANCE MARKET OF UKRAINE

У статті уточнено теоретико-методичні основи щодо визначення змісту та витоків поняття "кіберризик", наведено авторську конструкцію тлумачення змісту за обраними критеріями. Визначено зміст та основні завдання кіберстрахування як ефективного інструменту фінансування втрат за наслідками кіберризиків. Виявлено та проаналізовано особливості розвитку кіберстрахування в Україні та розвинених країнах світу. Узагальнено особливості та структуровано характеристики послуг із кіберстрахування. Охарактеризовано можливі варіанти страхового покриття кібервідповідальності з відокремленням покриття відповідальності першої і третіх осіб, а також кіберстрахування як різновиду майнового страхування. Окреслено напрями вдосконалення нормативно-правової бази розвитку кіберстрахування з урахуванням досвіду розвинених країн світу. Визначено стримуючі фактори та перспективи розвитку кіберстрахування в Україні з метою захисту від кіберзагроз інтересів фізичних та юридичних осіб.

The article clarifies the theoretical and methodological basis for determining the content and origins of the concept of "cyber risk", the author's construction of the interpretation of the content according to the selected criteria. Cyber risk is the likelihood of events affecting an organization's IT systems and cybersecurity due to the interference of digital and other electronic technologies, resulting in losses, destruction of digital assets and possible loss of the organization's reputation.

It was found that cybersecurity of systems in the modern information world is an extremely important tool for the protection of economic entities, and cyber insurance is one of the tools for its implementation. The content and main tasks of cyber insurance as an effective tool for financing losses due to cyber risks are identified. "Cyber insurance" can be defined as an insurance product that involves the transfer of financial risk to a third party, ie an insurance company, in order to help the state, society, businesses and individuals reduce the impact of risk by compensating for costs associated with potentially devastating consequences of cybercrime, provide protection against damage resulting from breaches of security and confidentiality.

The peculiarities of cyber insurance development in Ukraine and in developed countries of the world are revealed and analyzed. Features and characteristics of cyber insurance services are generalized and structured. There are two approaches to the formation of coverage of cyber risks in insurance: cyber liability insurance and property insurance of the consequences of possible cyber attacks.

Possible options for cyber liability insurance coverage with the separation of first and third party liability coverage, as well as cyber insurance as a type of property insurance are described. The directions of improving the regulatory framework for the development of cyber insurance are outlined, taking into account the experience of developed countries.

It is determined that the European Directive has a positive impact on the development of the cyber insurance market, namely awareness of potential threats, awareness of the need to improve cybersecurity and provide preventive measures through fines, especially for the Internet market, Internet search engines, cloud computing services. Restraining factors and prospects of cyber insurance development in Ukraine in order to protect the interests of individuals and legal entities from cyber threats have been identified.

Ключові слова: страховий ринок, страхова послуга, кіберризик, кіберстрахування, кібератака, кібербезпека, кібервідповідальність.

Key words: insurance market, insurance service, cyber risk, cyber insurance, cyber attack, cybersecurity, cyber responsibility.

ПОСТАНОВКА ПРОБЛЕМИ

Глобальна пандемія, яка розпочала нову еру віддаленої роботи, продемонструвала, що людство як ніколи є надзвичайно вразливим до кібератак, особливо тоді, коли все більше людей та компаній впроваджують використання нових технологій. Компанія, що має цифрові активи, є потенційною жертвою атаки програмою-зловим, злому інформаційних систем, зараження шкідливим програмним забезпеченням або фішингом та інших кібератак. Наслідки кібератак, наприклад, витік даних з серверів, можуть бути дуже істотними і не обмежуються прямими витратами на відновлення пошкодженої техніки.

У зв'язку зі зростанням масштабності кіберзлочинів ризик-менеджмент компаній повинен ввести до свого списку додаткову загрозу, якій раніше не приділяв значної уваги і, як наслідок, розпочати пошук шляхів оптимізації кібербезпеки серед яких — технологічна безпека, ознайомча робота із протидією та профілактикою кіберзлочинів, а також кіберстрахування. Цей вид страхування забезпечує фінансовими можливостями компанію щодо відновлення після великих втрат, повернення попередньої ефективності, дозволяє зберегти платоспроможність та знизити рівень витрат внаслідок простою виробництва, викликаного різного роду кіберзагрозами.

Підвищена зацікавленість та попит у підприємств і бізнесу щодо ринкових інструментів фінансування кібервтрат, особливо в умовах коли Україна і світ все частіше потрапляють під масовий вплив кібератак, актуалізує кіберстрахування, як особливий різновид страхового продукту і для страхових компаній. Тому реагуючи на потреби ринку серед страхових компаній постало завдання відпрацювати сучасну практику кіберстрахування, сформулювати перелік страхових продуктів, які можуть виступити такими інструментами фінансування.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Серед наукових досліджень присвячених кіберстрахуванню існують різні напрямки. Розвиток кіберстрахування в різних країнах світу, в тому числі і в Україні висвітлені в роботах таких вчених: Бем Р., Бернар Ю., Берк Д., Братюк В., Гудзь О., Ільчук В., Кафенбергер А., Кордоньєр А., Нагайчук Н., Приказюк Н., Тіглен М., Третьяк Н., Мак А. Слід зазначити, що в роботах зарубіжних вчених більша увага приділялася аналізу складових компонентів страхових тарифів, розширенню можливостей для компаній у забезпеченні своєї кібербезпеки, аналізу відповідних страхових портфелів та інш. Серед українських вчених більшою мірою переважають дослідження щодо можливостей та перспектив впровадження кіберстрахування як нового виду страхування. Сучасні виклики в економіці і суспільстві, зростання масових кібератак обумовлюють необхідність подальшого розвитку кіберстрахування в Україні на основі подальшого відпрацювання його теоретико-методичних основ, а також розробки практичних рекомендацій розвитку з урахуванням позитивного досвіду розвинених країн світу. Зазначене свідчить про особливу актуальність теми наукової роботи.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ

Метою роботи є удосконалення теоретичних основ та розробка практичних рекомендацій щодо розвитку кіберстрахування в Україні як інструменту фінансової безпеки юридичних та фізичних осіб.

Для досягнення поставленої мети в роботі окреслено і вирішено такі завдання:

- уточнено зміст та еволюція категорії "кіберризик";
- визначено зміст та основні завдання кіберстрахування;
- виявлено особливості розвитку ринку кіберстрахування в Україні та світі;
- наведена характеристика нормативно-правової бази функціонування кіберстрахування в Україні і світі;
- узагальнені особливості та виокремлені характеристики продукту кіберстрахування;
- визначено перспективи впровадження кіберстрахування для фізичних та юридичних осіб в Україні на основі міжнародного досвіду.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

У процесі дослідження використовувалися загальнотеоретичні та спеціальні методи: при уточненні наукових підходів до визначення кіберризиків використовували методи критичного аналізу літературних джерел та наукової абстракції, при розкритті змісту та основних завдань кіберстрахування — методи абстрагування і конкретизації; при виявленні особливостей ринку кіберстрахування — аналіз і синтез, порівняльний аналіз; при виокремленні нормативно-правової бази функціонування ринку кіберстрахування використовували системний підхід; при узагальненні міжнародного досвіду кіберстрахування та наданні пропозицій щодо його реалізації в Україні використано аналогію та логічне узагальнення.

Інформаційна база дослідження

Інформаційну базу дослідження становили статистичні матеріали Національного банку України, Європейської асоціації зі страхування та пенсійного забезпечення (EIOPA), відповідні наукові статті вітчизняних та зарубіжних вчених.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Головним об'єктом кіберстрахування є кіберризик. Визначення сутності поняття "кіберризик" наведено в роботах багатьох авторів і вирізняється, насамперед, цілями і підґрунтям. Відповідно до Chief Risk Officer Forum (групи професійних менеджерів з ризиків страхової галузі) поняття "кіберризик" охоплює такі позиції:

- це будь-який ризик, що виникає внаслідок використання та передачі електронних даних, включаючи

такі технологічні засоби, як Інтернет та телекомунікаційні мережі;

— фізичні збитки, які можуть бути завдані кібератаками;

— шахрайство внаслідок неправильного використання даних;

— неправовий доступ до конфіденційної електронної інформації, пов'язаної з фізичними особами, компаніями або урядом [10].

Українські дослідники наводять своє розуміння даної категорії. Наприклад, С. Волосович визначає, що кіберризик — це операційний ризик, який полягає в отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі [1], а Н. Приказюк розуміє під кіберризиком ймовірність виникнення збитків через збій у системі інформаційних технологій організації [5].

У трактуванні категорії "кіберризик" наведеними науковцями відсутні або результат, або зміст явища, і тому вони не містять в собі повноцінного опису вказаної категорії. При формуванні власного тлумачення змісту поняття "кіберризик" ми маємо звернути увагу на суть явища, а саме, що це, як зазначає Н. Приказюк, ймовірність настання, але не збитків, а подій; зміст явища, який докладно описують Chief Risk Officer Forum і полягає в тому, що кіберризик вражають роботу IT-систем та кібербезпеку організації через стороннє втручання цифрових та інших електронних технологій; та на результат — настання кіберризиків призводить до отримання збитків, руйнування цифрових активів та можливої втрати репутації організації.

Отже, кіберризик — 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.

При з'ясуванні сутності кіберстрахування слід звернути увагу на сферу діяльності сучасних технологій і розмежувати його зміст із змістом таких понять: "страхування кібервідповідальності", "страхування кібербезпеки", "страхування кіберризиків". За визначенням Нагайчук Н. кіберстрахування — це страховий продукт, що захищає компанію від ризиків, пов'язаних з використанням мережі Інтернет, а також із ризиками, що відносяться до інформаційних технологій, IT-інфраструктури та діяльності підприємства у кіберпросторі [3]. Такої ж думки дотримується і Гудзь Г., який характеризує кіберстрахування як страховий продукт, що захищає економічні суб'єкти від ризиків, які відносяться до інформаційно-комунікаційних технологій, використання Інтернет-мережі, ІКТ-інфраструктури та діяльності у кіберпросторі [2].

Німецькі дослідники Р. Бем і Г. Шварц під страхуванням кіберстрахування розуміють передачу фінансового ризику, пов'язаного з мережевими та комп'ютерними інцидентами, третіх сторін [8].

У наведених трактуваннях змісту кіберстрахування відсутні результати процесу страхування, що призводить до неповноцінного тлумачення сутності поняття. Особливу увагу слід звернути на наслідки використання зазначеного виду страхування для учасників угоди. Компанії самостійно несуть відповідальність за свою кібербезпеку, однак, якщо вони застраховані, то у випадку кібератаки покриття кібервідповідальності забезпечить вирішальну підтримку і допоможе бізнесу продовжити успішне функціонування.

Отже, "кіберстрахування" можна визначити як 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, забезпечи-

Таблиця 1. Можливі варіанти страхового покриття кібервідповідальності

Страхування відповідальності першої особи	Страхування відповідальності третьої особи
Витрати на відновлення даних	Мережева безпека та відповідальність за конфіденційність
Втрата доходу або додаткові витрати	
Кібервикрадення / кібершантаж	Електронна відповідальність за медіа
Витрати на реагування (IT-розслідування, сповіщення клієнтів)	Нормативне провадження
Мінімізація репутаційного збитку	Судові збори, штрафи
Юридична допомога: консультація і захист від вимог третіх осіб	

Джерело: складено авторами на основі [9; 12; 15].

ти захист від збитків, що виникають внаслідок порушення безпеки та конфіденційності.

Кіберстрахування покриває збитки, пов'язані з пошкодженням або втратою інформації з IT-систем та мереж, а також, як правило, включає значну допомогу та управління самим інцидентом, що може бути суттєвим при зіткненні з репутаційними збитками або примусовим регулюванням.

Можна виділити два підходи до формування покриття кіберризиків у страхуванні:

- 1) страхування кібервідповідальності;
- 2) майнове страхування можливих кібератак.

Перший із з них базується на тому, що відповідальність за ризики може покриватися для першої і третьої (тобто сторонньої) особи. Покриття кібервідповідальності третьої особи включає витрати, які компанія безпосередньо зазнає внаслідок порушень, наприклад, інформування клієнтів про хакерську атаку і застосовуються до претензій, які націлені на об'єкта від фізичних та юридичних осіб, які отримали збитки внаслідок дій або бездіяльності об'єкта (табл. 1). Наприклад, клієнт подає до суду за халатність після того, як хакер викраде його особисті дані з комп'ютерної системи та відкриє загальний доступ до них в Інтернеті.

Другий підхід до формування покриття кіберстрахування базується на видах кібератак та кіберінцидентів, які можуть трапитися із компанією та об'єктами, на які вони впливають. Проаналізувавши сучасну практику угод страхування провідних європейських, американських та українських компанії можна виокремити перспективні страхові поліси з майнового кіберстрахування (табл. 2).

Варіантом додаткового покриття в кіберстрахуванні може бути технічна заміна, що включає вартість заміни технічного обладнання. Такий вид покриття підпадає під класифікацію майнового страхування. Проте на страховому ринку відбувається дискусія стосовно включення даного покриття у страховий поліс, оскільки такий тип збитків може бути спричинений операційними помилками незалежно від того чи були технічні виключення, як випадкові, або шкідливі загрози, які можуть обумовити кінетичну шкоду. Тому страхові компанії на власний розсуд вирішують питання щодо доцільності включення даного покриття в страховий поліс, при цьому значно збільшуючи вартість покриття.

Кіберстрахування — це інструмент передачі ризику, який не потрібно розцінювати як забезпечення комп'ютерної безпеки для компанії. Між поняттям "кіберстрахування" та "кібербезпека" існує суттєва різниця. Згідно з Законом України "Про основні засади забезпечення кібербезпеки України": "кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталій розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі" [6].

Таблиця 2. Поліси майнового кіберстрахування

Поліси кіберстрахування	Покриття, які забезпечують поліси
Перерва в процесі виробництва	1. Збитки та відшкодування втрачених прибутків у результаті порушення в роботі IT-системи, мережі та вебсайтів з причини кібератаки (припинення роботи)
Крадіжка активів	1. Відшкодування викупної суми, сплаченої вимагачам, за дешифровку заблокованої інформації підприємства. 2. Витрати, які понесла компанія, відновлюючи інформацію
Знищення або шкода будівлям/обладнанню або іншому майну	1. Витрати у випадку збою безпеки мережі, які можуть обумовити витік даних, зараження зловмисним програмним забезпеченням: юридичні витрати, IT-криміналістика, відновлення даних, експертиза зв'язків з громадськістю. 2. Порушення безпеки комп'ютерної системи (Dos- та DDos-атаки, ураження вірусами, знищення, модифікація або видалення інформації)
Соціальна інженерія (нецільова атака)	Збитки від втрати грошових коштів і активів страхувальника, що сталися в результаті застосування технологій фішингу, картингу (нецільові атаки)
Технічна заміна	Вартість заміни технологічного обладнання, яке стає непридатним при атаці зловмисного програмного забезпечення

Джерело: складено авторами на основі [9; 12; 15].

Кіберстрахування можна вважати і запобіжним заходом кібербезпеки, але за жодних обставин цей вид страхування не може бути заміною міцної бази безпеки, яка вимагає сучасних технологій кібербезпеки, навчених команд та перевірених процедур. Якщо не досягти необхідного рівня безпеки, страхувальники можуть відмовитися укласти договір страхування, а страховики суттєво підвищать вартість страхування.

Із збільшенням кількості додатків, програмного забезпечення, пристроїв будь-якої організації стає більш вразливою до кібератак. Отже, кіберризик (зокрема фінансові) стають іманентно притаманною складовою діяльності організації і вимагають кіберстрахування як норми здорового економічного глузду.

Кіберстрахування може відігравати ключову роль у підтримці бізнесу будь-яких розмірів, воно може забезпечити стійкість бізнесу до порушень кібербезпеки, а в найгіршому випадку, допомогти відновити бізнес після масштабних кібератак.

Термін "кіберстрахування" зародився в США і такий продукт в основному зосереджувався на зобов'язаннях третьої сторони, які пов'язані з порушенням даних та конфіденційності, включаючи витрати на сповіщення. Такий акцент обумовлений порушенням законів про сповіщення, які прийняті у більшості штатів США і передбачають, що бізнес повинен повідомити про загрози лише постраждалих сторін, якщо є докази, які обґрунтовано припускають, що їх особисті дані будуть використовуватися зловмисно.

Історично це відрізняється від країн Євросоюзу, де натомість основну увагу зосереджено на покритті витрат за наслідками перерв у бізнесі через кіберінциденти.

З часом ця невідповідність і відтепер регулюється положенням про захист даних General Data Protection Regulation (GDPR) [14], прийнятим Європейським Союзом 25 травня 2018 року. Цей Регламент захищає основні права та свободи фізичних осіб і, зокрема, їхнє право на захист персональних даних.

У 2016 році, в рамках стратегії кібербезпеки ЄС, Європейська Комісія запропонувала директиву щодо мережевої та інформаційної безпеки ЄС (NIS: Directive on security of network and information systems). Директива NIS є першою частиною законодавства про кібербезпеку в усіх країнах ЄС. Підвищення кібербезпеки в Євросоюзі є основною метою Директиви NIS шляхом

встановлення загального рівня безпеки мережевих та інформаційних систем [13].

Європейська Директива 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 [13].

Оскільки Україна не входить до ЄС, Директива NIS не є зобов'язуючою, однак вона служить настановою з питань належної практики. Деякі з її положень було добровільно впроваджено в українському законодавстві, проте інші залишаються без уваги.

У 2005 році Україна ратифікувала Будапештську конвенцію — перший міжнародний договір, який прагне вирішити питання кіберзлочинності шляхом гармонізації національного законодавства, вдосконалення методик розслідування та посилення співпраці між країнами [4].

Окрім цього, у 2016 році було прийнято Стратегію кібербезпеки України, яка визначає пріоритети та напрямки розвитку кібербезпеки і є важливим структурним елементом для формування політики у сфері кібербезпеки, яка відповідатиме світовому рівню [7]. Для реалізації Стратегії кібербезпеки Парламент України ухвалив Закон "Про основні засади забезпечення кібербезпеки України" — основний законодавчий акт, що встановлює правові рамки для системи кібербезпеки [6].

Ця правова база є основою для подальшого розвитку ринку кіберстрахування в Україні, створює можливості щодо оцінки ефективності діяльності страховиків у боротьбі із кіберзлочинами шляхом створення необхідних страхових продуктів які можна запропонувати потенційним клієнтам.

Отже, страхування кіберризиків, на відміну від традиційного страхування, призначене для задоволення потреб фізичних та юридичних осіб у розбудові власної кібербезпеки. Поліс страхування кіберризиків, який також називають кіберстрахуванням чи страховим покриттям кібервідповідальності, призначений пом'якшити вплив кіберризиків шляхом компенсації витрат, пов'язаних із відновленням після порушень в кібербезпеці. Покриття кібервідповідальності може забезпечити вирішальну підтримку щодо відновлення і подальшого розвитку.

Страховим компаніям необхідно активно розвивати ринок кіберстрахування, адже зазначений сегмент може стати для них "блакитним океаном". Сучасні реалії розвитку страхового ринку України дозволяють зробити висновки стосовно факторів, що перешкоджають впровадженню і розвитку страхування кіберризиків: не існує довіри на стандартні послуги страхування, а такий інноваційний продукт як кіберстрахування взагалі не організує своє коло споживачів; не існує конкретних видів кіберстрахування, лише комплексні продукти, які націлені на страхування різних об'єктів з приводу одного виду небезпеки, наприклад — кібератаки.

Визначення драйверів такого сприйняття та підвищення страхової обізнаності можуть допомогти збільшити попит на страхування кіберризиків. Проте ефективність комунікаційних стратегій для покращення обізнаності та сприйняття кіберризиків також ставиться під сумнів на сучасному етапі.

Компаніям потрібно вкладати гроші в людей, процеси та системи. Зокрема, існує потреба у працівниках, які можуть допомогти усунути розрив між бізнес-менеджерами та ІТ-спеціалістами. Враховуючи нинішні обмеження безпеки, дизайн кіберстрахових продуктів та інноваційні способи передачі кіберризиків можуть бути цікавими сферами для бізнес-досліджень. Надалі можуть виникнути нові та інноваційні бізнес-моделі, які знижують та передають кіберризик, наприклад, через блокчейн.

Особливою рисою страхування кіберризиків є те, що потреба на нього формується в процесі виникнення кібератак або потенційних кіберзагроз. Відповідна пропозиція на ринку залежить від персональних особливостей настання кіберінцидентів у страхувальників, ціни страхового полісу, величини прибутку страховиків та повернення збитків від виникання страхових випадків, спроможності останніх узгоджувати страхові договори через Інтернет (оформлення онлайн-полісів).

Для ринку кіберстрахування характерна консервативна модель побудови, і страховикам необхідно: будувати репутацію серед страхувальників шляхом удосконалення страхових пропозицій у сфері інформаційної безпеки; аналізувати тенденції на кіберринку для можливості надання актуальних пропозицій.

Наприклад, з 2020 року розпочали впроваджувати технологію 5G, що може призвести до більш швидкої та розширеної мережі пристроїв IoT. Така новація відразу призведе до більших DDoS-атак і нових викликів щодо кібербезпеки. Страхові компанії повинні звернути особливу увагу на цю загрозу ще до її масштабного впливу.

Характерною тенденцією в сфері сучасних кіберзагроз є оновлення програмних забезпечень. Головна загроза полягає в тому, що незахищені вразливості є головною причиною системних компромісів. Підтримка Windows 7 закінчилася 14 січня 2020 року, що призвело до появи більше непідтримуваних та незахищених застарілих систем і, як наслідок, може проявитися тенденція до атак, як це було із атакою викупного програмного забезпечення WannaCry, через яку багато організацій зазнали нападу за нерегулярного оновлення операційних систем та використання застарілих та непідтримуваних операційних систем, таких як Windows XP (і незабаром це може стати Windows 7).

Більшість полісів кіберстрахування містять виключення для непідтримуваних систем, і страховики націлені на інформування своїх клієнтів про необхідність оновлення системних забезпечень, як тільки вони стають доступні. Отже, страховики мають забезпечити не тільки функцію страхового захисту, а й інформування для своїх потенційних та майбутніх [11].

Основною проблемою формування страхового захисту за рахунок кіберстрахування на сучасному етапі є відсутність достатніх статистичних даних про кіберзагрози та фінансові наслідки їх впливу, бо компанії не розкривають цю інформацію із власних суджень для

збереження своєї репутації. Для того щоб компанії зберегли свій бренд, а актуарії змогли проводити свої розрахунки та моделювати наслідки, необхідно регулятору страхового ринку (НБУ) започаткувати збір такої інформації. На основі таких даних актуарії зможуть побудувати актуарні таблиці на прикладі майнового або страхування життя.

Зобов'язанням регулятора для збору такої інформації може послужити Загальний європейський регламент щодо захисту даних (GDPR 2018). Його запровадження є обов'язковим для країн Євросоюзу, в тому числі і України, як претендента на повноцінне членство в ЄС, а також у рамках оновленого внутрішнього законодавства щодо кібербезпеки. За його обмеженнями бізнес може бути оштрафований за нерозголошення обставин порушення кібербезпеки — до 20 мільйонів євро або 4% його обороту [14].

Існує кілька ознак розвитку кіберстрахування, які свідчать про відносну незрілість ринку. По-перше, бракує стандартизації страхових пропозицій. Окремі страховики пропонують підходи, які передбачають чіткий поділ між традиційними полісами страхування кіберризиків. Інші страховики вирішили вбудувати кіберзахист в наявне у них покриття, керуючись аргументом, що цей варіант простіше продати клієнтів, ніж цілком новий вид страхування. Однак вкладення кіберстрахування в інше покриття може призвести до недостатньої ясності і якості щодо того, що охоплює такий вид покриття. За таких умов, страховики можуть опинитися в ситуації, коли їм доведеться покривати ті ризики, які можуть принести їм кумулятивний збиток, або не покривати їх і цим самим спровокувати невдоволення своїх клієнтів до страхової компанії та повного комплексу її послуг.

Подальший розвиток кіберстрахування в Україні суттєво залежить і від коректності формування страхових премій. З цієї метою страховим компаніям необхідно розуміти конкретні потреби компаній, переконалися, що вся мережа компанії покрита, а не лише окремі машини чи пристрої, врахувати, чи потрібне страхування третьої сторони (це стосується не тільки компанії та її співробітників, а й усіх клієнтів, дані яких можуть зберігатися на серверах). Це дозволить також уникнути витрат на непотрібні додаткові послуги.

Європейський досвід свідчить, що більше ніж 40% світової страхової премії за страхування кіберризиків припадає на перестраховиків. Для порівняння, у більш розвинених сферах страхової діяльності, таких як страхування майна або відповідальності, частки премій, що передаються перестраховикам, зазвичай залишаються між 10 та 15%. Переважно, страховики перестраховують свій бізнес за допомогою самостійних кібердоговорів, підкреслюючи еволюцію страхування кіберризиків як окремої сфери бізнесу [11]. Характерною тенденцією є укладання договорів пропорційного покриття застрахованих ризиків. Таким чином компанії перестраховують себе від ризиків введення нового виду страхування.

З урахуванням особливих загроз страхування кіберризиків страховики та перестраховики неохоче додають до своїх вже великих і важко оцінених ризиків ризики іншої компанії. Тому як перспективний варіант вирішення перестраховування діяльності страхових компаній у сфері кіберстрахування є використання катастрофічних облігацій, або так званих "cat bonds". Це є прикладом страхової сек'юрітизації, коли створюються цінні папери, пов'язані з ризиком, які передаються певний набір ризиків (як правило, ризики катастрофи, стихійного лиха чи кібератаки) від емітента чи спонсора (компанії, що передає кошти) інвесторам на ринку капіталу.

Типова структура cat bonds (рис. 1) передбачає, що страхова компанія укладає договір про страхування із страхувальником (або контрагентом), отримуючи від нього премії в обмін на забезпечення покриття. Страхова компанія випускає цінні папери інвесторам і отримує взаємні основні суми (заставу). Потім кошти пере-



Рис. 1. Структура реалізації катастрофічних облігацій

Джерело: [16].

кладаються на заставний рахунок, з якого вони, як правило, вкладаються у високорейтингові фонди грошового ринку. Для інвесторів дохід виплати відсотків складається з відсотків, які сплачує страхова компанія з суми застави та премій, які сплачує страховальник [16]. Якщо відбувається страховий випадок, який відповідає умовам активації виплати, страхова компанія ліквідує заставу, необхідну для здійснення платежу, та відшкодовує страховальнику всю суму відповідно до умов транзакції за cat bonds. Якщо страховий випадок не відбувається, застava ліквідується наприкінці строку котирувальної облігації, і повертається інвесторам із нарахованими відсотками.

Катастрофічні облігації сприяють диверсифікації портфеля страховика та можуть розглядатися як супутня інвестиція в рамках основної інвестиційної стратегії. Таким чином, інвестори беруть на себе ризик втрати внаслідок катастрофи або кібератаки, що настає, за привабливі ставки прибутку від інвестиції. Якщо така катастрофа чи названий випадок небезпеки трапиться, інвестори втратять частину або всю основну суму, яку вони інвестували, і емітент (як правило, страхова або перестраховальна компанія, але іноді корпорація або суверенна особа) отримає ці гроші для покриття своїх втрат. Якщо страховий випадок не відбудеться, інвестори отримують більш високу процентну ставку, ніж якби вони розмістили свої інвестиційні гроші в казначейських облігаціях.

З урахуванням сучасного стану розвитку вітчизняного страхового ринку та в умовах особливих викликів для українських компаній такий досвід є доцільним і особливо перспективним стосовно розвитку кіберстрахування.

ВИСНОВКИ

В умовах сучасних викликів для економіки і суспільства в цілому поширення цифрових послуг, використання різноманітних інформаційних технологій обумовлює появу кіберризиків як надзвичайного виду загроз.

Кіберризик — 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.

Одним із найбільш дієвих інструментів у системі ризик-менеджменту стосовно кіберризиків є кіберстрахування. Кіберстрахування можна визначити як 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.

Можна виділити два підходи до формування покриття кіберризиків у страхуванні: страхування кібервідпо-

відальності; і майнове страхування наслідків можливих кібератак.

Нормативно-правове забезпечення інноваційного сегменту страхового ринку — кіберстрахування, знаходиться на стадії формування і в Україні і світі. Європейська Директива щодо мережевої та інформаційної безпеки ЄС є першою частиною законодавства про кібербезпеку в усіх країнах ЄС. Підвищення кібербезпеки в Євросоюзі є основною метою Директиви NIS шляхом встановлення загального рівня безпеки мережевих та інформаційних систем. Європейська Директива має позитивний вплив на розвиток ринку кіберстрахування в Україні особливо для інтернет-ринків, пошукових систем в Інтернеті, служби хмарних обчислень і може стати основою відповідного законодавства в країні.

Страхові компанії України не мають достатніх ресурсів для розробки власного підходу щодо оцінки кіберризиків, а потенційні клієнти не проявляють попиту на відносно новий вид страхування. Проте поточні оцінки і прогнози свідчать, що попит на кіберстрахування щорічно збільшується в геометричній прогресії. Отже, страхові компанії, які зможуть запропонувати якісні кіберстрахові продукти за рахунок високих відсотків на покриття та адекватні страхові премії, зможуть відразу зайняти провідні позиції.

Література:

1. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. Зовнішня торгівля: економіка, фінанси, право. 2018. № 3. С. 101—115. URL: http://nbuv.gov.ua/UJRN/uazt_2018_3_10 (дата звернення: 24.11.2021).
2. Гудзь О. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. Економіка. Менеджмент. Бізнес. № 3 (29). 2019. Ст. 4—12. DOI: 10.31673/2415-8089.2019.030412.
3. Нагайчук Н.Г., Третяк Н.М., Ткаленко О. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. Фінансовий простір. 2019. № 1 (33). С. 97—111. DOI: 10.32702/2307-2105-2020.4.6.
4. Правова база української кібербезпеки: загальний огляд і аналіз. Міжнародна фундація виборчих систем в Україні. 2019. URL: <https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf> (дата звернення: 24.11.2021).
5. Приказюк Н.В., Гуменюк А.С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. Електронне наукове фахове видання "Ефективна економіка". 2020. № 4. DOI: 10.32702/2307-2105-2020.4.6.
6. Про основні засади забезпечення кібербезпеки України: Закон України № 2469-VIII від 21.06.2018. Відомості Верховної Ради України. 2017. № 45. Ст. 403. Поточна редакція від 15.12.2021. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 06.02.2022).

7. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України із змінами № 447/2021 від 26.08.2021. URL: <https://zakon5.rada.gov.ua/laws/show/96/2016> (дата звернення: 06.02.2022).
8. Bohme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework. Conference. 2010. URL: <http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf> (date of reference: 24.11.2021).
9. Burke D. Cyber Insurance 101: What Cyber Insurance Covers. Woodruff Sawyer. 2021. URL: <https://woodrufflaw.com/cyber-liability/cyber-101-liability-insurance/> (date of reference: 24.11.2021).
10. CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk. CRO Forum. June 2016. URL: https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf
11. Cyber Insurance Top 11 Threat Trends for 2020. URL: <https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-top-11-threat-trends-for-2020/> (date of reference: 24.11.2021).
12. Cyber risk insurance. URL: <https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/> (date of reference: 24.11.2021).
13. Directive (eu) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. L 194/1. 19.7.2016. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN> (date of reference: 24.11.2021).
14. General Data Protection Regulation: Regulation (EU) 2016/679 in the current version of the OJ L 127, 23.5.2018. URL: <https://gdpr-info.eu/> (date of reference: 24.11.2021).
15. What Does a Cyber Liability Policy Cover? URL: <https://www.thebalancesmb.com/what-s-covered-under-a-cyber-liability-policy-462459> (date of reference: 24.11.2021).
16. What is a catastrophe bond (or cat bond)? URL: <https://www.artemis.bm/library/what-is-a-catastrophe-bond/> (date of reference: 24.11.2021).

References:

1. Volosovych, S. and Klapkiv, L. (2018), "Determinants of the emergence and implementation of cyber risks", *Zovnishnia torhivlia: ekonomika, finansy, pravo*, vol. 3, pp. 101—115, available at: http://nbuv.gov.ua/UJRN/uazt_2018_3_10 (Accessed 24 Nov 2021).
2. Hudz', O. (2019), "Insurance development: new instruments and methods of risk management in the digital economy", *Ekonomika. Menedzhment. Biznes*, vol. 3 (29), pp. 4—12. DOI: 10.31673/2415-8089.2019.030412.
3. Nahajchuk, N.H. Tretiak, N.M. and Tkalenko, O. (2019), "Insurance in the cyber risk management system of the enterprise in a digital economy", *Finansovij prostir*, vol. 1 (33), pp. 97—111.
4. Shypilova, Yu. (2019), "The legal framework of Ukrainian cybersecurity: an overview and analysis", available at: <https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf> (Accessed 24 Nov 2021).
5. Prykaziuk, N. and Gumenyuk, L. (2020), "Cyber-insurance as an important tool of enterprise protection in the digitization economy", *Efektivna ekonomika*, [Online], vol. 4, available at: <http://www.economy.nayka.com.ua/?op=1&z=7777> (Accessed 06 Feb 2022). DOI: 10.32702/2307-2105-2020.4.6
6. Verkhovna Rada of Ukraine (2018), The Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (Accessed 06 Jan 2022).

7. President of Ukraine (2016), Decree "On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine"", available at: <https://zakon5.rada.gov.ua/laws/show/96/2016> (Accessed 06 Jan 2022).
8. Bohme, R. and Schwartz, G. (2010), "Modeling Cyber-Insurance: Towards A Unifying Framework. Conference", available at: <http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf> (Accessed 24 Nov 2021).
9. Burke, D. (2021), "Cyber Insurance 101: What Cyber Insurance Covers. Woodruff Sawyer", available at: <https://woodrufflaw.com/cyber-liability/cyber-101-liability-insurance/> (Accessed 24 Nov 2021).
10. CRO Forum (2016), "CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk", available at: https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf (Accessed 24 Nov 2021).
11. Marciano, C. (2019), "Cyber Insurance Top 11 Threat Trends for 2020", available at: <https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-top-11-threat-trends-for-2020/> (Accessed 24 Nov 2021).
12. ABI (2021), "Cyber risk insurance", available at: <https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/> (Accessed 24 Nov 2021).
13. Official Journal of the European Union. (2016), "Directive (eu) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN> (Accessed 24 Nov 2021).
14. General Data Protection Regulation (2021), "General Data Protection Regulation: Regulation (EU) 2016/679 in the current version of the OJ L 127, 23.5.2018", available at: <https://gdpr-info.eu/> (Accessed 24 Nov 2021).
15. Bonner, M. (2021), "What Does a Cyber Liability Policy Cover?", available at: <https://www.thebalancesmb.com/what-s-covered-under-a-cyber-liability-policy-462459> (Accessed 24 Nov 2021).
16. Artemis (2021), "What is a catastrophe bond (or cat bond)?", available at: <https://www.artemis.bm/library/what-is-a-catastrophe-bond/> (Accessed 24 Nov 2021).

Стаття надійшла до редакції 08.02.2022 р.

www.economy.nayka.com.ua

Електронне фахове видання

Ефективна ЕКОНОМІКА

Виходить 12 разів на рік

**Журнал включено до переліку наукових фахових видань України з ЕКОНОМІЧНИХ НАУК (Категорія «Б»)
Спеціальності – 051, 071, 072, 073, 075, 076, 292**

e-mail: economy_2008@ukr.net

тел.: (044) 223-26-28

(044) 458-10-73