

УДК 336 (477)

Бабенко-Левада В.Г.¹, Лотарьова С.О.²

¹канд.економ.наук, доц. НУ «Запорізька політехніка»

²студ. гр. ФЕУ-110 НУ «Запорізька політехніка»

СТРАХУВАННЯ ВІД КІБЕРЗАГРОЗ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Розвиток глобалізації та інтеграції у сучасній інформаційній економіці викликає нові види ризиків, пов'язаних із кіберзагрозами та кібератаками. Ці ризики мають транснаціональний та транскордонний характер, що може поширюватися на декілька країн одночасно. У зв'язку з цим, необхідно негайно вирішувати проблему покращення кіберзахисту та розвитку інноваційних інструментів ризик-менеджменту, зокрема, застосування кіберстрахування.

В Україні ринок кіберстрахування знаходиться на початковому етапі розвитку і вимагає розробки нових підходів до подальшого зростання, з урахуванням досвіду зарубіжних країн у цьому напрямку [1].

Подія, що сталася влітку 2017 року, коли вірус Petya. А вразив економіку України, відображає важливість захисту від кібертероризму для будь-якої компанії, незалежно від її розміру, специфіки та технічної оснащеності. У зв'язку з епідемією COVID-19, яка змусила частину суб'єктів господарювання працювати в онлайн-просторі, ризики кібератак зросли ще більше. Дослідження IT-компанії Sophos, що було опубліковане в квітні 2022 року, показує, що витрати бізнесу на відновлення після атак вірусів-зидників у світі у річному обчисленні зросли майже удвічі з 761 106 тис. доларів США до 1,85 млн. доларів США [2].

Розвиток ринку кіберстархування в кожній країні залежить від соціально-економічного та технічного становища, рівня інформатизації та впровадження IT-технологій в суспільство. З розвитком штучного інтелекту, мережових структур, хмарних технологій та ринку аутсорсингу, методи хакерських атак стають більш складними і призводять до зростання кіберзлочинності. Це призводить до збільшення ймовірності кіберризиків, що потребують впровадження інноваційних підходів до продуктів страхування [1].

Хоча кіберстрахування не може замінити міцну базу безпеки, яка потребує сучасних технологій, навченого персоналу та перевірених процедур, воно може стати ефективним запобіжним заходом кібербезпеки для бізнесу будь-яких розмірів. Кіберстрахування може забезпечити стійкість бізнесу до порушень кібербезпеки та допомогти відновити бізнес після масштабних кібератак, що може забезпечити ключову роль у підтримці бізнесу. Однак, не досягнувши необхідного рівня безпеки, страхувальники можуть відмовитися укладати договір страхування, а страховики можуть суттєво підвищити вартість страхування [3].

Страхування кіберризиків може бути вкрай складним завданням, оскільки потрібно визначити збитки та довести їх причинно-наслідковий зв'язок зі страховим випадком. Крім того, оцінка суми збитків може бути непростою і потребує документального підтвердження. Наприклад, складно застрахувати масиви даних, оскільки визначення витоку даних та їх вартості може бути проблематичним для невеликих компаній та приватних осіб [1].

Факторами, що стримують розвиток страхування кіберризиків в Україні є наявність неякісної IT-інфраструктури, у багатьох компаній неліцензійне програмне забезпечення та потреба у доведенні підприємством саме факту кібератаки. Не всі із постраждалих від кібератак бажають повідомляти про витоки даних та проломи у системі безпеки. Перешкодою є й висока вартість страхових програм, оскільки страховики працюють із недостатньою страхо-

вою статистикою, а відтак важко правильно розрахувати страхові тарифи [4, с. 16].

Становлення та функціонування кіберстрахування супроводжується проблемами, що можна розділити за декількома ознаками. Інституційна проблема полягає у відсутності законодавчо-нормативної бази регулювання кіберстрахування та недостатній діяльності страхових компаній, що можуть надавати послуги зі страхування кіберризиків. Фінансова проблема включає в себе недостатній обсяг фінансових ресурсів, що вкладаються у сферу забезпечення кібербезпеки на різних рівнях, а також відсутність ефективних фінансових інструментів і важелів розвитку кіберстрахування. Інформаційна проблема виникає через помилки в розробці та підтримці інформаційних систем страховиків і страхувальників, розвиток кібершпіонажу та перенесення персоналом комерційної інформації в соціальні мережі. Організаційна проблема полягає в відсутності кваліфікованого персоналу в сфері страхування кіберризиків, недостатній довірі юридичних і фізичних осіб до діяльності страхових компаній і ринку кіберстрахування, а також тимчасовому характері страхових відносин. Маркетингова проблема включає в себе низький попит на продукти кіберстрахування через їх високу вартість, небажання клієнтів надавати необхідну інформацію для виявлення страхових випадків, відсутність досвіду страхових компаній у врегулюванні ситуацій настання страхових подій. Ще однією проблемою становлення і функціонування кіберстрахування є відсутність науково-методичного обґрунтування методик визначення показників оцінювання та розрахунку кіберризиків, стандартів оцінки збитків від настання кібератак та суми їх відшкодування страхувальниками [4, с.9-10].

Отже, кіберзагрози стають все більш поширеними і небезпечними в сучасному світі та можуть призвести до витоку конфіденційної інформації, фінансових втрат, порушення роботи комп'ютерних систем та інших негативних наслідків. Через це, страхування від кіберзагроз стає все більш актуальним. Однак, необхідно відзначити, що страхування від кіберзагроз не є панацеєю. Компанії повинні приділяти увагу захисту своєї мережі та інформації в цілому, інакше вони можуть стати жертвою кібератак. Повна безпека може бути досягнута тільки в результаті комплексного підходу, який включає в себе не лише страхування, а й профілактику та захист від кіберзагроз. Також можливо, що у майбутньому будуть розроблені нові види страхування від кіберзагроз, які будуть спеціалізовані для конкретних видів ризиків, таких як ризики, пов'язані з шифруванням даних або зловживанням доступом до мережі. Це може стати важливим кроком у захисті компаній від кіберзагроз.

Враховуючи вищесказане, можна стверджувати, що кіберстрахування є однією з найбільш перспективних галузей страхування, оскільки попит на нього зростає внаслідок збільшення кількості кіберзагроз, що призводить до

розвитку нових продуктів страхування та використання нових технологій для оцінки ризиків. Даний вид страхування має великий потенціал для подальшого розвитку та може стати ключовим напрямком для страхових компаній у майбутньому. Компанії, які будуть активно розвивати цей напрямок, матимуть перевагу на ринку та зможуть задовольняти потреби клієнтів у захисті від кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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/pdf/5_2018/5.pdf

2. Ксьонжик І В., Жовта Н. А., Павліна А.І. Страхування ризиків кібербезпеки діяльності суб'єктів господарювання в сучасному інформаційному просторі. Економіка та суспільство. 2021. № 34. – URL: <file:///C:/Users/admin/Downloads/1042%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-998-1-10-20220214.pdf>

3. Пікус Р. В., Бабенко Ю.Л. Кіберстрахування: нові можливості для страхового ринку України. Економічна наука. 2022. №2. – URL: http://www.economy.in.ua/pdf/2_2022/25.pdf

4. Кіберстрахування 2022: Розвиток кіберстрахування як сегменту глобального страхового ринку. 30 с. URL: https://kon-insurance.mnau.edu.ua/files/work_2020/6.pdf