УДК 368

М.А. Дзямка[1]
В.Й. Плиса[1]

РОЗВИТОК КІБЕРСТРАХУВАННЯ В УМОВАХ ПРИСКОРЕННЯ ПРОЦЕСІВ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУЧАСНОГО СУСПІЛЬСТВА

[1]Львівський національний університет імені Івана Франка

Анотація: Розглянуто проблеми розвитку кіберстрахування в умовах прискорення процесів цифрової трансформації сучасного суспільства.
Ключові слова: кіберстрахування, кіберризик, кібератака, кіберзахист, кіберзагроза.

Abstraction: The problems of the development of cyber insurance in the conditions of accelerating the processes of digital transformation of modern society are considered.
Keywords: cyber insurance, cyber risk, cyberattack, cyber defense, cyber threat.

Не викликає сумніву той факт, що „розвиток та здешевлення нових технологій, які лежать в основі електронного сервісу, подолання цифрової нерівності шляхом розвитку цифрових інфраструктур, стрімке збільшення числа користувачів Internety, агресивне формування кіберфізичного простору (насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного), реалізація прискоренного сценарію цифрового розвитку національних економік, активізація створення та стрімкий технологічний розвиток цифрових інфраструктур як основи використання переваг цифрового світу у повсякденному житті та платформи для досягнення ефективності економіки взагалі, масовий процес адаптації цифрових технологій у бізнес-моделі, прискорення процесів цифрової трансформації в суспільстві”[1, с. 87], сигналізують страховому бізнесу про можливості розширення практики кіберстрахування.

В останні роки кіберзагрози стають дедалі помітнішими та вважаються найбільшою глобальною загрозою для фінансового сектора та економіки в цілому. Збільшення частоти та складності кібератак, швидка цифрова трансформація та збільшення використання великих даних і хмарних обчислень зробили суб’єктів господарювання все більш уразливими до кіберзагроз.

Добре розвинений ринок кіберстрахування може зіграти ключову роль у забезпеченні переходу до цифрової економіки шляхом підвищення обізнаності про кіберризики, адже в Україні розвиток та правове регулювання такого страхування, як кіберстрахування, гальмується недостатнім розумінням величини потенційних фінансових втрат, спричинених незаконними діями кіберзлочинців, низькою довірою страхувальників до страхових компаній та відсутністю належного регулювання.

Ландшафт кіберризиків швидко розвивається, і кількість кібератак зросла. Однак більшість підприємств і домогосподарств й надалі не застраховані або рівень страхового захисту від цих ризиків є мінімальним, неадекватним загрозам. Премії кіберстрахування складають лише частку загальних збитків від кібератак, за оцінками, розрив у захисті становить 90% [5]. З огляду на це, потрібно створити ефективну систему страхування, спроможну забезпечити належний захист від ризиків (виробити стійкість до кіберризиків), і для цього мобілізувати потенціал співпраці між бізнесом, страховою індустрією та владою.

Можливою стороною співпраці можуть стати потуги усіх сторін спрямовані на покращення якості моделювання статистичних даних для більш точного ціноутворення у кіберстрахуванні. Кіберризики важко оцінити кількісно через відсутність стандартизованих даних і обмежень моделювання, а також через високий ступінь невизначеності щодо очікуваних втрат і потенціалу накопичення втрат. Майбутні ризики зазвичай визначають на основі ретроспективних даних, але цей підхід має обмежену цінність у швидко мінливому середовищі кіберризиків. Тут велика надія на перестраховиків, які використовуючи свій потенціал можуть інвестувати в „кіберробочу силу”, щоб допомогти зміцнити їхні актуарні, технічні та криміналістичні навички, необхідні для циклів

андеррайтингу та управління претензіями. Також перестраховики повинні оновити механізм формулювання політики співпраці стосовно узгодженості положень щодо зниження вразливості до сценаріїв системного ризику, який важко застрахувати.

Нарешті, є простір для нових типів державно-приватних механізмів розподілу ризиків. Одним із варіантів є схема страхування державно-приватного партнерства, де покриття системних ризиків, таких як загрози критичній інфраструктурі, розподіляються між страховиками та фондом, що підтримується державою. Інший – залучення альтернативного капіталу, наприклад, шляхом розвитку ринку цінних паперів, пов'язаного із кіберстрахуванням.

Вагомими проблемами, що стримують розвиток кіберстрахування в Україні, є: складність ідентифікації та виявлення кіберризиків; неможливість повної компенсації збитків, спричинених кіберзагрозами; неповне та несвоєчасне інформування про кібератаки через можливе погіршення іміджу організації; відсутність законодавчої бази для регулювання кіберстрахування; недостатній рівень контролю з боку страхувальників; відсутність спеціальних схем страхування [3, с. 63].

Подальший розвиток кіберстрахування має супроводжуватися використанням програмного забезпечення високого рівня безпеки, зокрема комп'ютерів і мобільних пристроїв, регулярним оновленням комп'ютерних систем, впровадженням комплексу профілактичних заходів (сканування інформації для запобігання та усунення загроз) у цій сфері [4, с. 11]. Враховуючи специфіку цього виду страхування, в українському законодавстві вкрай необхідні певні зміни щодо визначення нормативних вимог до страховиків та застрахованих осіб, суб'єкта та предмета кіберстрахування, умов відшкодування збитків, порядку проведення на від імені страхових компаній Cyber Risk Check. Таке державне втручання матиме можливість активно сприяти розвитку кіберстрахування як сектору страхового ринку.

В Україні наразі відсутня стандартизована система оцінки кіберризиків. Щоб виправити це, страхові компанії повинні використовувати розширений аналіз ризиків для належної оцінки своїх кіберризиків. Це принесе їм користь, заробивши податкові пільги та розширивши можливості покриття. Страхові компанії також повинні збільшити кількість освічених людей, які працюють на них, оскільки це допоможе їм уникнути шахрайства через людську фактор. Крім того, вони можуть розробити нові варіанти страхування та розширити обсяг доступного покриття.

Таким чином, тенденції розвитку глобального інформаційного суспільства, яке ґрунтується на використанні глобальної інформаційної інфраструктури утвореної за рахунок об'єднання національних інфокомунікаційних мереж, визначають необхідність розвитку кіберстрахування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Плиса В., Плиса М., Плиса З. Управління ризиками у сфері електронних страхових послуг. *Вісник Львівського університету. Серія економічна*. 2021. Випуск 60. С. 86-104. DOI: http://dx.doi.org/10.30970/ves.2021.60.0.6008
2. Кіберстрахування: новий інструмент ризик-менеджменту URL: http://forbes.net.ua/ua/opinions/1426423-kiber-strahuvannya-novij-instrument-rizikmenedzhmentu.
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. 60-65
4. Селіверстова Л.С., Трухан Д.А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. Економіка та держава. 2020. № 1. С. 11–19.
5. Eckert C. & Osterrieder K. (2020). How digitalization affects insurance companies: overview and use cases of digital technologies. Zeitschrift für die gesamte Versicherungswissenschaft. https://doi.org/10.1007/ s12297-020-00475-9

Дзямка Максим Антонійович здобувач освітньо-кваліфікаційного рівня „Магістр", Львівський національний університет імені Івана Франка, Львів, e-mail: Maksym.Dziamka@lnu.edu.ua.

Maksym Antoniyovych Dziamka, recipient of the Master's degree, Ivan Franko National University of Lviv, Lviv, e-mail: Maksym.Dziamka@lnu.edu.ua.

Плиса Володимир Йосипович, кандидат економічних наук, професор, професор кафедри фінансів, грошового обігу і кредиту, Львівський національний університет імені Івана Франка, Львів, e-mail: V_plysa@ukr.net

Plysa Volodymyr Yosypovych, Candidate of Economic Sciences, Professor, Professor of the Department of Finance, Money Circulation and Credit, Ivan Franko National University of Lviv, Lviv, e-mail: V_plysa@ukr.net