

Список літератури

1. Бобрович О. Б. Проблемні аспекти методики здійснення аудиту фінансової звітності страхових компаній /О. Б. Бобрович// Науковий вісник НЛТУ України. – 2013. – Вип. 23.15– С. 176–185.
2. Закон України «Про страхування» від 18.11.2021 р. № 1909-IX. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1909-20#n690>.
3. Калінська Т.А., Самчинська Я.Б. Об'єкти аудиту діяльності страхових компаній [Електронний ресурс]. – Режим доступу: http://business-navigator.ks.ua/journals/2012/28_2012/34.pdf
4. Мельничук І. І. Формування моделі внутрішнього аудиту фінансових результатів страхових компаній: синергетичний підхід до побудови [Текст] / І. І. Мельничук // Науковий вісник Ужгородського університету : Серія: Економіка / редкол.: В.П. Мікловда (гол. ред.), В.І. Ярема, Н.Н. Пойда-Носик та інші. – Ужгород: Вид-во УжНУ «Говерла», 2017. – Вип.1(49). Том 1. – С. 347–350.
5. Радіонова Н.Й. Особливості організації служби внутрішнього аудиту на підприємстві/ Н.Й. Радіонова// Economy, finance, law: current problems and development prospects: collective monograph. Anisiia Tomanek OSVČ. (Prague, Czech Republic) – 2023. – С.5 -16.
6. Розпорядження Національної комісії, що здійснює державне регулювання у сфері фінансових послуг «Про затвердження Порядку проведення внутрішнього аудиту (контролю) у фінансових установах» від 05.06.2014 р. №1772. - [Електронний ресурс]. – <https://zakon.rada.gov.ua/laws/show/z0885-14#Text>

УДК 368.3.06

В. Апацький, І. Тарасенко

vva0919@gmail.com, irataras@ukr.net

Київський національний університет технологій та дизайну, Київ

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ СТРАХУВАННЯ КІБЕРИЗИКІВ В УКРАЇНІ

Страхування кіберризиків – це страховий продукт, який призначений для захисту компанії від ризиків, пов'язаних із використанням мережі Інтернет та із ризиками, що виникають під час використання інформаційних технологій, IT-інфраструктури та діяльності підприємства в кіберпросторі. Слід відзначити, що діяльність у галузі страхування кіберризиків нерозривно пов'язана з кібербезпекою. Це передбачає знання та розуміння характеру кіберзагроз для інформаційних систем, які становлять небезпеку для бізнесу та урядових організацій, а також внутрішніх факторів, як, наприклад, особливості комп'ютерних систем та специфіка їх роботи.

Саме профілактика кіберзлочинів є предметом страхування кіберризиків, а також забезпечення мінімізації потенційних фінансових втрат від інцидентів під час функціонування інформаційних цифрових систем. Для України в кіберпросторі особливу загрозу становить і країна-агресор, тому розвиток страхування кібер-ризиків є нагальною потребою для страхового ринку України та економіки в цілому в умовах сучасних викликів. Все це зумовлює актуальність дослідження тематики страхування кіберризиків в Україні, поглиблення теоретичних засад у цьому напрямі та впровадження досвіду високорозвинених країн. Ефективно організоване управління кіберризиками та наявність деталізованого страхового захисту в разі настання кіберінцидентів є запорукою успішної діяльності з урахуванням стрімкої діджиталізації суспільно-господарської діяльності в умовах сучасних викликів, які постають в кіберпросторі.

Найбільш значний внесок у становлення та розвиток теорії страхування кіберризиків внесли такі українські вчені як: Р. Пікус, Н. Приказюк, В. Братюк, С. Волосович, Л. Клапків, О. Харченко, В. Яремич, а також іноземні: Г. Шварц, Р. Бохме, А. Цохоу, В. Діаманополоу, С. Грітзаліс та інші. Проте, ряд питань теоретичного і практичного характеру до цих пір є дискусійними та недостатньо опрацьованими.

Розвиток інформаційних технологій, зокрема мережі Інтернет, відкрив небачені раніше можливості для світового економічного зростання. Це збільшило ефективність та швидкість комунікації, прискорило бізнес-процеси, сприяло їх автоматизації, створило чимало нових сфер для ведення бізнесу, зокрема і таких, в яких діяльність повною мірою здійснюється в мережі Інтернет. Виникнення Big Data, фінтех, криптовалют, блокчейну, хмарних сховищ та обчислень, штучного інтелекту дозволило значно поглибити та прискорити розвиток світової економіки. Однак із розвитком цифрових технологій з'явилися нові виклики – кіберризиків, які часто призводять до колосальних збитків навіть для найбільших та найпотужніших транснаціональних корпорацій.

У зв'язку із цими викликами все більш актуальним стало кіберстрахування як засіб для мінімізації фінансових втрат у разі витоку корпоративних даних, втрати інтелектуальної власності, витоку даних клієнтів тощо.

Для України страхування кіберризиків набуло особливої актуальності через агресію з боку російської федерації, яка активно проводила кібер-атаки на інформаційні системи українських компаній та урядових організацій. Проте розвиток кіберстрахування все ще перебуває на етапі зародження, тому особливо важливим

стають питання вивчення поняття «кіберризик» та вдосконалення підходів до його трактування, що обумовлює актуальність даного дослідження.

Поняття «кіберризик» є досить новим у науковій літературі і навколо його визначення продовжуються дискусії. Існує чимало підходів до визначення цього терміну. Найбільш змістовним є визначення кіберризиків, які наводять у своїх працях Пікус Р. В. та Бабенко Ю. Л. [1, с. 136], що повністю розкриває сутність, зміст та вказує на результат явища. В українському законодавстві також є визначення поняття «кіберризик» або ж «кіберзагроза» [2], яке, на нашу думку, потребує уточнення з урахуванням наслідків кіберзагроз.

За результатами проведеного дослідження сформульовано таке визначення: кіберризик – це ймовірність настання несприятливих подій, які вражають функціонування інформаційних систем та позначаються на кібербезпеці економічних суб'єктів, урядових організацій і фізичних осіб, наслідком яких є отримання прямих чи непрямих збитків, руйнування цифрових активів, витоки корпоративної чи приватної інформації, втрати інтелектуальної власності, потенційно можливі втрати репутації організації.

Економічні наслідки виникнення кібер-ризиків можуть бути як прямими, так і непрямыми. Прямі – це фінансові втрати від необхідності проведення розслідування інциденту, його правового супроводу, заходів для інформування клієнтів щодо існування проблеми з інформаційною системою, заходи на посилення інформаційної безпеки. Непрямі втрати включають в себе втрату репутації, потенційного доходу, знецінення інтелектуальної власності тощо. Виміряти непрямі наслідки реалізації кібер-ризиків набагато складніше, ніж прямі. Вони є довготривалими і менш помітними, але водночас приносять значну шкоду для подальшої діяльності компанії.

Страховання кіберризиків – це наймолодший напрям у страхуванні, який виник вже у XXI столітті як одна з історичних форм розвитку страхування. Чимало вчених дотримуються позиції, що кіберстрахування – це все ж страховий продукт, а не сегмент ринку. Наприклад, українські дослідники Н. Нагайчук, Н. Третяк і О. Ткаленко [3, с. 102] стверджують, що кіберстрахування – це страховий продукт, призначений захищати компанію від ризиків, пов'язаних із використанням мережі Інтернет та таких, які виникають під час використання інформаційних технологій, IT-інфраструктури і діяльності підприємства в кіберпросторі. Німецькі вчені Г. Шварц та Р. Бем [4] кіберстрахування трактують як передачу фінансового ризику, пов'язаного з мережевими та комп'ютерними інцидентами третій стороні чи сторонам, оскільки є частою практика використання перестрахування. Тобто, на їх думку, це більше послуга, ніж сегмент ринку.

У страхуванні кіберризиків надзвичайно важливим аспектом є методологія оцінки кіберзагроз. Завдання такої оцінки полягають в тому, щоб: виявити загрози, які спрямовані на активи; визначити та спрогнозувати якомога більш точно наслідки реалізації кіберризиків; виявити вразливі місця для кібер-загроз в інформаційній безпеці організації; проаналізувати наявні методи контролю ризиків та визначити той, який дозволить мінімізувати виявлені загрози; оцінити ймовірність виникнення та реалізації кіберризиків.

Як зазначається в [1, с. 138], існує суттєва розбіжність серед страховиків щодо розуміння кіберризиків. Більшість з них розглядають загрози в кіберпросторі саме як ризики, тоді як значно менше страховиків ставляться до страхування кібер-ризиків як до окремого продукту. Кіберризики досить часто включають до класичних полісів страхування, тобто страхування майна, страхування відповідальності перед третіми особами та навіть до страхування екологічних ризиків.

Страховання кіберризиків виникло у зв'язку із нагальною потребою мінімізувати втрати від кіберзагроз відносно недавно, але попит на нього зростає з кожним роком. США були і залишаються лідером в галузі страхування кіберризиків. Навіть на страховому ринку Європи онлайн-страхування з'явилося порівняно недавно. У 2014 році обсяги фінансування страхування в кіберпросторі в Європі становили трохи більше 1 млн. доларів США [5].

В Україні страхування кіберризиків перебуває на етапі становлення. Тривалий час кіберстрахування лишалося додатковою послугою в договорах майнового страхування і не користувалося популярністю. Головним поштовхом до впровадження страхування кіберризиків в Україні стали масовані кібератаки 2017 року, коли Україна стала другою країною серед понад 90 країн, що постраждала найбільше після США. Саме хвиля кібератак у 2017 році й стала поштовхом до появи в Україні повноцінного спеціалізованого страхування кіберризиків. У 2018 році на страховому ринку України з'явилися спеціалізовані послуги зі страхування кіберризиків, а першою компанією, яка запропонувала такі послуги, стала СК AIG [6], яка, однак, згодом вийшла зі страхового ринку України. Пізніше страхові послуги зі страхування кіберризиків стали також надавати СК «АОН», СК UPSK, СК АСКА [7-9].

Другим поштовхом до необхідності впровадження кіберстрахування в Україні стала пандемія COVID-19. У 2022-2023 роках весь український страховий ринок опинився в глибокій кризі через повномасштабну війну, розпочату РФ проти України, коли паралельно ще триває перша в світовій історії кібервійна. За таких умов необхідність страхування кіберризиків зростає ще більшою мірою. Але, зважаючи на глибоку економічну кризу і те, що страхування не є послугою першої необхідності, поки що цей напрям був і залишається на етапі становлення. Однак він буде надзвичайно перспективним, коли страховий ринок України відновиться після завершення війни, оскільки з поглибленням діджиталізації та зважаючи на стратегію побудови цифрової держави, попит на кібербезпеку та все, що з нею пов'язано буде зростати.

Список літератури

1. Пікус Р. В., Ю. Л. Бабенко. Кіберстрахування: нові можливості для страхового ринку України. Економіка та держава. №2. 2022. С. 134-140. DOI: 10.32702/2306-6806.2022.2.134

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII (rada.gov.ua). URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
3. Нагайчук Н. Г., Третяк Н. М., Ткаленко О. Страхування в системі управління кіберризиками підприємства в умовах цифрової економіки. Фінансовий простір. №1 (33). 2019. URL: <http://fpnpu.cibs.ubs.edu.ua/article/view/177102>
4. Bohme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework. Conference. 2010. URL: <http://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf>
5. Institute of Risk Management. URL: <https://www.theirm.org/knowledge-andresources/thought-leadership/cyber-risk>
6. Офіційний сайт страхової компанії AIG. URL: <https://www.aig.com/home>
7. Офіційний сайт страхової компанії АСКА. URL: <https://aska.ua/ua/business-insurance/industry/cyber-insurance>
8. Офіційний сайт страхової компанії UPSK. URL: <https://cyber.upsk.com.ua/>
9. Офіційний сайт страхової компанії АОН. URL: <https://www.aon.com/ukraine/solutions/risk-insurance-solutions/cyber-risk-insurance.jsp>

УДК 336.71

Ю. Русіна

rusinaulia80@gmail.com

Київський національний університет технологій та дизайну, Київ

ОСОБЛИВОСТІ РОЗВИТКУ ТА ФУНКЦІОНУВАННЯ РИНКУ ФІНАНСОВИХ ТЕХНОЛОГІЙ В УКРАЇНІ

На сучасному етапі фінансовий сектор перебуває в центрі цифрової трансформації, трендом якої стають фінансові технології. У сфері фінансових технологій відбуваються радикальні зміни, пов'язані з підвищенням рівня автоматизації, відкритості та орієнтованості на споживача. Крім того в умовах карантину, вимушеної ізоляції та нині в умовах воєнного стану, роль використання цифрових технологій виходить на перший план в усьому світі, в тому числі й в Україні [4].

Нині фінтех-ринок слід розглядати з одного боку як екосистему, що об'єднує всіх учасників фінансового ринку, включаючи фінтех-стартапи, регулятори, банки, міжнародні платіжні системи, асоціації банкірів та фінансистів, та постачальників, а з іншого боку – як складну систему, яка об'єднує сектори нових технологій та фінансових послуг, стартапів та пов'язану з ними інфраструктуру.

Розвиток фінансових технологій в Україні особливо помітний в останні п'ять років, що обумовлено низкою факторів:

- світова економічна криза, що розпочалася у 2008 році та її наслідки;
- зростання світових процесів діджиталізації;
- активне поширення мережі Інтернет;
- розвиток конкуренції на фінансових ринках;
- стрімке поширення соціальних мереж та месенджерів;
- прагнення до інновацій, підвищення вимог до зручності користування, якості та швидкості отримання інформації;
- успіхи технологічних компаній в інших секторах економіки;
- зростання електронної комерції;
- державні карантинні обмеження 2019–2020 рр. [2, с. 190].

Фінтех-компанії не лише стають важливою складовою світової та національної економіки, вони трансформують сектор фінансових послуг за допомогою інноваційних продуктів, принципово змінюючи механізм роботи основних традиційних учасників ринку. Динамічний розвиток фінансових технологій передбачає необхідність обґрунтування ролі та місця фінтех-компаній на ринку фінансових послуг, розподілу сфер впливу та визначення взаємовідносин нових та традиційних учасників ринку [1, с. 204].

Фінтех відкриває величезні можливості для всіх суб'єктів фінансової сфери. Він забезпечує клієнтам зниження витрат, платежі в реальному часі, більш широкий вибір послуг та більшу зручність. Фінтех може сприяти розширенню доступу до фінансування для фізичних осіб, малих та середніх підприємств, недостатньо охоплених фінансовими послугами. Розкриваючи позитивний вплив фінансових технологій для всіх його суб'єктів, дослідники відзначають зростання конкуренції на ньому, консолідацію інформаційних технологій фінансовими організаціями для диверсифікації свого бізнесу, зменшення інформаційної асиметрії та підвищення ефективності ціноутворення, розширення набору фінансових послуг та кола потенційних клієнтів, забезпечення фінансової доступності в країнах з економікою, що розвивається і розвиненою економікою.

Поряд з вищезазначеними перевагами використання фінансових технологій має ряд недоліків: недостатній рівень нормативного регулювання внаслідок використання фінтех-компаніями відмінних від