УДК 368:330

А. С. Селіверстова,
д. е. н., професор, професор кафедри фінансів,
Київський національний торговельно-економічний університет, м. Київ,
ORCID ID: 0000-0002-2231-0558
Д. А. Трухан,
студент 3 курсу факультету фінансів, банківської справи та страхування,
Київський національний торговельно-економічний університет, м. Київ,
ORCID ID: 0000-0002-6632-7343

DOI: 10.32702/2306-6806.2020.1.23

ПІДХОДИ ДО РОЗВИТКУ КІБЕРСТРАХУВАННЯ ЯК СЕГМЕНТУ ГЛОБАЛЬНОГО СТРАХОВОГО РИНКУ

L. Seliverstova,
Doctor of Economic Sciences, Professor,
Professor of Department of Finance, Kyiv National University of Trade and Economics, Kyiv
D. Truhan,
student, 3 courses of the Faculty of Finance, Banking and Insurance,
Kyiv National University of Trade and Economics, Kyiv

APPROACHES TO THE DEVELOPMENT OF CYBER INSURANCE AS A SEGMENT OF THE GLOBAL INSURANCE MARKET

Глобалізація світової економіки та процеси інтеграції в умовах інформаційної її складової приводить до появи нових видів ризиків, пов'язаних з кіберзагрозами та кібератаками, негативний вплив яких має глобальний характер. У зв'язку з цим потребують розвитку підходи до кіберстрахування як сегменту глобального страхового ринку. В Україні кіберстрахування перебуває на початковому етапі становлення та потребує розробки підходів до подальшого розвитку, враховуючи накопичений позитивний досвід зарубіжних країн у цьому напрямі. З розвитком кіберзагроз та кібератак страхування стає вагомим інструментом ризик-менеджменту для підприємств як державної, так і недержавної форми власності. Це перспективний напрям розвитку страхового бізнесу, оскільки створення страхових програм захисту, крім безпосереднього відшкодування збитків, значною мірою охороняє від таких ризиків та не дозволяє припинити або знищити бізнес.

The globalization of the world economy and the processes of integration in the context of its information component lead to the emergence of new types of risks related to cyber threats and cyberattacks, which are negatively impacted by global character. In this regard, we need to develop cyber insurance approaches as a segment of the global insurance market. In Ukraine, cyber insurance is in its infancy and needs to develop approaches to further development, taking into account the accumulated positive experience of foreign countries in this area. With the development of cyber threats and cyberattacks, insurance has become a significant risk management tool for both state and non-state enterprises. This is a promising direction for the development of the insurance business, since the creation of insurance protection programs, in addition to the direct compensation of losses, largely protects against such risks and does not allow to terminate or destroy the business.

As cyber insurance in Ukraine is in its infancy, it is necessary to make extensive use of the positive experience of the world's leading countries in the development of approaches to its further development, which demonstrates the spectrum diversification of cyber insurance services and the application of certain cyber insurance policies, hacking attacks and damages in the process of their occurrence. The impetus for the development of this market

will be the adoption of relevant legislation in the field of cybersecurity at the level of the state and individual entities, a clear definition in the Law of Ukraine "On Insurance" the nature of cyber insurance, with its classification as a voluntary or mandatory type of insurance. The cybercrime range is wide enough and ranges from access to information databases, intellectual property assets, computer system interference to financial gain. The implementation of the proposed approaches in combination with ensuring transparency and widening the boundaries of cooperation of insurance companies with other economic agents will lead to diversification of insurance services and development of domestic cyber insurance, which will significantly reduce the amount of losses from the occurrence of cybercrime.

Ключові слова: кіберстрахування, страхування, ризики, кіберзагроза, кібератака, хакери, договір страхування.

Key words: cyber insurance, insurance, risks, cyber threat, cyberattack, hackers, insurance contract.

ПОСТАНОВКА ЗАВДАННЯ

З поширенням цифрових послуг відповідальність бізнесу за зберігання, обробку, використання, контроль за конфіденційністю персональних даних істотно збільшилася. Помилки в роботі з великими обсягами персональних даних обертаються величезними штрафами, витратами на відновлення, захист ділової репутації. Перехід економіки до цифрового типу включає в себе як позитивні, так і негативні моменти, які передусім пов'язані з інформаційною безпекою. І Україна не є виключенням у списку країн, яким характерні кіберінциденти, і до цього часто виявляються не готові ні влада, ні бізнес.

Поняття кіберстрахування для України є доволі новим і мало дослідженим, але сьогодні воно набуває актуальності, оскільки багато українських підприємств та організацій потребують захисту від кібератак.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблеми становлення та перспективи розвитку кіберстрахування, впровадження підходів до управління кіберризиками у страхуванні досліджені в наукових працях вітчизняних та зарубіжних дослідників, вчених та практиків, зокрема: В. Братюка, С. Ванга, В. Ільчука, Дж. Кесена, О. Кондратьєва, Й. Малкотра, А. Мамаєвої, Т. Моташко, О. Парубець, С. Перцовой, Н. Приказюка, Т. Ротової, Д. Сугоняко, К. Хейеса, Ю. Шевченко, С. Шекелфорда.

Розрізненість підходів до формування поняття кіберстрахування у вітчизняній та зарубіжній практиці, законодавча невизначеність основних понять, що входять до його складу зумовлюють необхідність проведення подальших досліджень у напрямі обґрунтування підходів до розвитку кіберстрахування як сегменту глобального страхового ринку.

ПОСТАНОВКА ЗАВДАННЯ

Сучасне глобальне взаємопов'язане бізнес-середовище посилює імовірність кіберзагроз для організацій. Для зменшення ризиків і оптимізації нових можливостей організації мають бути захищеними, пильними і гнучкими. Саме тому, завдання дослідження полягають у комплексному вивченні підходів до розвитку кіберстрахування як сегменту глобального страхового ринку.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Кіберзлочинність в останні роки стає практично буденним явищем. У новинах щоразу чути про зникнен-

ня великих сум з рахунків найбільших світових банків або про затримання чергового хакера.

Як явище значущє в світовому масштабі факт кіберзлочинності відзначають як найбільші бізнесмени і економісти світу в на форумах, наприклад, у Давосі в 2012 році, так і найбільші консалтингові компанії. Зокрема, Pricewaterhouse Coopers випустили Всесвітній огляд економічних злочинів, де відзначили вибухове зростання кібератак в останні роки.

Кіберризик — це ризик, пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення як в місцевих (локальних) мережах, так і в глобальній інтернет-мережі; в розрахунково-платіжних системах, у системах інтернет-торгівлі і в промислових системах управління. Також це ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних [1].

Кіберінциденти здатні наносити серйозний фінансовий та репутаційний збиток компаніям і економіці країн. Яскравим прикладом уразливості українського інформаційного сектору став вірус Petya, який масово атакував підприємства країни в 2017 році. Через атаку вірусу Petya влітку 2017 року вітчизняна економіка зазнала втрат на 0,4—0,5% від річного ВВП. Ця ситуація чітко показала: абсолютно будь-яка компанія вразлива до кібертероризму, незалежно від розміру, специфіки та технічного обладнання [2].

Статистика свідчить про те, що втрати світової економіки внаслідок кібератак збільшуються з кожним роком. І ці невтішні дані все частіше наводять керівництво компаній на думку про необхідність страхування кіберризиків.

Одним з можливих методів захисту від кібератак і негативних наслідків від них може виступати кіберстрахування. Цей вид страхування є сегментом глобального страхового ринку і забезпечує фінансовий механізм відновлення після великих збитків, допомагаючи підприємствам повернутися до нормального функціонування, збереження стабільності, платоспроможності і зниження втрат у результаті перерви у виробництві, викликаного різного роду кіберзагрозами.

Страхування як фінансовий інструмент набув поширення на міжнародному ринку ще у 2010 році. За оцінками Munich Re, обсяги доходів від кіберстрахування у 2020 році складуть \$8—9 млрд проти \$3,4—4 млрд у 2017 році. Щорічні втрати світової економіки від кіберзлочинності у 2017 році перевищили \$400—600 млрд і склали 0,8% світового ВВП, що на 35% більше порівняно з 2015 роком [3]. Тільки атака вірусів WannaCry і Petya в 2017 році торкнулася 150 країн і завдала збитків

більш ніж на \$ 12 млрд. Тому компанії витрачають на кіберзахист все більше коштів. У дослідженні агентства MarketsandMarkets йдеться, що за підсумками 2018 року витрати бізнесу на захист від хакерів склали майже \$ 153 млрд, а в 2023-му вони перевищать \$ 248 млрд [2].

Під час щорічного дослідження глобальних ризиків від Allianz Global Corporate & Specialty AGCS), яке проведено 2415 експертами з 86 країн (включаючи топ-менеджерів компаній, страхових експертів, брокерів і ризик-менеджерів), кіберризиків (кіберзлочинність, збої у роботі IT-систем, вразливість даних, штрафи), ставлять кіберризиків на друге місце серед глобальних ризиків підприємств та фінансового сектора на 2019 рік [4].

З цими оцінками складно не погодитися. Особливо якщо подивитися на те, з якою швидкістю цифрові технології накривають планету. За даними компанії Herjavec Group, яка спеціалізується на консалтингу в сфері кібербезпеки, зараз у світі більше 4 млрд користувачів інтернету, в 2022 році їх число зросте до 6 млрд, а у 2030 — до 7,5 млрд. А за прогнозами Ericsson, до 2023 року кількість підключених до глобальної мережі пристроїв досягне 30 млрд.

Водночас від зазіхань хакерів страждають навіть більшою мірою не рядові користувачі, а великий бізнес, який втрачає колосальні гроші. Найбільш привабливими для кіберзлочинців є фінансово-кредитні установи, особливо банки, які широко використовують сучасні IT і реєстроутримувачі цінних паперів. У зоні ризику також будь-яка компанія, що зберігає інформацію щодо клієнтів в електронному вигляді: аудитори, рітейлери, брокерські, туристичні, транспортні, страхові компанії, заклади сфери розваг.

Кіберстрахування — явище нове не тільки для України, а й для всього світу. За даними Munich Re, подібний захист пропонують в цілому 60 страхових компаній в різних країнах. Водночас страхуванням покрито лише 5% кіберризиків [3].

Проте швидке зростання загроз з боку хакерів стимулює розвиток цього напрямку, і за оцінками страхової групи Allianz, ринок кіберстрахування зростає на 25—50% щороку.

Лідером кіберстрахування по праву можна вважати США з їх потужною IT-інфраструктурою, де були відзначені перші в світі серйозні кіберзагрози для бізнесу та де діє жорстка законодавча база по захисту персональних електронних даних.

Кіберстрахування є динамічним сегментом глобального ринку страхових послуг. Безсумнівно, цей вид страхування розглядається як метод управління ризиками та захисту від різних загроз, що виникають при здійсненні електронної комерції.

До основних ризиків можна віднести:

- крадіжку засекреченої і конфіденційної інформації персоналом організації;
- крадіжку номерів кредитних карт;
- розкрадання фінансових коштів з депозитів;
- втрату носіїв інформації;
- фішинг;
- кібервимагання;
- порушення роботи комп'ютерної мережі внаслідок хакерських атак.

Але головним завданням кіберстрахування залишається захист від великомасштабних хакерських атак.

Свою популярність в розвинених країнах кіберстрахування отримало завдяки розумінню, що при впровадженні новітніх рішень у сфері кібербезпеки та проведенні постійної роботи з персоналом завжди залишається 1% ризику компрометації системи, який неможливо передбачити і реально оцінити.

Перші договори страхування кіберризиків були укладені ще в 2010—2011 роках. Як зазначалося, цю тему активно обговорювали на щорічному форумі в Давосі в 2012 році. Але активне зростання даного виду страхування почалося кілька років по тому, після масових

зломів корпоративних і урядових ресурсів в США. Тому 90% ринку страхування кіберризиків припадає саме на Сполучені Штати Америки.

Укладення договору страхування кіберризиків пов'язане з комплексною оцінкою клієнта та його систем. Оцінюється економічний стан компанії, канали продажів, безпека комп'ютерних мереж, ступінь захисту персональних даних клієнтів. Чим більше у страховальника доступу до конфіденційної інформації користувачів, тим дорожче буде ціна страхової програми. Також впливає фізична охорона серверних даних, доступ до них, наявність ключів доступу, регулярність резервного копіювання даних.

Про формування повноцінного сектору кіберстрахування в Україні говорити поки зарано: інтерес до послуги почав формуватися у 2017 році, коли компанії розраховували збитки та втратили прибуток через до нападу вірусу Petya.

Крім того, основна інфраструктура, необхідна для розвитку цього виду страхування, лише формується. Так, Закон "Про основні засади забезпечення кібербезпеки України" набув чинності у травні 2018 року [5], а Державний центр реагування на кіберзагрози був створений лише у лютому 2018 року.

Кіберризик — дуже нагальна проблема, але щоб вирішити її за допомогою страхових інструментів, необхідно створити умови. Це вимагає законодавчої бази, технічних можливостей та готовності клієнтів співпрацювати зі страховиком для створення системи корпоративної кібербезпеки [6].

Експерти відзначають, що в українських реаліях далеко не завжди можливо навіть провести перевірку перед аудитом інформаційної системи клієнта, і для цього є багато причин. Як результат, не всі страховики готові надавати повноцінні програми страхування кіберризиків в Україні. Страховими компаніями, які працюють над розробкою і впровадженням таких програм страхування в Україні є "PZU Україна", "ВУСО", "АСКА", "Global Garant", "Українська страхова група", "ІНГО Україна",

Факторами, що стримують розвиток страхування кібер-ризиків 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 страховою статистикою, а відтак важко правильно розрахувати страхові тарифи [7, с. 177].

Збитки від кіберризиків можна розділити на три групи:

1. Безпосередньо збитки самого страховика. Відновлення втрачених (недопущених вигідних) від перевірочної діяльності та затримки на відновлення пошкодженої інфраструктури (наприклад, при прибутковому новому комп'ютерному обладнанні) та про введення в дію програм у системах кібербезпечного страхування, які стають причиною виникнення інцидентів.

2. Збитки перед третіми особами. У цьому випадку покривається відповідальність в рамках матеріальної шкоди, морального збитку, порушення прав інтелектуальної власності та ін. Страхування відповідальності перед третіми особами у сфері IT особливо актуальне для IT-провайдерів, хостінг-центрів, розробників програмного забезпечення.

3. Витрати на кризовий менеджмент. Страхова компанія закладає витрати на залучення експертів до IT-безпеки, консультантів, юристів для усунення та мінімізації втрат у кібернетичній атаці.

Найчастіше договори страхування кіберризиків покривають перші дві групи збитків. Тобто втрати страхувальника та шкоду, завдану третім особам.

У додатковому покритті деяких страхових програм страхових компаній є послуга, яка покриває витрати на

кризовий менеджмент і на відновлення репутації компанії після кібератаки

Основна складність при страхуванні кіберризиків — це фіксація збитків і доказ причинно-наслідкового зв'язку між страховим випадком і заявленим збитком. Крім того, суму збитків потрібно якось підрахувати і документально підтвердити. Так, наприклад, найскладніше застрахувати масиви даних, які важко оцінити. Зовсім не просто встановити скільки коштує витік даних невеликої фірми або конкретного приватної особи та яким чином оцінювати такий збиток.

Якщо збитки понесла безпосередньо компанія-страхувальник, проводиться експертиза, завдання якої — довести або спростувати вторгнення третіх осіб в комп'ютерну систему, чиї дії спровокували псування майна і простої у виробництві.

У разі страхування відповідальності перед третіми особами факт настання страхового випадку підтверджується рішенням суду, при цьому страховик не несе відповідальність за грубі порушення співробітниками компанії-страхувальника вимог з кібербезпеки; за шахрайські дії страхувальника і дії його співробітників, які викликані їх недостатньою кваліфікацією.

Таким чином, договір страхування кіберризиків допомагає захиститися від загроз, у результаті яких може статися витік даних, вихід з ладу різного обладнання і збитки, які через ці події несе страхувальник. Найчастіше попит компаній на таке покриття задовольняється через покупку додаткових розширень у договорах майна, відповідальності. Але покриття за кіберрисками в таких договорах, з огляду на специфіку даних видів страхування, досить обмежена.

Тому договір кіберстрахування — це, як правило, комплексний продукт, який включає в себе страхування майна, відповідальності та фінансових ризиків. Основний страховий випадок — збитки, які виникли в результаті порушення роботи комп'ютерної мережі (або її систем безпеки) страхувальника через вторгнення третіх осіб.

Прикладами наслідків такого вторгнення можуть бути: надання несанкціонованого доступу до комп'ютерних систем компанії; зміна, видалення або передача електронних даних, програмного забезпечення; використання ресурсів комп'ютерної системи і т. д. Також несанкціоноване вторгнення зазвичай має на увазі використання будь-яких засобів деактивації і обхід систем захисту комп'ютерної мережі (включаючи віруси і шкідливі програми, фішинг) і DoS/DDoS-атаки.

Розвиток кіберстрахування потребує об'єднання зусиль страхових компаній, Департаменту кіберполіції, Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації задля протидії кіберзагрозам. У Законі "Про основні засади забезпечення кібербезпеки України" зазначено, що "державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом: періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки [7, с.178].

Отже, з розвитком кіберзагроз та кібератак страхування стає вагомим інструментом ризик-менеджменту для підприємств як державної, так і недержавної форми власності. Це перспективний напрямок розвитку страхового бізнесу, оскільки створення страхових програм захисту крім безпосереднього відшкодування збитків, значною мірою охороняє від таких ризиків та не дозволяє припинити або знищити бізнес.

ВИСНОВКИ З ПРОВЕДЕНОГО ДОСЛІДЖЕННЯ

Таким чином, потенційний ринок для кіберстрахування величезний, оскільки будь-яка компанія, яка займається зберіганням даних, операціями з ними і передачею даних, виявляється в зоні ризику. Уразливі перед хакерами не тільки Big Data, а й особисті сторінки в со-

ціальних мережах, електронні поштові скриньки, веб-сайти спільнот або блогерів, онлайн-ігрові компанії. Розвиток ринку кіберстрахування в Україні нині знаходиться на початковому етапі, але з часом він може стати якісним засобом забезпечення інформаційної безпеки і захисту від кіберзагроз.

Література:

1. Кібер-ризик. Вікіпедія. URL: [uk.wikipedia.org > wiki > Кібер-ризик](http://uk.wikipedia.org/wiki/Кібер-ризик)
2. Підсумки 2018. URL: <https://cyberpolice.gov.ua/results/2018/>
3. Пігулка від хакерів: як бізнес захищає себе від кібератак. URL: <https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak>
4. Барометр ризиків. Allianz назвав глобальні ризики підприємств і фінансового сектора на 2019 год. URL: <https://forinsurer.com/news/19/01/16/36513?hl=%EA%E8%E1%E5%F0%F0%E8%F1%EA%E8>
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
6. 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/?op=1&z=6295>
7. Ротова Т.А., Шевченко Ю. Страхування як фінансовий інструмент захисту від кібер-ризиків. Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукр. наук.-практ. конф. Київ: КНТЕУ, 2019. 244 с. С. 177—178.
8. Seliverstova L.S. Trends in the development of the ukrainian insurance market / L.S. Seliverstova // Товари і ринки. — 2018. — № 1. — С. 135—144.

References:

1. wikipedia (2019), "Cyber risk", available at: <https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80-%D1%80%D0%B8%D0%B7%D0%B8%D0%BA> (Accessed 15 Dec 2019).
2. Department of Cyber Police of the National Police of Ukraine (2019), "Results 2018", available at: <https://cyberpolice.gov.ua/results/2018/> (Accessed 15 Dec 2019).
3. Kharlamov, P. (2019), "The hacker hack: how business protects itself against cyberattacks", available at: <https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak> (Accessed 15 Dec 2019).
4. forinsurer.com (2019), "Barometer of risks. Allianz named global risks for enterprises and the financial sector for 2019", available at: <https://forinsurer.com/news/19/01/16/36513?hl=%EA%E8%E1%E5%F0%F0%E8%F1%EA%E8> (Accessed 15 Dec 2019).
5. Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/2163-19> (Accessed 15 Dec 2019).
6. Il'chuk, V.P. Parubets', O.M. and Suhoniako, D.O. (2018), "Innovative approaches to the development of cyber-insurance market in Ukraine", *Efektivna ekonomika*, vol. 5, available at: <http://www.economy.nayka.com.ua/?op=1&z=6295> (Accessed 15 Dec 2019).
7. Rotova, T.A. and Shevchenko, Yu. (2019), "Insurance as a financial cyber risk protection tool", *Bezpeka sotsial'no-ekonomichnykh protsesiv v kiberprostorі: materialy Vseukr. nauk.-prakt. konf. [Security of Socio-Economic Processes in Cyberspace: Proceedings of the All-Ukrainian Scientific and Practical Conference]*, KNTEU, Kyiv, Ukraine, pp. 177—178.
8. Seliverstova L.S. (2018), "Trends in the development of the ukrainian insurance market", *Tovary i rynky*, vol. 1, pp. 135—144.

Стаття надійшла до редакції 23.12.2019 р.