Сейсебаєва Н. Г.
кандидат економічних наук, доцент,
доцент кафедри фінанси, банківська справа і страхування
Запорізького національного університету
Курдупа В. С.
студентка
Запорізького національного університету

DOI: https://doi.org/10.36059/978-966-397-254-1-6

КІБЕРСТРАХУВАННЯ ЯК НОВИЙ СЕГМЕНТ СТРАХОВОГО РИНКУ

Кіберзлочинність стає все більш масовою, масштабною та витонченою, стає ясно, що одних лише технологічних засобів захисту вже недостатньо для охорони бізнесу від кібератак. Вона перетворилася з вертикально інтегрованої, індивідуалістичної діяльності на надзвичайно складну та добре організовану, розподілену операцію, де вкрадені дані продаються та зіставляються на біржах, а у справу вступають високоспеціалізовані професіонали. Кіберзлочинність порушує недоторканність життя людей і бізнесу та безпеку їх даних, особливо хакерство, шкідливе програмне забезпечення, крадіжка особистих даних, фінансове шахрайство, медичне шахрайство, а також деякі злочини проти особи, пов'язані з розкриттям особистої інформації.

Центр стратегічних та міжнародних досліджень (CSIS) зробив висновок про те, що в результаті кіберзлочинів у 2019 році було витрачено близько 1 трильйона доларів, або майже один відсоток світового ВВП, що вище, ніж у дослідженні 2017 року, згідно з яким глобальні втрати становлять близько 600 мільярдів доларів. У звіті, зростання за три роки пояснюється тим, що кіберзлочинці швидко освоюють нові технології, а простота скоєння кіберзлочинів зростає у міру того, як учасники використовують чорні ринки та цифрові валюти. Очікується, що до кінця 2021 року кіберзлочинність коштуватиме світу 6 трильйонів доларів. До 2025 року ця цифра зросте до 10,5 трлн [4].

Епідемія коронавірусу викликала підвищення небезпеки кібератак і зробила компанії вразливішими. У зв'язку зі спалахом пандемії країни по всьому світу вжили запобіжних заходів. Школи закриваються, мешканців просять залишатися вдома, а багато організацій знаходять спосіб дати можливість своїм співробітникам працювати з дому. Це призвело до зростання запровадження платформ відеозв'язку. За останні чотири

місяці різко зросла кількість реєстрацій нових доменів на цих платформах відеозв'язку, включаючи Zoom. Водночас віддалені співробітники можуть розширити поверхню атаки організації, використовуючи менш захищені домашні мережі та особисті пристрої.

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 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 [3].

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.

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.

Глобальний ринок кіберстрахування оцінювався в 7291 млн доларів США в 2020 році і, за прогнозами, зростатиме з темпом зростання 21,4% протягом прогнозного періоду 2021–2031 років. Ринок кіберстрахування зростає в міру того, як все більше підприємств усвідомлюють необхідність захисту від фінансових та репутаційних втрат, пов'язаних із порушеннями безпеки та кібератаками.

Кіберстрахування допомагає захистити бізнес від потенційних наслідків кібератак. Воно допомагає організації знизити ризики, компенсуючи витрати після того, як сталася кібератака/злом. Простіше кажучи, кіберстрахування призначене для покриття зборів, юридичних витрат, пов'язаних з кіберзагрозами, що відбуваються після злому організації або в результаті крадіжки та втрати інформації клієнтів/співробітників.

За даними Центру стратегічних та міжнародних досліджень (CSIS), кіберзлочини, що включають пошкодження і знищення даних, крадіжку грошей, втрату майна, крадіжку інтелектуальної власності та інші сфери,

в даний час обходяться світу майже 600 мільярдів доларів США щорічно, або 0,8% світового ВВП [4].

Спочатку попит на ринку кіберстрахування спостерігався у сфері ЗМІ, телекомунікацій, технологій та професійних послуг. Проте зараз зростання спостерігається у всіх основних галузях. У 2018 році основними покупцями кіберстрахування були організації охорони здоров'я, освіти та грального бізнесу. Телекомунікаційний сектор, значною мірою схильний до кібератак, вважається основним кінцевим користувачем ринку кібербезпеки. Приблизно 43% телекомунікаційних організацій постраждали від шкідливих програм на основі DNS у 2019 році. Поряд із телекомунікаційним сектором, аерокосмічна промисловість вважається ще одним ключовим кінцевим користувачем ринку кіберстрахування.

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, які підлягають кіберстрахуванню 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.

При укладенні договору страхування кіберризиків проводиться комплексна оцінка клієнта та його систем. Оцінюється економічний стан компанії, канали продажів, рівень безпеки комп'ютерних мереж, ступінь захисту персональних даних клієнтів. Чим більше у страхувальника 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 [1].

Про формування і подальший розвиток повноцінного сектору кіберстрахування в Україні говорити поки зарано: сплеск інтересу до послуги був зареєстрований в 2017 році, коли компанії зіткнулися зі збитками через напад вірусу Petya. На сьогоднішній день добровільних свідомих запитів небагато. 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 [2], а Державний центр реагування на кіберзагрози був створений лише у лютому 2018 року.

Серед страхових компаній, які працюють над розробкою і впровадженням програм кіберстрахування в Україні, можна відзначити «PZU Україна», «ВУСО», «АСКА», «Global Garant», «Українська страхова група», «ІНГО Україна».

Головним фактором, який стоїть на перешкоді розвитку кіберстрахування, як нового сегменту страхового ринку в Україні це недосконала ІТ-інфраструктура компаній, а саме неякісне технічне обладнання, відсутність ліцензійного програмного забезпечення, а також відсутність програмних засобів захисту інформації. Багато постраждалих від кібератак не бажають повідомляти про витік інформації і персональних даних. Перешкодою становиться висока вартість страхової програми, так як страховики працюють з неповною страховою статистикою, з відсутністю єдиного стандарту надання страхових послуг в сфері кіберстрахування та нестачею кваліфікованих кадрів, все це ускладнює розрахунок страхового тарифу.

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 [3].

Таким чином, кіберстрахування це перспективний напрямок страхового бізнесу, оскільки може відіграти важливу роль у відновленні компанії після витоку даних, так як витрати можуть включати зрив бізнесу, втрату доходів, пошкодження обладнання, судові витрати, витрати на зв'язки з громадськістю, судову експертизу та витрати, пов'язані з повідомленнями, передбаченими законом. Потенційний ринок для кіберстрахування величезний, оскільки майже всі компанії займаються зберіганням своїх даних та персональних даних клієнтів, операціями з ними та їх передачею, тому знаходяться в зоні ризику. 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. 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. С. 177–178.

2. Марценюк О. В. Умови залучення іноземних інвесторів до розвитку страхової індустрії в Україні. *Причорноморські економічні студії*. 2019. Випуск 39. Ч 2. С. 73–78.

4. Пігулка від хакерів: як бізнес захищає себе від кібератак. URL: https://mind.ua/publications/20192978=pigulkavidhakerivyakbizneszahishchaesebevidkiberatak. (дата звернення: 07.11.2021).

5. The Center for Strategic and International Studies (CSIS) / Economic Impact of Cybercrime. URL: https://www.csis.org (дата звернення: 06.11.2021).