Дем'янчук М.А.
кандидат економічних наук,
доцент кафедри фінансів, банківської справи та страхування
Одеського національного університету
імені І.І. Мечникова

Станкова В.В.
студентка спеціальності
«Фінанси, банківська справи та страхування»
Одеського національного університету
імені І.І. Мечникова
м. Одеса, Україна

ОРГАНІЗАЦІЙНА МОДЕЛЬ ПРОЦЕСУ КІБЕРСТРАХУВАННЯ

Діяльність кожного суб'єкта ринкових відносин пов'язана з ризиком, який необхідно попереджувати та зменшувати, на що спрямовано страхування. Страхування є основною складовою ринку небанківських фінансових послуг і від його ефективного функціонування залежить стабілізація підприємницької діяльності та економіки України, особлива роль якого проявляється у сучасних умовах глобального економічного розвитку, інформатизації суспільства, необхідності стимулювання розвитку економіки тощо. Однак у цих умовах постійно зростає і економічна злочинність у глобальному просторі, що

проявляється у вигляді хакерських атак (кібератак) та позначається у втраті корпоративних даних, інтелектуальної власності або даних клієнтів чи втрата всього переліченого. Наслідки даних загроз варіюються від штрафів регулюючих органів та репутаційних втрат до повної втрати бізнесу.

Проблеми становлення та перспективи розвитку ринку кіберстрахування, впровадження інновацій у сфері страхування досліджені в наукових працях вітчизняних та зарубіжних вчених: В. П. Братюк [1], С. Ванг [2], Дж. Кесен та К. Хейєс [3], Й. Малкотр [4], С. Шекелфорд [5]. Проте приймаючи до уваги існуючи теоретичні підходи до формування ринку кіберстрахування та законодавчо невизначену сутність основних понять його структури зумовлюють необхідність проведення досліджень з визначення та обґрунтування процесу кіберстрахування в Україні, що і є метою роботи.

Кіберстрахування є однією з найбільш динамічно областей, що розвиваються на ринку страхування. Збитки від кіберзлочинів зростають з кожним роком. За прогнозами експертів збитки від кіберзлочинів в 2019 році перевищать 2 трлн. долл., а витрати на кіберстрахування – 7,5 млрд. долл. Тому ринок кіберстрахування набуде великого масштабу до 2020 року, у чому переконані експерти в сфері IT та кібербезпеки. Якщо в 2015 році ринок кіберзахисту складає 75 млрд. долл., а до 2020 повинен зрости до 175 млрд. долл.

Основними трендами в області кібербезпеки 2018 року, представлених в рамках Cyber Security Forum [6], є:

1) поява нових вірусів і розширення арсеналу кіберзлочинців за рахунок використання нових технологій. Кіберзлочинці частіше атакують розробників легітимного ПЗ, а не кінцеву мету. У зоні ризику великі компанії з надійним і багатошаровим кіберзахистом, основними з яких є промислові системи. Ще одна приваблива для хакерів ціль – персональні дані;

2) інфраструктурні кіберзагрози – атаки на програмні інтерфейси, масові зломи роутерів і модемів, злом банкоматів і POS-терміналів, створення централізованої системи управління мережами зв’язку, а також атаки на хмарні сервіси;

3) атаки на криптовалюти. Для цих цілей кіберзлочинці активно використовують ботнет-мережі для майнінг, а також провадять атаки на біржі і користувачів;

4) зміни в законодавстві. Пріоритетним завданням діяльності компаній з огляду на нововведення у законодавстві стає збільшення витрат на забезпечення кібербезпеки;

5) соціальний аспект. Позначається розвиток ідеї страхування від кіберзагроз. Компанії починають розглядати кіберзагрози як один з ключових комерційних ризиків. Фінансові організації та технологічні компанії повинні бути першими, хто буде впроваджувати страхування кіберризиків. Спостерігається зростання маніпулювання і зломів ЗМІ і соціальних медіа заради отримання прибутку з роздрібних коливань, спровокованих інформаційними фальшивками. При цьому користувачі інтернету залишаються «слабкою ланкою» і одним з основних інструментів кіберзлочинців. Більшість вірусів потрапляють в корпоративні мережі через електронну пошту і відкриття співробітниками файлів і посилань.

Отже, враховуючи проведені дослідження авторами визначено організаційну модель процесу кіберстрахування (табл. 1).

Таблиця 1

Організаційна модель процесу кіберстрахування

Етапи	Характеристика
1	2
1. Визначення суб'єктів страхових відносин кіберстрахування	страховик – організація, яка відповідно до отриманої ліцензії бере на себе за певну плату зобов'язання у разі настання страхового випадку відшкодувати страхувальникові чи третім особам завданий збиток або виплатити страхову суму страхувальник – суб'єкти господарювання різних сфер економічної діяльності – від приватних до державних – що працюють з великими базами даних конференційної інформації: банківські установи, страхові компанії, інвестиційні компанії чи фонди, медичні заклади, державні установи, промислові підприємства, стратегічні підприємства держави тощо набувач – страхувальники-суб'єкти господарювання; треті особи, що постраждали
2. Встановлення мети та предмету кіберстрахування	мета – захист страхувальників від наслідків кіберзлочинів з метою відновлення їх фінансового стану після збитків, сприяючи поверненню до нормального функціонування, збереження стабільності, платоспроможності та зниження втрат у результаті перерви у виробництві предмет – ризик втрати (знищення), нестачі або пошкодження певного стану суб'єкта господарювання, ризик збитків у підприємницькій діяльності
3. Ризикові обставини кіберстрахування	визначення проблемних місць в області інформаційної підтримки та забезпечення за допомогою об'єктивного IT-аудиту на основі тестування на проникнення (тести на подолання захисту, penetration testing, pentest, пентест) шляхом санкціонованої спроби обійти існуючий комплекс засобів захисту інформаційної системи.
4. Страхова подія	страхова вартість – дійсна вартість відповідальності перед третіми особами та активів, що страхуються, на розмір якої безпосередньо впливає ступінь захищеності даних, умови страхування страхова сума – максимальне покриття на суму до 50 мільйонів євро страховий платіж – розраховується індивідуально, відповідно до технічного завдання, для кожної інформаційної системи та залежить як від її складності, так і від особливостей її взаємодії з загальнодоступними мережами
5. Страховий випадок	витік даних, фішинг, кардинґ, sms шахрайство, фінансове шахрайство, розкрадання баз даних, промислове шпигунство, DDoS атаки, кібервимагання, навмисна шкода та розкрадання інформації, знищення інформації, сприяння цільової атаці
6. Збиток	прямий – збиток у зв'язку з порушенням даних, адміністративним розслідуванням, витратами на реагування при порушенні даних побічний – збиток у зв'язку з утриманням інформації, віртуальне вимагання, від збоїв у роботі мережі, втрата прибутку
7. Страхова виплата	франшиза – встановлюється відповідно до стану ризикових обставин страхове забезпечення (види) [7]: 1 – збитки пов'язані з порушенням даних – відповідальність за порушення персональних даних, корпоративної інформації (комерційні таємниці, професійна інформація, бюджети, переліки клієнтів та ін.),

Закінчення таблиці 1

	безпеки комп'ютерної системи (зараження вірусами, знищення, модифікація або видалення інформації, фізична крадіжка або втрата апаратного забезпечення і ін.); 2 – адміністративне розслідування відносно даних – адміністративне розслідування відносно даних – збитки страхувальника у зв'язку з розслідуванням в результаті порушення законодавства чи інших нормативно-правових актів у зв'язку з обробкою даних або корпоративної інформації, за які страхувальник несе цивільну відповідальність, у розмірі, що не перевищує витрати на захист; 3 – витрати на реагування при порушенні даних – витрати на реагування та попереджувальну програмно-технічну експертизу, відновлення репутації страхувальника і фізичних осіб, повідомлення суб'єктів даних, моніторинг, на відновлення електронних даних і програм; 4 – відповідальність за зміст інформації – збитки страхувальника в результаті публічного розкриття, викликаного помилкою, хибною заявою, що вводить в оману заявою або недоглядом в зв'язку із здійсненням ними діяльності в області мультимедіа, які призводять до порушення авторського права, права власності, слогана, товарного знаку, торгового найменування, порушення доменного імені, плагіату, порушення видавничого права або незаконного привласнення або крадіжці ідей; будь-якого невірного висвітлення, публічного розкриття фактів приватного життя, здійсненим без наміру, внаслідок записаного, вимовленого або трансльованого висловлювання, включаючи, але не обмежуючись, емоційне потрясіння або психічну біль в зв'язку з такими діями; або вторгнення, посяганню на приватне життя, протизаконному вторгнення або позбавлення власності, вчинення правопорушення або несанкціонованого вилучення інформації; 5 – збитки від віртуального вимагання – грошові кошти, виплачені страхувальником з письмової згоди страховика для обмеження або припинення загрози безпеки, яка інакше може викликати збиток страхувальникові; і вартість проведення розслідування для визначення причини загрози безпеці. При цьому збитки від віртуального вимагання не включають будь-які виплати особам, відповідальним за загрозу безпеці. 6 – перерва в роботі мережі – збитки від збоїв в роботі мережі в розмірі неотриманого прибутку (доходи, які повинні були бути отримані, зменшені на величину витрат, які повинні були бути проведені).

Джерело: розроблено авторами

Для захисту персональних даних від розкрадання, дій хакерів, помилок персоналу та багато чого іншого рішення страховій організації необхідно надати клієнтам доступ до послуг компаній, що спеціалізуються на кібербезпеки і розслідуваннях кіберзлочинів, юридичної консультації та антикризового PR. Це інструмент для запобігання збиткам і подолання наслідків витоку даних. Він надає професійну, цілодобову, фінансову допомогу для співробітників, клієнтів і членів їх сімей, які постраждали від розкрадання персональних даних.

Тому, на основі проведених досліджень авторами запропонована організаційна модель процесу кіберстрахування, яке дозволяє звести до мінімуму наслідки кризи, викликаної витоком даних. З метою надання більш повного пакету послуг вітчизняним страховим компаніям необхідно надати клієнтам доступ до послуг компаній, що спеціалізуються на кібербезпеки і розслідуваннях кіберзлочинів, юридичної консультації та антикризового PR. Також страховим компаніям доцільно створити експертні штаби з фахівців з багаторічним досвідом в області кібербезпеки і інформаційних технологій, повинна бути вибудувана партнерська екосистема з лідерами галузі, що дозволить ідентифікувати потенційні кіберзагрози для клієнта, об'єктивно оцінювати ризики і пропонувати зрозумілі для ринку рішення.

СПИСОК ЛІТЕРАТУРИ:

1. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. Актуальні проблеми економіки. Київ, 2015. № 9. С. 421-427.
2. Wang S. S. Integrated Framework for Information Security Investment and Cyber Insurance. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_ id=2918674 [in English].
3. Kesan J. P. & Hayes, C. (2017). Strengthening cybersecurity with cyber insurance markets and better risk assessment. Minnesota law review. 102(1), 191-276. Retrieved from: https://www.researchgate.net/publication/322295117_Strengthening_cybersecurity_with_cyberinsurance_markets_and_better_risk_assessment [in English].
4. Malhotra Y. (2015). Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-atRisk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era. New York: Suny Polytechnic Institute. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553547 [in English].
5. Shackelford S. J. (2012). Should Your Firm Invest in Cyber Risk Insurance? Business Horizons. Retrieved from: https://papers.ssrn.com /sol3/papers.cfm?abstract_id=1972307 [in English].
6. Cyber Security Forum. URL: https://runet-id.com/event/csf18/ (дата звернення: 24.10.2018).
7. Страховка от кибер-рисков. URL: https://habr.com/company/ruvds/blog/326530/ (дата звернення: 24.10.2018).