Klapkiv Lyubov
Dr.
Maria Curie Skłodowska
University w Lubline (Poland);

КІБЕР-РИЗИК В АСПЕКТІ МОЖЛИВОСТЕЙ РИНКУ СТРАХОВИХ ПОСЛУГ

Інформаційні технології та комунікаційні можливості покращили ефективність та функціональність сучасної інфраструктури. Однак вони також призводять до підвищеного ризику, пов'язаного з кібер-системами, які зараз є вкрай важливими для безпечної та безперервної роботи. Кіберстрахування в даний час доступне, але обмежене передусім із позиції менеджменту ризиків.

Втрати кібер можуть бути пов'язані з відповідальністю за втрату, передачу даних клієнта, пошкодження майна та крадіжки (наприклад, аварії, спричинені втручанням в автоматизовані системи) [1], пошкодження даних (наприклад, злом систем управління), втрата доходу внаслідок відключень та відмов, псування веб-сайтів та вимагання в Інтернеті [2]. Кібератаки можуть бути ініційовані хакерами, злочинними організаціями та іншими компаніями чи організаціями, терористами, зловмисними інсайдерами та підрядниками, що обумовлено браком соціальної відповідальності в суспільстві [3].

Існує чотири основних шари кіберсистем, кожен з яких знаходиться в ризик кібератаки. Перший – це перцептивний шар, який пов'язує кібер-світ та фізичний за допомогою таких компонентів, як бездротові датчики та GPS. Другий – це мережеві системи, які передають інформацію (наприклад, супутникові мережі та Інтернет-мережа мобільного зв'язку).

Третій – це системи підтримки, такі як хмарні рішення та інтелектуальні обчислення, а четвертий – прикладний рівень, який пов'язує користувачів та фізичний світ з кібер-системами (інтелектуальне транспортування та моніторинг навколишнього середовища [4]).

Можна виокремити ряд стратегій щодо пом'якшення цих збитків, які можуть включати методи проектування, що вдосконалюють архітектуру та діяльність системи, або операційні методи, що включають зміни в ділових операціях. Окремі підходи до управління кіберризиком включають контрзаходи, такі як програмне забезпечення, вдосконалення системи безпеки та інвестиції в кіберробочу силу. Заходи захисту, такі як брандмауери, шифрування програмного забезпечення, виявлення вірусів та систематизація систем, також використовуються для зменшення кібер-ризику. Переваги цих захисних заходів у безпеці повинні бути збалансовані з пов'язаними витратами та втратами продуктивності [5].

Сучасні можливості репрезентовані ринком страхових послуг щодо кібер-ризиків, як правило, включають страхування відповідальності, покривають можливі штрафи, та в першу чергу призначені для покриття збитків, пов'язаних із порушенням захисту даних. Нові або майбутні продукти повинні мати цілісне страхове покриття операцій, збоїв у системі, перебоїв у діяльності чи зривів ланцюгів постачання [6].

На додаток до передачі ризику бажаючим партнерам, переваги кіберстрахування включають стимулювання інвестицій в IT-безпеку та підвищення загальної IT-безпеки, оскільки зі збільшенням кіберстрахування найкращі практики та стандарти поширюються по економіці [7].

Однак ринок кіберстрахування є відносно новим. Визначення розміру страхових премії – ключове питання для розвитку та є особливо складним через відсутність актуарних даних за минулі події та відсутність нормативних стандартів [8]. Деякі кіберризики не можуть бути кількісно вимірюваними, а отже, застраховані. Можливість моделювання кіберризику в даний час обмежена, але покращиться істотно, оскільки накопичується та обмінюється більшою кількістю даних. Крім того, у кіберстрахувальних продуктів відсутні чіткі тригери збитків та об'єктивне визначення можливих розмірів збитків.

Окрім питань, що стосуються кількісної оцінки ризику, існують концептуальні проблеми навколо корельованого ризику та відсутності перестрахування. Також традиційні питання страхового ринку стосуються кіберстрахування, включаючи моральний ризик та несприятливий відбір, спричинений

асиметрією інформації. Наприклад, існує моральний ризик, пов'язаний з компаніями, які можуть не відчувати потреби в поліпшенні кібербезпеки, якщо вони застраховані [9]. Інші проблеми, пов'язані з кіберстрахуванням, включають відсутність законодавчої бази, невизначеність відповідальності та відсутність кіберстандартів.

Розуміння передбачуваних ймовірностей та наслідків кібератак, а також досвіду та сприйняття заходів щодо пом'якшення наслідків та страхових потреб може полегшити розробку стратегій подолання цих упереджень та покращити готовність ринку страхових послуг до надання якісного покриття та формування продуктів кіберстрахування, які відповідають сучасним потребам.

Список використаних джерел

1. Szymańska A., Klapkiv J. Impact of the e-commerce on distribution channels of insurance services. Proceedings of the 10th International Conference on Applied Economics Contemporary Issues in Economy: Finance. Olsztyn: Institute of Economic Research. 2019. P.171-180.

2. Klapkiv Y., Klapkiv J. Technological Innovations in the Insurance Industry. Rozprawy Ubezpieczeniowe, nr 26 (4), 2017. s. 67-78

3. Trynchuk, V., Khovrak, I., Dankiewicz, R., Ostrowska-Dankiewicz, A., Chushak-Holoborodko, A.The role of universities in disseminating the social responsibility practices of insurance companies. Problems and Perspectives in Management, 2019. 17(2). c.449-461.

4. Klapkiv L., Klapkiv Y. Methods for the identification of cyber risks: an analysis based on patent data CBU International Conference Proceedings Vol 6, 2018. p. 241-246'

5. Клапків Ю., Мелих О. Трансформація діджиталізації ринку фінансових та страхових послуг. Review of transport economics and management, 2019. № 2(18). С.83-89.

6. Łyskawa, K.; Kędra, A.; Klapkiv, L.; Klapkiv, J.. Digitalization in insurance companies International Scientific Conference Contemporary Issues In Business, Management And Economics Engineering 2019, 842- 852.

7. Tonn, G., Kesan, J.P., Zhang, L., Czajkowski, J., Cyber risk and insurance for transportation infrastructure. Transport Policy. 2019. 1-16

8. Klapkiv Y., Klapkiv L., Zarudna N Online distribution of insurance of civil liability of owners of vehicles, the experience of Poland, opportunities of Ukraine. Baltic Journal of Economic Studies, Vol. 4, No. 1, 2018.- pp.195-201.

9. Trynchuk V. Management of visual communications in insurance companies (on the example of using icons in logos). Problems and Perspectives in Management, 2017. 15 (2-2). 319-331.