2. Андрос С.В., Герасимчук В.Г. Фінансування сільського господарства і роль банків у кредитному забезпеченні аграрного сектора України.URL: https://economics.net.ua/ejopu/2023/No3/5.pdf.

КІБЕРСТРАХУВАННЯ ЯК ВІДПОВІДЬ НА СУЧАСНІ ВИКЛИКИ ЦИФРОВОГО ПРОСТОРУ

Пономаренко Ольга Володимирівна
викладач, здобувач третього освітньо-наукового рівня вищої освіти (доктор філософії)
Уманський національний університет садівництва

Зростаюча залежність сучасного суспільства від цифрових сервісів змушує організації вкладати значні кошти в адміністративні та технічні заходи щодо запобігання випадковим або зловмисним інцидентам кібербезпеки. Однак реальність сучасних кібератак та інцидентів кібербезпеки із серйозними наслідками засвідчила, що управління кібербезпекою організації не може покладатися лише на заходи зі зниження ризиків [1].

Кіберстрахування, також відоме як страхування кібервідповідальності або страхування кібербезпеки, - це поліс, який компанії можуть придбати для зниження фінансових ризиків, пов'язаних із веденням бізнесу в Інтернеті. Поліс передає частину ризику страховику в обмін на щомісячну або щоквартальну премію [2]. Такі поліси можуть змінюватися з місяця в місяць, враховуючи динамічний і мінливий характер пов'язаних з ними кіберризиків. На відміну від усталених страхових планів, андеррайтери полісів кіберстрахування мають обмежену кількість даних для формулювання моделей ризиків з метою визначення страхового покриття, тарифів і премій.

Кіберстрахування з'явилося наприкінці 1990-х років як відповідь на зростання залежності від технологій і збільшенням кількості кіберзагроз. Спочатку воно охоплювало витік даних і комп'ютерні атаки, але згодом розширилося і стало охоплювати широкий спектр кіберзлочинів, зокрема здирництво, кіберздирництво, атаки соціальної інженерії, збої в роботі систем і переривання бізнесу внаслідок інцидентів, пов'язаних із кібербезпекою [3].

Кіберстрахування походить від страхування помилок і упущень (E&O) - окремої форми страхування, що захищає від помилок і дефектів у послугах, які надають компанії. Страхування помилок і упущень аналогічно страхуванню відповідальності за якість продукції для компаній, що продають фізичні або цифрові товари. Деякі поліси кіберстрахування містять окремі

пункти про страхування відповідальності за підприємницькі ризики, але більшість провайдерів продають їх як окремий поліс. Поліси страхування відповідальності не покривають втрату даних третіх осіб, наприклад, номерів кредитних карт клієнтів. Клієнти, яким необхідний такий захист, можуть придбати таке кіберстрахування.

Останніми роками кіберстрахування привертає увагу вчених і страхової індустрії як бізнес, що розвивається. Купуючи кіберстрахування, страховики прагнуть захистити себе від кіберзагроз, передаючи кіберризики третім особам. На відміну від традиційних страхових продуктів, кіберстрахування виходить за рамки компенсації фінансових втрат. Бізнес-модель, що лежить в основі кіберстрахування, передбачає комплекс послуг, спрямованих на мінімізацію негативних наслідків для організації від кіберінцидентів [1].

Кіберстрахування надає ряд переваг, включаючи захист від кіберризиків, фінансовий захист, юридичну підтримку, відчуття безпеки і акцент на прихильності до безпеки. Кіберстрахування визнано важливим інструментом захисту бізнесу від кіберподій, включаючи кібератаки та інциденти, пов'язані з тероризмом. Фінансовий захист, який забезпечує кіберстрахування, включає компенсацію витрат на розслідування, правову допомогу та інші витрати, пов'язані з витоком даних, а також компенсацію за втрату доходів і відновлення комп'ютерних систем. Крім того, кіберстраховий захист надає компаніям відчуття безпеки та спокою, що дозволяє їм зосередитися на своїй основній діяльності. Нарешті, відображає прихильність компанії до захисту даних і може підвищити її репутацію та довіру до неї з боку зацікавлених сторін [4].

У США існує низка великих страхових компаній, які пропонують своїм клієнтам кіберстрахування. Залежно від вартості та змісту полісу, клієнти можуть розраховувати на покриття додаткових витрат, пов'язаних з фізичним знищенням або крадіжкою ІТ-активів. Ці витрати можуть включати:

- виконання вимог зловмисників в результаті атаки програм-вимагачів;
- повідомлення клієнтів про порушення безпеки;
- оплата судових витрат і витрат, понесених у зв'язку з порушенням конфіденційності;
- залучення експертів з комп'ютерної криміналістики для відновлення скомпрометованих даних;
- відновлення персональних даних клієнтів, чиї персональні дані були скомпрометовані.
- відновлення змінених або викрадених даних.
- ремонт або заміна пошкоджених або скомпрометованих комп'ютерних систем.

Оскільки традиційні страхові поліси зазвичай не включають покриття кібер-ризиків, страхування кібер-безпеки стає все більш популярним як окремий вид захисту. Потенційними клієнтами є компанії, які здійснюють цифрові транзакції або зберігають персональні дані клієнтів, включаючи медичну та фінансову інформацію [5].

У сучасному цифровому світі кіберзагрози стають дедалі серйознішим викликом для організацій у всіх секторах. З огляду на постійно зростаючий ризик кібератак і витоку даних, кіберстрахування стає важливим інструментом захисту компаній від цих загроз. Хоча профіль ризиків кожної організації відрізняється, більшість компаній можуть отримати вигоду від кіберстрахування. Галузі, які підходять для кіберстрахування, включають підприємства різного масштабу, постачальників медичних послуг, фінансові установи, державні установи, навчальні заклади. Кіберстрахування корисне для широкого спектру галузей, від малого та середнього бізнесу до великих корпорацій та державних установ. Захист від кіберзагроз є важливим аспектом сучасного ризик-менеджменту, а кіберстрахування - ефективним інструментом забезпечення фінансової стабільності та безпеки організацій у цифровому середовищі.

Список використаних джерел

1. Schütz F., Rampold F., Kalisch A., Masuch K. (2023). Consumer Cyber Insurance as Risk Transfer: A Coverage Analysis. Procedia Computer Science 219. 521–528.

2. International Telecommunication Union (ITU). Measuring digital development: Facts and figures 2021. Режим доступу: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf;

3. European Insurance and Occupational Pensions Authority (EIOPA). Understanding Cyber Insurance: A Structured Dialogue with Insurance Companies. Luxembourg: Publications Office of the EU; 2018.

4. Risk Management Solutions. Managing Cyber Insurance Accumulation Risk: Report prepared in collaboration with and based on original research by the Centre for Risk Studies. University of Cambridge; 2016

5. Martin Lee (2022). Cyber insurance: The good, the bad and the ugly. Режим доступу: https://www.computerweekly.com/opinion