Вишневський П. П.,
здобувач вищої освіти обліково-фінансового факультету
Науковий керівник – **Мельник О. І.**, канд. екон. наук, доцент,
доцент кафедри фінансів, банківської справи та страхування,
Миколаївський національний аграрний університет, м. Миколаїв

РИЗИКИ КІБЕРСТРАХУВАННЯ: АКТУАЛЬНІСТЬ У СУЧАСНОМУ БІЗНЕС-СЕРЕДОВИЩІ

У наш час проблема кібербезпеки є особливо актуальною. Враховуючи стрімкий розвиток сучасних технологій та їх інтеграцію у різні сфери життя суспільства, інформаційна безпека або кібербезпека є одними із найбільш вагомих питань, які хвилюють як уряди держав та міжнародних організацій, так і сучасні підприємства. З огляду на це, варто зазначити, що на сьогодні існує низка проблем, пов’язаних з глобальними порушеннями кібербезпеки на різних рівнях. Зокрема, до актуальних проблем кібербезпеки можна віднести: технічні проблеми; вразливість; соціальні та поведінкові проблеми; кримінальну діяльність у кіберпросторі; кібератаки; порушення конфіденційності та безпеки даних тощо.

Особливо актуальними ці проблеми є саме сьогодні, що пов’язано як з актуальним станом розвитку сучасних технологій, зокрема – з появою штучного інтелекту, так і з сучасним станом безпеки у бізнес-середовищі на регіональному та глобальному рівні. Діяльність компаній безпосередньо пов’язана з новітніми технологіями, соціальними мережами, базами даних, електронною комунікацією тощо. Тому у мережі Інтернет зберігаються конфіденційні та стратегічно важливі дані компаній, які обов’язково мають бути захищені. Враховуючи зростаючі загрози у віртуальному просторі, актуальним стає кіберстрахування, що дає можливість уникнути негативних наслідків від кіберзагроз та сучасних ризиків бізнес-середовища.

Згідно з визначенням сучасних дослідників, кіберстрахування є страховим продуктом, що пов’язаний із передачею фінансового ризику третій стороні – страховій компанії, з метою надання допомоги державі, суспільству, суб’єктам господарювання або фізичним особам зменшити вплив ризику за допомогою компенсації витрат, які пов’язані з ймовірно руйнівними наслідками кіберзлочинів, забезпечити їх захист від збитків, які можуть настати внаслідок порушення безпеки та конфіденційності. У такому випадку суб’єкти господарювання отримують страхові послуги від страхової компанії, яка надає необхідну допомогу у разі настання кіберзагроз з метою ліквідації їх негативних наслідків, а також для того, аби захистити компанію від збитків, які можуть виникнути внаслідок цього [1]. Крім того, у випадку кіберстрахування компанії захищені від різноманітних кібер-загроз, а саме – кібератак, крадіжки даних, вірусів та інших видів кіберзлочинності [2].

Роль кіберстрахування зростає протягом останніх років у зв'язку зі збільшенням кількості кіберризиків або ризиків кіберстрахування. Кіберризик характеризують як ймовірність виникнення подій, які шкодять роботі IT-системи та кібербезпеці організації внаслідок стороннього втручання цифрових та інших електронних технологій. Наслідком таких подій є виникнення збитків, руйнування цифрових активів, а також можлива втрата репутації організації. Серед найбільш актуальних кіберризиків зазначимо наступні:

- ризики викрадення конфіденційних даних у вигляді паролів доступу чи інших конфіденційних даних і збою системи, що є результатом DDoS-атак;
- ризик виникнення фінансових збитків компанії у результаті збою комп'ютерної системи;
- ризики фінансових втрат, які виникають внаслідок регресу компанії, причиною чого є витік особистої інформації або її крадіжка;
- ризик фінансових збитків, які можуть виникнути внаслідок вимагання коштів у комп'ютерній системі, яка була пошкоджена вірусом;
- ризики фінансових втрат, які можуть бути спрямовані на поновлення програмного забезпечення компанії, а також її інформації, які були пошкоджені чи викрадені у результаті дій кіберзлочинців.

Усі ці кіберризики є актуальними для сучасного бізнес-середовища. Пов'язано це з тим, що бізнес-середовище фактично представлене і у реальному житті, і у віртуальній мережі, тому майже усі компанії зберігають у спеціальних базах даних та хмарних джерелах особисту інформацію, важливі документи та кошти. Окрім цього, зростає кількість випадків виникнення кібератак, від яких страждають вітчизняні підприємства. Кібератаки стають причиною зупинки діяльності компаній, у результаті чого вони можуть понести суттєві втрати.

Кіберризики мають різну природу та різні наслідки, у зв'язку з чим застосовуються особливі напрями кіберстрахування. Серед найбільш поширених зазначимо такі:

- відшкодування витрат на відновлення інформаційних технологій;
- вахист компаній від збитків, які можуть завдати кіберзлочинці;
- компенсація компаніям збитків, які можуть бути завдані у результаті витоку персональних даних;
- покриття витрат на розблокування інформаційних систем у разі виникнення кіберзлочинів;
- відшкодування вартості програмного забезпечення, відновлення втраченої інформації тощо.

Ризики кіберстрахування стають все більш поширеними для сучасних компаній. Все частіше вони стають жертвами кібератак, витоку даних, шкідливого програмного забезпечення, страждають від масових кібератак та збоїв в інформаційних системах тощо. Також на компанії покладена відповідальність зберігати конфіденційні дані клієнтів. У зв'язку з цим, зростає

актуальність кіберстрахування, яке передбачає страхування підприємств від кіберризиків. В Україні кількість таких компаній обмежена: станом на 2023 рік послуги з кіберстрахування надавали ПрАТ «UPSK» та ПрАТ «АСКА». Перша компанія пропонує клієнтам комплексне страхування, куди входить також страхування від кіберризиків. Друга компанія пропонує страхування на випадок конкретного ризику, тобто має місце індивідуальний підхід.

В Україні немає чітких стандартів та правил у контексті страхування кіберризиків, також недостатньо розвинене кіберстрахування в цілому. Крім того, вітчизняні страхові компанії не мають достатньо досвіду у роботі з кіберризиками, тому це може принести додаткові ризики для їхньої фінансової стабільності. У такому випадку ризики кіберстрахування можна розглядати також у контексті ризиків для діяльності страхових компаній, які надають послуги зі страхування на випадок кіберризиків [3].

Таким чином, кіберстрахування в умовах розвитку сучасного бізнес-середовища стає все більш актуальним, оскільки дає можливість захистити компанії від виникнення кіберзагроз та кіберризиків, а також їхніх негативних наслідків. Ризики кіберстрахування пов’язані з тим, що діяльність компанії безпосередньо пов’язана з віртуальним середовищем, тому виникнення кіберзагроз може мати негативні наслідки, що створює необхідність у забезпеченні кіберстрахування. Розвиток кіберстрахування в Україні не є достатнім, тому в майбутньому важливо вдосконалювати цей напрям страхування, з огляду на зростаючі ризики у бізнес-середовищі.

Список використаних джерел:

1. Пікус Р. В., Бабенко Ю. Л. Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава.* 2022. №2. С. 134-140. URL: http://www.economy.in.ua/pdf/2_2022/25.pdf
2. Попович Д. В., Бундз Н. Б., Іванків В. О. Проблеми та перспективи розвитку страхування кіберризиків на національному ринку. *«Молодий вчений».* 2023. №4 (116). С. 168-172. URL: https://financial.lnu.edu.ua/wp-content/uploads/2015/10/2.pdf
3. Кіберстрахування несе значні ризики для фінансової стабільності страховиків. URL: https://forinsurer.com/news/24/02/08/43507