СТРАХУВАННЯ КІБЕРРИЗИКІВ ЯК СКЛАДОВИЙ ЕЛЕМЕНТ СИСТЕМИ ЕФЕКТИВНОГО МЕНЕДЖМЕНТУ: КЕЙС УКРАЇНИ

Ганна Нямещук
ORCID: https://orcid.org/0000-0003-3199-8988
Дніпровський національний університет імені Олеся Гончара, Дніпро

Вероніка Біла
ORCID: https://orcid.org/0009-0002-6810-0473
Дніпровський національний університет імені Олеся Гончара, Дніпро

Розвиток цифрової економіки, імпульс якого задається постійним вдосконаленням технологій, актуалізує питання кібербезпеки [6, 8]. Природньою реакцією сучасних організацій на підвищення ризику кібератак є зростання попиту на відповідні послуги страхування [7]. Вагомий внесок у дослідження нового сегменту ринку страхових послуг в Україні зробили такі автори, як В.П. Братюк, В.П. Ільчук та Д.О. Сугонянко; О.М. Парубець.

Кіберризик – це ймовірність виникнення того, що робота IT-систем або кібербезпека організації буде порушена через несанкціоноване втручання в роботу цифрових або інших електронних технологій, знищення цифрових активів та завдасть потенційну шкоду репутації організації [4].

У відповідь на актуалізацію проблеми кіберризиків, українські страхові компанії диференціюють свою продуктову політику («UPSK», «ACKA», «AON» та інші). Як основні джерела загроз, при цьому, ідентифікують такі: витік конфіденційної інформації, вимоги викупу після атак програм-викрадачів (вимагачів), помилка програмування. Страхування кіберризиків стає важливим інструментом захисту бізнесу та організацій.

У цій статті розглянемо важливість страхування від кіберризиків в Україні, проаналізуємо поточні тенденції на ринку страхування кіберризиків та розглянемо перспективи його розвитку. Страхування від кіберризиків допомагає підприємствам зменшити фінансові ризики, пов'язані з кібератаками, та забезпечити фінансову підтримку в разі настання страхової події.

В Україні у 2023 р. кількість кібератак зросла порівняно з 2022 р. на 15,9 % до 2543 інцидентів (рис.1). За даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, протягом 2022 р. Україна стикнулася з 7000 кібератак на національну інформаційну інфраструктуру. Україна – друга серед найбільш атакованих

країн світу після США, каже технічний директор IT-компанії UNITY-BARS, що розробляє ПЗ для фінансових установ, О. Музика.

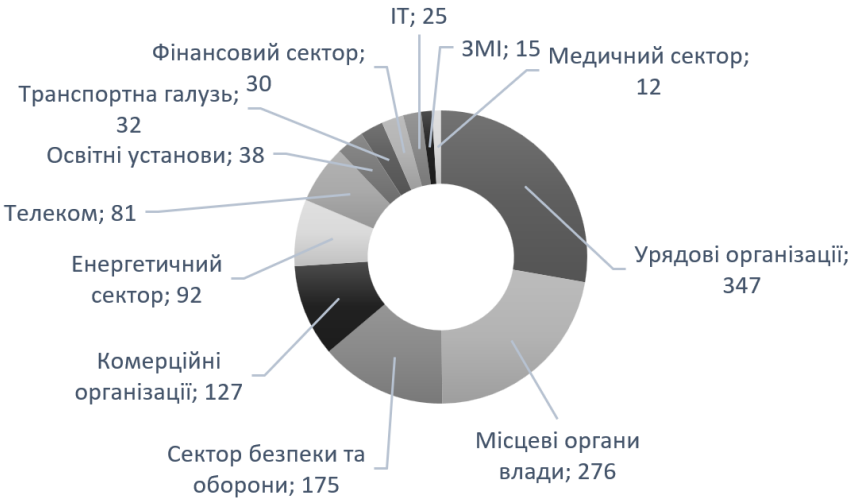

Рисунок 1 – Кількість кібератак в Україні за секторами національної економіки в 2023 р., од.

У 2022 р. кібератак побільшало у 3,5 рази порівняно з 2021-м – на фінансовий сектор України припадає 5 % усіх атак, на IT-сектор – 10 % [9].

Страхові компанії диференціюють пропоновані спеціалізовані продукти залежно від розміру підприємств-споживачів. Нові страхові поліси охоплюють різні аспекти кібербезпеки: відшкодування збитків, юридична підтримка та послуги експертів з безпеки. На сьогоднішній день український ринок страхових послуг у сфері кіберризиків значно відстає за ступенем свого розвитку від зарубіжного. Великі страхові компанії світу, які є давніми акторами ринку, вже успішно ввели цей продукт у перелік надаваних послуг.

На фоні військового стану передбачуваною виглядає схильність кіберзлочинців до здійснення більш агресивних і складних кібератак, бо агресор має на меті не тільки захоплення територій України. Зокрема, об'єктом цільових атак можуть стати системи інфраструктури, електронні системи комунікації та інформаційні ресурси країни. Прогнозується, що організації стикатимуться із підвищеними ризиками витоку конфіденційної інформації, знищення даних та перериванням роботи [1]. Тому ПАСТ « Новий Дніпро», зокрема, вже розглядає як стратегічний крок можливість розвитку страхування кіберризиків.

Страхування кіберризиків, на нашу думку, може стати важливим інструментом підтримки організацій під час військового стану. Використання такого інструменту дозволить суб'єктам господарювання компенсувати фінансові збитки, пов'язані з кіберінцидентами, забезпечити швидке відновлення бізнес-операцій, отримати доступ до експертної допомоги з кібербезпеки та ресурсів, що є необхідними для реагування на загрози.

Незважаючи на позитивні зрушення вцілому, страхування кіберризиків в Україні стикається зі своїми викликами:

- недостатнє розуміння джерел, форм кіберризиків та їх наслідків бізнес-суб'єктами та страховими компаніями. Це може призводити до недооцінки ризиків і неправильного вибору страхового покриття ;

- складність оцінки ризиків. Кіберризики є динамічними, що ускладнює процес їх оцінки страховими компаніями. Відсутність історичних даних або точних моделей ризику може ускладнювати визначення правильного рівня покриття та встановлення адекватних премій;

- висока вартість страхування. Україна на сьогодні є країною з високим рівнем ймовірності кіберагресії, що може призводити до значних витрат на страхування кіберризиків. Для багатьох українських підприємств, в умовах економічної кризи, це може стати додатковим і непосильним фінансовим тягарем. Особливо це є актуальним для малих та середніх підприємств;

- висока індивідуалізація умов страхового полісу. У сфері страхування кіберризиків ще не сформувалися чіткі стандарти та умови полісів. Кожна страхова компанія може реалізовувати власний підхід до формулювання умов страхування, що ускладнює порівняння та вибір оптимального страхового продукту;

- ранній етап становлення національного ринку. Ринок страхування кіберризиків в Україні є значно «молодшим» і нерозвиненим у порівнянні із ринками країн світу, що обумовлює обмеженість набору страхових продуктів і послуг.

Зважаючи на виявлені особливості національного ринку страхування кіберризиків, перед Україною постають виклики розробки адекватної стратегії та швидкої адаптації. Найпершим, на наш погляд, інструментом для ефективного розвитку такого ринку, є якісна профільна освіта та обізнаність. Безперешкодний доступ до інформації про потенційні кіберризики, способи запобігання і захисту від них може значно знизити ймовірність настання страхової події.

Урядові програми, тренінги для бізнесу та освітні ініціативи для шкіл й університетів можуть сприяти посиленню кібербезпеки в Україні. Різноманітні інформаційні плакати в громадському транспорті,

на вулицях, реклама на телебаченні і в мережі Інтернет відіграють важливу роль для підвищення рівня обізнаності населення і бізнес-суб'єктів.

Наступним кроком ефективного розвитку ринку може бути створення відповідної кіберінфраструктури: розробка найсучасніших технологій кіберзахисту, створення центрів обробки даних і розробка національної програми кібербезпеки. Інвестуючи в інфраструктуру, країни стають більш стійкими до кіберризиків. Багато країн Європи, таких як Великобританія, Німеччина, Франція та Швеція, також роблять значні інвестиції в кібербезпеку, як на рівні уряду, так і в приватному секторі [10].

Ефективна стратегія попередження кіберризиків вимагає співробітництва між державними установами, приватним сектором та громадськістю. Налагодження партнерських відносин та обмін актуальною інформацією про потенційні та актуальні загрози з компаніями, що здійснюють діяльність у секторі кібербезпеки, можуть розглядатися як необхідні елементи системи реагування і попередження кіберризиків.

Удосконалення сучасної правової бази є важливим аспектом покращення захисту від кіберризиків. Це допомогає встановити відповідальність за порушення кіберзаконодавства та врегулювати поширення інформації в цифровому просторі.

Підбиваючи підсумки зазначимо, що страхування кіберризиків є лише одним складовим елементом системи кібербезпеки. Страхування не може замінити надійну систему безпеки, яка вимагає сучасних технологій, навчених команд фахівців й перевірених процедур. Страхування кіберризиків в Україні набуває все більшого значення як інструмент захисту підприємств.

Страхування кіберризиків дозволяє організаціям відшкодовувати фінансові втрати, пов'язані з кіберінцидентами, забезпечувати швидке відновлення бізнес-операцій, отримувати доступ до експертної допомоги з кібербезпеки та необхідних ресурсів для реагування на загрози.

Розвиток страхування кіберризиків має великий потенціал за напрямом захисту конфіденційної інформації. Важливо і надалі інвестувати в розвиток інформування населення та бізнесу про загрозу атак. Якщо буде співпраця між державою, бізнесом та суспільством , то буде значно менше кібератак і люди будуть мати захист в разі виникнення проблем.

Посилання

1. Кевлюк, В. (2024, March 27). *Росія: експорт хаосу*. LB.ua. https://lb.ua/news/2024/03/27/605459_rosiya_eksport_haosu.html

2. *Кібер-страхування: новий інструмент ризик-менеджменту*. (n.d.). Parasol.UA. https://parasol.ua/ua/news/kiber-strahovanie-noviy-instrument-risk-menedzhmenta

3. Про основні засади забезпечення кібербезпеки України, Закон України No. 2163-VIII (2024) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text

4. План для підприємця уникнення від кібер-ризику. URL: https://www.thebalancesmb.com/cyber-liability-insurance-coverage-fordata-breaches-462582

5. Пікус, Р.В., Бабенко, Ю.Л. (2022). Перспективи розвитку страхування від кібератак в Україні. *Економіка*. 2, 25. https://doi.org/0.32702/2306-6806.2022.2.134

6. Нямещук, Г. В. (2014). Розвиток інформаційно-мережевих технологій як джерело загроз глобальної економіки. *Економічна безпека в умовах глобалізації світової економіки*, Т. 1. 466, 158-165.

7. Нямещук, Г. В. (2019). Крихкість як стратегічна проблема глобальних експонентних організацій. *Економічний простір. Збірник наукових праць*. 152, 29 – 42. https://doi.org/10.32782/2224-6282/152-3

8. Нямещук, Г. В. (2021). Технологічний бек-граунд сучасного етапу розвитку міжнародних економічних відносин. *Системний аналіз міжнародних економічних відносин*, 301, 167 – 169.

9. Бегаль, І. (2023, May 4). *У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики — forbes.ua*. Forbes.ua https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454

10. *Cybersecurity policy*. (n.d.). ENISA. https://www.enisa.europa.eu/topics/cybersecurity-policy/?tab=publications