НЕОБХІДНІСТЬ ТА ОСОБЛИВОСТІ КІБЕРСТРАХУВАННЯ

Бобовніков О.А., здоб. ОС «магістр»
Науковий керівник – канд. екон. наук, доц. **О.В. Жилякова**
Державний біотехнологічний університет

Кіберстрахування донедавна сприймалося як інновація, сьогодні – це обов'язкова умова існування бізнесу, тому що пандемія Covid-19 суттєво прискорила процеси цифрової трансформації та, як наслідок, неминуче посилилися кіберзагрози. Витікають вони, як з поширення цифровізації, так і зі зростання значення для компаній так званих «нематеріальних активів» – об'єктів інтелектуальної власності, які потребують особливого захисту.

Протягом 2022 року Україна стикнулася з 7000 кібератак на інформаційну інфраструктуру. За минулий рік в Україні було зареєстровано у 3,5 раза більше кіберінцидентів – на фінансовий сектор України припадає 5% усіх атак, на IT-галузь – 10%ніж у 2021-му. З початку 2023 року (порівняно з IV кварталом 2022-го) кібератак від проросійських угруповань поменшало, але вони систематичні та інтенсивні. За I квартал цього року фахівці CERT-UA опрацювали 549 кібератак, серед яких 13 – на фінсектор, 23 – на комерційний сектор і 11 – на розробників програмного забезпечення. Цьогоріч, крім банків, кіберзлочинці атакують страхові компанії і розробників ПЗ для банків, кажуть у НБУ[1].

За таких умов кіберстрахування стає бажаною та реальною можливістю для компаній скоротити збитки від подібних інцидентів.У зв'язку зі значною інтеграцією до міжнародної спільноти в Україні з'явився та зростає попит на поліси кіберстрахування.

Поняття «кіберризик» стосується усіх уразливостей, які виникають у зв'язку з використанням комп'ютерного обладнання та програмного забезпечення в інтернет-мережі, платіжних системах, сфері електронної комерції, CRM-системах, IT-інфраструктурах. Також в це поняття входять ризики, пов'язані з накопиченням, зберіганням та використанням в електронному вигляді персональних даних.

Поліси кіберстрахування як страхові продукти для захисту бізнесу та фізичних осіб поки не мають уніфікованих характеристик. У різних страхових компаніях вони істотно різняться за умовами та лімітами відповідальності. Страхуванню підлягають такі страхові кіберризики: технічні збої, помилки програмування та відмови роботи IT-систем; нецільові атаки – фішинг, sms-шахрайство, картинг, хактивізм; цільові (таргетовані) атаки – DDoS атаки, промислове

шпигунство, кріптолокерство (кіберздирництво); внутрішні атаки – викрадення конфіденційної інформації та відомостей, що являють собою комерційну таємницю, сприяння зовнішнім атакам зсередини.

Враховуючи, інноватівність кіберстрахування законодавче регулювання цієї сфери страхових послуг поки відсутнє. В переліку видів добровільного страхування згідно Закону України «Про страхування» кіберстрахування чи аналогічний за змістом напрям відсутні. Тобто кіберстрахування потрапляє під визначення «інші види добровільного страхування»[2].

Особливість кіберстрахування полягає у тому, що у зв'язку з відсутністю законодавчого регулювання сфери кіберстрахування в Україні, основою для встановлення регламентів, прав та зобов'язань між страхувальником і страховиком, а також для можливого вирішення спорів є договір кіберстрахування.

Також, враховуючи невелику кількість статистичних даних щодо страхових випадків в кіберсфері, формуючи пропозиції для клієнтів, кожна компанія може спиратися тільки на власну експертизу та пропонувати свій пакет кіберстрахування.

В сучасних умовах страхові компанії швидко змінюються. На разі стрімко розвивається InsurTech, що передбачає технології машинного навчання та передові розробки у сфері кібербезпеки, технологію блокчейн та аналіз великих даних. Це дозволяє формувати для споживачів дійсно актуальні продукти зі страхування кіберризиків.

До основних напрямів державної підтримки слід віднести: розробку моделей ризику на основі вже зібраних даних; структурування премій страховими компаніями для стимулювання поведінки, що знижує ризики, і впроваджувати кращі світові практики у свою діяльність; стимулювання або впровадження обов'язкового кіберстрахування для державних та фінансових установ, які відповідають мінімальним стандартам.

Таким чином, поняття кіберстрахування для України є доволі новим і мало дослідженим, але сьогодні воно набуває актуальності, оскільки українські підприємства та організації потребують захисту від кібератак.

Інформаційні джерела

Бегаль І. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики. URL: https://forbes.ua/news/-04052023-13454

Закон України «Про страхування» URL: https://zakon.rada.gov.ua/laws/show/85/96-%D0%B2%D1%80#Text