РОЗВИТОК КІБЕРСТРАХУВАННЯ В УКРАЇНІ ТА СВІТІ

***Дєвочко О.А.**, здобувач вищої освіти*
***Костенко Ю.О.**, канд. техн. наук, доцент*
Харківський національний автомобільно-дорожній університет

Розвиток технологій та цифровізація суспільства призвели до того, що кіберзагрози стали невід'ємною частиною життя. Інформаційна безпека стає все важливішою для компаній та фізичних осіб, які намагаються захистити свої дані та інформацію від кібератак. У зв'язку з цим, кіберстрахування стає все більш популярним видом страхування.

Проблеми становлення та перспективи розвитку кіберстрахування, впровадження підходів до управління кіберризиками у страхуванні досліджені в наукових працях вітчизняних та зарубіжних дослідників, вчених та практиків, зокрема: В. Братюка, С. Ванга, В. Ільчука, Дж. Кесена, О. Кондратьева, Й. Малкотра, Л. Мамаевої, Т. Моташко, О. Парубець, С. Перцової, Н. Приказюка, Т. Ротової, Д. Сугоняко, К. Хейєса, Ю. Шевченко, С Шекелфорда. Серед проблем кіберстрахування можна виділити неналежну нормативно-правова базу в сфері кіберстрахування, низьку свідомість юридичних осіб щодо кіберризику та його наслідків.

У Вікіпедії наводиться таке визначення кіберризику «… це ризик, пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення як в місцевих (локальних) мережах, так і в глобальній інтернет-мережі; в розрахунково-платіжних системах, у системах інтернет-торгівлі і в промислових системах управління. Також, це ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних» [1].

Статистика свідчить про те, що втрати світової економіки внаслідок кібератак збільшуються з кожним роком.

І ці невтішні дані все частіше наводять керівництво компаній на думку про необхідність страхування кіберризиків.

Кіберстрахування – це страхування, яке захищає від наслідків кібератак, крадіжок даних та інших подібних загроз, що пов’язані з використанням інформаційних технологій.

Згідно з дослідженням компанії Allianz Global Corporate & Specialty, кіберзагрози зараз є одним з найбільших ризиків для бізнесу у всьому світі. Інциденти, такі як відключення інформаційних технологій, атаки з вимогою викупу або порушення безпеки даних, займають перше місце вже другий рік поспіль. Частота атак програм-вимагачів залишається підвищеною, а середня вартість витоку даних знаходиться на рекордно високому рівні в 4,4 мільйона доларів і, як очікується, зросте до більш ніж 5 мільйонів доларів цього року.

Існує багато видів кіберзагроз, з якими стакається малий та середній бізнес. Koziol J., Watts R., Bottorff C. виділяють декілька основних:

– «прогами-вимагачи. Прогами-вимагачи можуть бути різних форм і розмірів, але всі вони функціонують з однією основною концепцією: ви повинні заплатити викуп, щоб отримати доступ до своїх даних. Часто зловмисники отримують другий викуп, щоб запобігти продажу вкрадених даних в Інтернеті;

– поширення облікових даних. Поширення облікових даних відбувається, коли зловмисник використовує вкрадені облікові дані однієї організації для доступу до облікових записів користувачів в іншій організації. Ці облікові дані, як правило, отримані в разі злому або придбані в темній мережі. Як приклад, можна навести злом облікових записів Disney Plus, але Disney не знайшов доказів примусового входу. Це пов'язано з тим, що заповнення облікових даних просто передбачає вхід в обліковий запис жертви за допомогою власного імені користувача та пароля;

– соціальна інженерія. Соціальна інженерія – це не порушення системи, а скоріше компрометація людини, яка змушує її несвідомо оприлюднювати конфіденційну інформацію. Найчастіше це відбувається у формі фішингової атаки електронної пошти, під час якої особу обманом змушують завантажити шкідливе програмне забезпечення або відмовитися від своїх облікових даних. Як правило, соціальна інженерія є першим кроком у багатоступеневій кібератаці» [2].

Перші договори страхування кіберризиків були укладені ще в 2010-2011 роках. Цю тему активно обговорювали на щорічному форумі в Давосі в 2012 році. Але активне зростання даного виду страхування почалося кілька років по тому, після масових зломів корпоративних і урядових ресурсів в США. Тому 90% ринку страхування кіберризиків припадає саме на Сполучені Штати Америки [3].

Розвиток кіберстрахування зростатиме. За даними Standard & Poor's Corp у найближчому майбутньому страхові внески в цій сфері збільшаться в середньому на 20-30% на рік. Використання нових технологій в бізнесі, таких як IoT, цьому всіляко сприяють. Тож не дивно, адже таким чином кількість векторів атак збільшується, а бажаючих спробувати свої сили хакерів теж не стає менше.

У міру того, як кіберстрахування ставатиме більш зрілим, правила страхування і управління кіберризиками посиляться. Високу планку задаватимуть регулюючі органи, які будуть прагнути забезпечити належні стандарти збору даних і регулярної звітності. Можливо, кіберстрахування стане однією з обов'язкових вимог для певних компаній – представників фінансового сектора і охорони здоров'я. [4]

Війна в Україні та ширша геополітична напруженість підвищили ризик широкомасштабної кібератаки з боку спонсорованих державою суб'єктів. [5]

Вона не стала стартом для кібератак зі сторони рф, проте стала своєрідним каталізатором, адже кількість та інтенсивність кіберзлочинів значно зросла. Щодня Росія вдається до кібератак різного масштабу та рівня.

Проте, за даними страхових компаній, ринок кіберстрахування в Україні є досить незначним у порівнянні зі світовими трендами. Це пов'язано з тим, що свідомість про кіберзагрози ще не настільки висока, але зростає.

На даному етапі український страховий ринок відстає від світового рівня розробки і впровадження напрямку кіберстрахування. Лише дві компанії - «UPSK» та «АСКА» пропонують комплексний поліс покриття кібер-ризиків, що свідчить про перспективність розвитку вказаної ніші страхування.

Важливими проблемами, що стримують розвиток кіберстрахування в Україні є: складність щодо виявлення та ідентифікації кіберризиків; неможливість повного покриття збитків від кіберзагроз; неповна та невчасна інформація про кібератаку в зв'язку з можливістю погіршення іміджу організації; низька капітальна база страхових компаній; складність при розрахунку ціни страхового поліса; недостатній рівень контрольних заходів з боку страхувальника; відсутність спеціалізованих програм страхування. [6]

На сьогодні в Україні діє низка Законів України та нормативних документів різних рівнів, які охоплюють проблеми правового забезпечення кібербезпеки. Це, зокрема, Закон України «Про інформацію» [7], Закон України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаціях та інформаційно-комунікаційних системах» [8] та Закон України «Про основні засади забезпечення кібербезпеки України» [9]. Крім того, Верховна Рада України ратифікувала «Конвенцію про кіберзлочинність» [10].

У той же час у вітчизняному нормативно-правовому полі сфери інформаційної безпеки спостерігається використання термінів, які не узгоджені між собою та не мають визначень. Таким чином, доцільно виділити ще три проблеми, які ускладнюють боротьбу з кіберзлочинами в Україні:

– відсутність визначень ключових термінів та категорій у науковій та фаховій літературі;

– неузгодженість чинних нормативно-правових документів у сфері протидії кіберзлочинності;

– відсутність державної системи протидії кіберзлочинам, у тому числі шляхом страхування кіберризиків.

На думку Сергієнкової О.В. та Мелентьєвої О.В., «для ефективного та швидкого розвитку кіберстрахування в Україні необхідно впроваджувати певні заходи державної підтримки, зокрема, до важливих напрямів розвитку кіберстрахування слід віднести:

1. Уряд країни має допомогти страховому ринку в розробці моделей ризику на основі вже зібраних даних.

2. Страхові компанії – оператори кіберстрахування, повинні структурувати премії для стимулювання поведінки, що знижує ризики, і впроваджувати кращі світові практики у свою діяльність.

3. Уряд має стимулювати або впроваджувати обов'язкове кіберстрахування для державних та фінансових установ (купівлю полісів кіберстрахування), які відповідають мінімальним стандартам.

4. Уряд за підзвітністю має надати засновані на даних оцінки витрат на зобов'язання оборонних підприємств купувати кіберстрахування» [11].

Селіверстова Л.С. і Трухан Д.А вважають, що «… для підвищення рівня кіберстрахування в Україні, страховим компаніям потрібно співпрацювати з професійними асоціаціями та регулюючими органами, щоб створити достатній обсяг даних для належного ціноутворення та продажу пос-

луг у сфері кіберстрахування. Додатково, слід орієнтуватися на дрібних клієнтів, оскільки страхові продукти в галузі страхування кіберризиків для невеликих учасників ринку залишаються мало експлуатованими. Також необхідно проводити спеціалізовані освітні кампанії, щоб навчити громадян про питання кіберстрахування та допомогти страховим компаніям оцінити потребу у послугах з кіберстрахування» [12].

Для подальшого розвитку кіберстрахування необхідно використовувати програмне забезпечення з високим рівнем безпеки, включаючи комп'ютери і мобільні пристрої, та регулярно оновлювати комп'ютерні системи. Також потрібно вживати превентивні заходи для запобігання і знищення загроз у цій сфері, такі як сканування інформації. Оскільки кіберстрахування має свої особливості, потрібні певні зміни до законодавства України, які визначать нормативні вимоги до страховиків та застрахованих осіб, суб'єктів та предметів кіберстрахування, умови відшкодування збитків та порядок проведення експертизи кіберризиків від імені страхових компаній. В результаті державне втручання сприятиме росту кіберстрахування як сектору світового страхового ринку [13].

Кіберризик – це проблема, яку можна вирішити за допомогою страхових інструментів і необхідних сприятливих умов. Для вирішення даної загрози потрібна відповідна законодавча база, технічні можливості і готовність клієнтів співпрацювати з страховими компаніями для утворення системи корпоративної кібербезпеки. Оскільки кіберстрахування в України перебуває на початковому етапі свого становлення, під час розроблення підходів щодо його подальшого розвитку треба широко використовувати накопичений позитивний досвід провідних у цій галузі країн світу, який свідчить про диверсифікацію спектра послуг кіберстрахування і застосування окремих полісів страху-

вання від комп'ютерних злочинів, хакерських атак та покритті збитків у процесі їх настання.

Запровадження запропонованих підходів у сукупності із забезпеченням прозорості та розширенням меж взаємодії і співробітництва страхових компаній з іншими економічними агентами приведе до розвитку вітчизняного кіберстрахування, що дасть змогу суттєво зменшити обсяг збитків від настання випадків кібершахрайства.

Перелік посилань:

1. Koziol J., Watts R., Bottorff C. Most Common Cyber Security Threats In 2023. *Forbes*. web-site. URL: https://www.forbes.com/advisor/business/common-cyber-security-threats/ (дата звернення 05.05.2023)

2. Кібер-ризик. *Вікіпедія* : веб-сайт. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80-%D1%80%D0%B8%D0%B7%D0%B8%D0%BA (дата звернення 05.05.2023)

3. Кібер-страхування: новий інструмент ризик-менеджменту. *Parasol.ua*. веб-сайт URL: https://parasol.ua/ua/news/kiber-strahovanie-noviy-instrument-risk-menedzhmenta (дата звернення 05.05.2023)

4. Кіберстрахування: чого чекати в найближчі 5 років? *10Guards*. веб-сайт URL: https://10guards.com/ua/articles/cyber-insurance-what-to-expect-in-the-next-five-years/ (дата звернення 05.05.2023)

5. Cyber: The changing threat landscape. *Allianz Global Corporate & Specialty (AGCS)*. web-site. URL: https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2022.html (дата звернення 05.05.2023)

6. Ротова Т., Шевченко Ю. Страхування як фінансовий інструмент захисту від кібер-ризиків. *Безпека соціально-економічних процесів в кіберпросторі* : матеріали Всеукр. наук.-практ. конф. Київ : КНТЕУ, 2019. С. 177- 178.

7. Про інформацію: Закон України від 02 жовт. 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 06.05.2023).

8. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаціях та інформаційно-комунікаційних системах: Постанова КМУ від 29 бер. 2006 р. № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text (дата звернення: 06.05.2023).

9. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 06.05.2023).

10. Конвенція про кіберзлочинність: Конвенцію ратифіковано із застереженнями Законом України від 07 вер. 2005 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 06.05.2023).

11. Сергієнкова О. В., Мелентьєва О. В. Проблеми і перспективи розвитку страхування банківських ризиків в Україні. URL: http://конференция.com.ua/pages/view/508 (дата звернення: 06.05.2023)

12. Приказюк Н. В., Гуменюк Л. С. Передумови розвитку кіберстрахування. *Інвестиції: практика та досвід*. 2020. № 15-16. С. 28–34.

13. Селіверстова Л.С., Трухан Д.А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава*. 2020. № 1. С. 23–26.

ЕВОЛЮЦІЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ТА ЇЇ РОЛЬ У БУХГАЛТЕРСЬКОМУ ОБЛІКУ

***Кравченко О.В.**, канд. екон. наук, доцент*
Сумський державний університет

Традиційний система бухгалтерського обліку та методи його ведення створили єдині стандарти в цій галузі. Якщо поєднати ці стандарти з транзакціями в блокчейні, то можна використовувати будь-яку фінансову транзакцію як сертифіковане підтвердження бухгалтерського обліку та обліку витрат. Саме тому однією з перспективних сфер застосування блокчейну є бухгалтерський облік.

Стосовно полеміки щодо того блокчейн чи цифровізація взагалі знищують робочі місця, слід поглянути в минуле. З одного боку, Інтернет і, до цього, механізація замінили певні види діяльності, якими раніше займалися люди. З іншого боку, були також створені нові робочі місця за відповідними умовами. Оцифровка та розширені можливості блокчейна в основному залежать від людей, які їх створюють, контролюють та розвивають.

Саме так має розвиватися технологія – керована людиною, з урахуванням людської поведінки та реагуванням