УДК 342.951

КАЛАЙДА Ю.П., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ
ORCID: https://orcid.org/0000-0002-1408-2145

ЗАРУБІЖНИЙ ДОСВІД ЗАПРОВАДЖЕННЯ ТА РОЗВИТКУ СИСТЕМИ СТРАХУВАННЯ КІБЕРРИЗИКІВ: ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ

DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334891

Анотація. *Визначено поняття, роль та значення кіберстрахування, сучасні тенденції розвитку світового ринку кіберстрахування. Окреслено підстави та умови розробки та запровадження системи страхування від кіберризиків. Узагальнено основні аспекти щодо запровадження системи кіберстрахування у світових масштабах. Досліджено досвід США, Канади та Австралії щодо створення та розвитку системи кіберстрахування з урахуванням існуючих національних особливостей. Деталізовано механізми оцінки втрат суб'єктів господарювання внаслідок кібератак для можливості їх відшкодування, які використовуються у проаналізованих державах. Окреслено подальші напрямки впровадження та розвитку вітчизняної системи кіберстрахування з урахуванням кращих практик зарубіжного досвіду у цій площині. Визначено перелік заходів, практичне впровадження яких надасть змогу сприяти впровадженню кіберстрахування в Україні.*

Ключові слова: *кібербезпека, кібератака, кіберризик, кіберстрахування, інформаційно-комунікаційні системи, кіберінцидент, ландшафт кіберзагроз, оцінка, методологічне забезпечення, методика, управління вразливостями, управління ризиками, збитки, механізми оцінки втрат.*

Summary*. The concept, role and importance of cyber insurance, current trends in the development of the global cyber insurance market are defined. The grounds and conditions for the development and implementation of a cyber risk insurance system are outlined. The main aspects of the introduction of a cyber insurance system on a global scale are summarized. The experience of the United States, Canada and Australia in creating and developing a cyber insurance system, taking into account existing national characteristics, is studied. The mechanisms for assessing losses of business entities as a result of cyber attacks for the purpose of their compensation, which are used in the analyzed countries, are detailed. Further directions for the introduction and development of the national cyber insurance system are outlined, taking into account the best practices of foreign experience in this area. A list of measures has been determined, the practical implementation of which will facilitate the introduction of cyber insurance in Ukraine.*

Keywords: *cybersecurity, cyberattack, cyber risk, cyber insurance, information and communication systems, cyber incident, cyber threat landscape, assessment, methodological support, methodology, vulnerability management, risk management, losses, loss assessment mechanisms.*

Постановка проблеми. Активізація хакерської діяльності, глобалізація небезпеки поширення транснаціональної кіберзлочинності продовжують зростати і поступово стають загрозою як світового масштабу, так і для національного рівня, зокрема державного сектора, більшості підприємств, комерційних організацій тощо. За таких умов ІТ-безпека стає пріоритетом для усіх, хто прагне захистити свої системи й конфіденційні дані, інформаційні ресурси та масиви. Але навіть за наявності дієвих та ефективних заходів у сфері кібербезпеки, порушення штатної роботи систем й зокрема

умов гарантування безпеки та збереження даних іноді трапляються і можуть виявитися неймовірно коштовними. Саме тому кіберстрахування залишається важливим напрямком страхування, оскільки воно захищає від наслідків кіберінцидентів, надаючи фінансову компенсацію та кризове управління, коли щось піде не так. Останнім часом зберігається світова тенденція зростання попиту на послуги у сфері кіберстрахування за наслідками скоєння хакерами або кіберзлочинцями масштабних кібератак. Наприклад, після атаки на сервери американської компанії Yahoo (друга за популярністю у світі пошукова система) ще у 2014 році, попит на страхування кіберризиків тільки в США зріс утричі. Тоді хакери зламали близько 500 млн. акаунтів користувачів та отримали доступ до особистої інформації користувачів [1]. Також в США у 2017 році активізація попиту на кіберстрахування суттєво зросла після зламу хакерами системи бюро кредитних історій "Equifax", коли зловмисники заволоділи особистою та фінансовою інформацією понад 143 млн. американців, такою як номери водійських посвідчень, рахунки соціального страхування тощо [2].

Аналіз світового досвіду дає підстави констатувати, що кіберстрахування — особливий напрям страхування, який швидко та динамічно розвивається завдяки активному посиленню цифровізації міжнародної економіки і зростанню тенденцій, пов'язаних із занепокоєнням світової спільноти масштабуванням кіберризиків і одночасного орієнтованого на зниження збитків страхувальників і бенефіціарів, викликаних хакерськими кібератаками, у зв'язку із знищенням чи крадіжками конфіденційних даних, атаками кібервимагання, а також спрямований на мінімізацію їх втрат.

Оскільки кібератаки стають найвищою небезпекою, а ймовірність заподіяних ними збитків є високою, загальноприйнятим є визначення, що кіберстрахування, у першу чергу, спрямовано на організацію захисту від наслідків кіберризиків щодо майнових інтересів страхувальників, тобто як фізичних, так і юридичних осіб. У цьому контексті важливою складовою системи кіберстрахування виступають механізми оцінки втрат суб'єктів господарювання різних організаційно-правових форм внаслідок кібератак з метою пошуку оптимальних можливостей їхнього відшкодування та його перспективний розвиток. Цілком логічно, що динамічна зміна ландшафту кіберзагроз принципово не впливає на темпи та кількість кібератак, проте вірогідно очікується значне зростання попиту, ролі та значення кіберстрахування протягом наступного десятиліття. Тільки у період з 2023 по 2024 рік світовий ринок кіберстрахування виріс з 16,66 до $21 млрд. та за прогнозами авторитетних міжнародних експертів має досягти 120 млрд. доларів у 2032 році [3].

Таким чином, в сучасних умовах спостергіається перехід на якісно новий рівень розвитку світового ринку кіберстрахування. При цьому зберігається загрозлива тенденція збільшення кількості кіберзлочинів, поширення їх проявів, удосконалення засобів вчинення та зростання кількості диверсифікації кібератак. Системні негативні наслідки та збитки від втрат, пов'язані із викраденнням інформації, набирають шалених масштабів у світі. Також у світових вимірах досить потужним важелем для активізації світового страхового ринку став спалах пандемії COVID-19, зв'язку з чим відбулося прискорення переходу різноманітних операцій і процесів у режим онлайн, що, у свою чергу, спровокувало значне збільшення кількості кібератак, що одночасно призвело до підвищення розмірів фінансування та виділення асигнувань з метою мітігації (пом'якшення) кіберризиків. На цьому фоні, останнім часом спостерігаються високі темпи зростання ринку кіберстрахування. Це, у свою чергу, сприяє динамічному

розвитку цифрових технологій, зростанню попиту на послуги у сфері оцифровування, використанню різномантіних технологічних рішень та інтелектуальних досягнень в ІТ-сфері з метою пошуку шляхів посилення кіберзахисту та уникнення будь-яких збитків.

Загальновідомо, що комплексне страхування від кіберзагроз та кіберризиків дозволяє компенсувати можливі та передбачувані втрати від пошкодження, знищення або крадіжки корпоративних та клієнтських даних, а також подолати кризу в бізнес-діяльності, яка може виникнути внаслідок дії кіберризику. Останнім часом світовий ринок кіберстрахування стикається з унікальною комбінацією підвищених загроз і стабільного страхового середовища, яке підтримується потужними механізмами контролю кіберризиків, що створює основу для розвитку світового ринку кіберстрахування, переважно за рахунок інновацій. Драйвером зростання ринку кіберстрахування є динамічне збільшення кількості кібератак, у тому числі за допомогою поширення програм та вірусів-вимагачів. Ще однією важливою загрозою залишаються фішингові атаки через електронну пошту. При цьому страхове покриття у випадку заподіяних збитків внаслідок фішингу передбачається страховками нечасто, найчастіше в цій ситуації компанії доведеться розбиратися зі збитками самостійно. Таким чином, саме кіберстрахування дозволяє як державному сектору, так і приватним суб'єктам господарювання пом'якшити удар у разі вчинення кібератаки і хоча б частково фінансово захиститися від втрат. Також очікується, що в деяких країнах світу у таких галузях, як охорони здоров'я або фінансовий сектор, придбання страхових полісів від кіберризиків у перспективі стане обов'язковою умовою для усіх.

Виходячи із викладеного, доцільно вказати, що роль та значення кіберстрахування у питаннях мінімізації кіберризиків не можна недооцінювати. Світовий ринок кіберстрахування виходить на новий етап розвитку. В контексті сучасного світового геополітичного ландшафту, для України кіберстрахування набуває особливої актуальності через російську військову агресію, яка на перманентній основі провокує кіберзагрози та цілеспрямовано проводить кібератаки на інформаційні та інформаційно-комунікаційні системи державного сектору, урядових організацій та вітчизняних приватних компаній. Тому актуальним та своєчасним є розгляд кращих практик зарубіжного досвіду щодо формування організаційно-правових засад розвитку системи кіберстрахування та його запозичення для України в умовах правового режиму воєнного стану значно посилює тематику обраного напрямку цієї наукової статті.

Результати аналізу наукових публікацій. Кіберстрахування як самостійна галузь перебувала у фокусі уваги таких вітчизняних науковців-економістів: Н. Приказнюк та Л. Гуменюк [4], Р. Пікус та Ю. Бабенко [5], Г. Партин та А. Гребенюк [6], А. Шолойко [7]. Особливості кіберстрахування як дієвого засобу забезпечення господарського правопорядку в інформаційній сфері досліджували: Н. Пацурія та О. Заярний [8], І. Олійник [9], І. Ксьонжик, Н. Жовта, А. Павліна [10]. Проте жоден із вказаних фахівців не здійснював огляд кращих практик зарубіжного досвіду у сфері законодавчого забезпечення розвитку системи кіберстрахування як важливою складової посилення кібербезпеки.

Метою статті є узагальнення на базі аналізу основних сучасних тенденцій розвитку світового ринку кіберстрахування кращих світових практик у сфері кіберстрахування, зокрема висвітлення організаційно-правових засад й особливостей впровадження механізму оцінки втрат суб'єктів господарювання внаслідок кібератак для їхнього відшкодування в країнах із розвиненою цифровою економікою та високим рівнем кіберзагроз.

Виклад основного матеріалу. Положення Стратегії кібербезпеки України [11] та пункту 82 Плану реалізації Стратегії кібербезпеки України, уведеного в дію Указом Президента України від 01.02.2022 р. №37 [12], визначають, що в рамках стратегічного планування в Україні протягом другого півріччя 2025 року передбачається розробка організаційно-правових засад запровадження механізму оцінки втрат суб'єктів господарювання внаслідок кібератак з метою їх відшкодування та як елемент подальшого впровадження системи кіберстрахування, що набуває актуальності особливо в умовах правового режиму воєнного стану за наслідками російського вторгнення в Україну, яке триває вже четвертий рік поспіль. Розробка та запровадження системи страхування від кіберризиків є актуальним питанням в умовах зростання міжнародної та одночасно російської кіберзлочинності на фоні широкого впровадження та застосування технологій штучного інтелекту, IoT та цифрових сервісів.

В глобальних масштабах та вимірах система кіберстрахування спрямована на компенсацію втрат суб'єктам господарювання від кібератак, включаючи знищення, пошкодження, викрадення даних, зупинку бізнес-процесів, репутаційні збитки тощо. У світових масштабах кількість кіберзлочинів та їхня різноманітність постійно зростає, а диверсифікація кібератак стає дедалі ширшою. Наслідки від втрат та розкрадання інформації набувають форми збитків, які постійно зростають. Основні аспекти запровадження системи кіберстрахування включають збитковість, яка пов'язана із можливістю втрати даних, порушенням умов та правил конфіденційності, цілісності та доступності інформаційно-комунікаційних систем, а також фінансові втрати. Оцінка втрат охоплює як прямі збитки, які передбачають втрату даних, пошкодження обладнання, а також непрямі збитки у формі раптової зупинки виробництва, втраченої вигоди та витрат на відновлення систем (юридичні, технічні, репутаційні). При цьому, досить широко використовуються такі методи, як: ідентифікація активів, що включає визначення обсягів критичних інформаційних систем та даних, які можуть постраждати або зникнути; оцінка вразливостей, яка ґрунтується на аналізі ризиків, пов'язаних із кіберпростором за допомогою постійного моніторингу безпеки та аналізу повідомлень систем безпеки; кількісний аналіз визначення фінансових втрат, таких як різниця між страховою сумою та фактичним прибутком від успішної господарської діяльності; категоризація критичності, яка передбачає визначення рівнів кіберінцидентів (некритичний, низький, середній, високий) з метою здійснення оцінки їх впливу на державний сектор або бізнес-структри. Враховуючи викладене, доцільним є висвітлення кращих практик зарубіжного досвіду на прикладі таких провідних держав світу, як США, Канада та Австралія щодо створення та розвитку системи кіберстрахування, що у першу чергу передбачає успішне розроблення та впровадження національних механізмів оцінки втрат суб'єктів господарювання внаслідок кібератак.

США. Кіберстрахування набуває властивостей особливого засобу забезпечення господарського правопорядку в інформаційній сфері, нерозривно пов'язаного із забезпеченням кібербезпеки держави, суспільства, суб'єктів господарювання. Ця провідна держава світу залишається лідером світового ринку кіберстрахування, який за оцінками експертів має зрости до 2030 року на рівні 43 млрд. доларів [13]. Ринок кіберстрахування демонструє шалені перспективи, пов'язані із зростанням премій та капіталу страховиків й перестраховиків. Він постійно розширюється задля задоволення глобальних бізнес-потреб та в інтересах національної безпеки. У США кіберстрахування є однією з найрозвиненіших галузей страхування, що сприяє здійсненню реальних оцінок вразливостей за наслідками кібератак, визначенню та узагальненню потенційних фінансових втрат та збитків. У США кіберстрахування покриває витрати, пов'язані із

попередженням кібератак, відновленням даних та поточні юридичні витрати. Страхові компанії використовують власні методики оцінки ризиків, які включають наявні історичні дані про кібератаки, одночасно вимагаючи від суб'єктів господарювання провести попередні оцінки вразливостей з метою визначення розміру страхових премій. Наприклад, такі страхові компанії як AIG, Chubb, Lloyd's використовують стандартизовані методи оцінки кіберризиків, які базуються на міжнародних стандартах, таких як NIST та Cybersecurity Framework.

Американські страхові компанії виділяють такі елементи, які впливають на ставку кіберстрахування: 1) вартість застрахованого об'єкту. Так, наприклад компанія Lloyd's визначає страховий внесок у розмірі 2 тис. доларів США за умови вартості інформації, яка страхується, $1 млн; 2) наявність антивірусного захисту та інших засобів, що також впливає на розмір ставки страхового покриття за таким принципом: що більш відома та надійна система захисту, то менший розмір страхового тарифу; 3) кількість кібератак та посягань протягом останніх 5 років на страхувальника.

Одним із головних завдань IT-страхування, що неодноразово висвітлюється в релізах зарубіжних страхових компаній, стало створення сприятливих умов для розвитку мережевої торгівлі. Найбільш відому програму такого страхування під назвою Internet Asset and Income Protection Coverage розробила компанія Lloyd's. Важливою особливістю полісу страхування є можливість самостійного вибору постачальника засобів безпеки. Ця програма охоплює ризики втрати або пошкодження інформаційних активів внаслідок злому або збою в системах безпеки. При цьому під інформаційними активами розуміються, перш за все, списки клієнтів, номери кредитних карток, службова документація.

Також слід вказати, що в США немає єдиного федерального закону, який би регулював питання проведення оцінки втрат від кібератак, але діють, як вже зазначалося, галузеві стандарти NIST та Cybersecurity Framework, завдяки яким складаються методології для здійснення оцінки кіберризиків та втрат, зміст якої включає: прямі збитки у форматі витрат на відновлення даних, виплати за викуп у разі проведення успішних атак завдяки програм-вимагачів, судові витрати; непрямі збитки, які передбачають втрату доходу через зупинку бізнесу, репутаційні ризики. Проте окремі штати схвалили спеціалізоване законодавство у сфері безпеки даних і кіберризиків, яке впливає на американський ринок кіберстрахування. Так, у штаті Кентуккі з 1 січня 2023 року набув чинності закон, який встановлює вимоги до страхових компаній щодо захисту даних і управління кіберризиками, а у штаті Меріленд у 2022 році було ухвалено закон про кібербезпеку страхових компаній, який включає встановлені вимоги з метою проведення оцінки кіберризиків [14]. Нові закони встановлюють зобов'язання щодо умов та правил забезпечення безпеки даних для страхових компаній і загалом вимагають вжиття таких заходів:

- на постійній основі проводити оцінку кіберризиків;
- розробити, впровадити та підтримувати комплексну програму безпеки на основі оцінки ризиків і забезпечити, щоб ця програма включала: (1) визначені заходи безпеки даних, (2) вимоги до безпечних практик розробки та (3) план реагування на інциденти кібербезпеки;
- опановувати та вивчати нові загрози й вразливості, розробляти алгоритми заходів безпеки під час обміну інформацією;
- враховувати загрози кібербезпеки під час управління ризиками підприємства;
- забезпечити персонал навчанням з питань кібербезпеки;

- зобов’язати постачальників послуг впроваджувати та підтримувати відповідні заходи безпеки даних;
- регулярно звітувати про загальний стан програми інформаційної безпеки, дотримання страховою компанією законодавства про безпеку даних та питання, пов’язані з програмами інформаційної безпеки (такі як оцінка ризиків, рішення щодо управління ризиками та контролю, результати тестування кібербезпеки, події, пов'язані з кібербезпекою та рекомендації щодо будь-яких змін до програми інформаційної безпеки);
- щорічно подавати письмові сертифікати відповідності відповідному державному комісару зі страхування;
- здійснювати ведення обліку дотримання страховою компанією законодавства у сфері кібербезпеки;
- повідомляти про будь-які кіберінциденти державному уповноваженому зі страхування протягом трьох робочих днів після встановлення того чи іншого факту.

Також важлива роль відводиться Федеральній торговій комісії (FTC) та Федеральній агенції з питань кібербезпеки (CISA), які в рамках компетенції надають рекомендації щодо умов та правил здійснення кіберстрахування, зокрема в контексті покриття витрат за наслідками кібератак, відновлення даних. Відповідно до американського законодавства поняття “кіберризик” стосується абсолютно 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 до цього поняття входять ризики, пов’язані із накопиченням, зберіганням та використанням в електронному вигляді персональних даних.

Поліси кіберстрахування як страхові продукти для захисту бізнесу та фізичних осіб навіть в США не мають уніфікованих типових характеристик. У різних страхових компаніях вони істотно різняться між собою за умовами та лімітами відповідальності (покриттям). Загальноприйнятим є той факт, що застрахувати можна збитки, що ймовірно настануть в результаті таких кіберінцидентів: технічні збої, помилки програмування та відмова роботи IT-систем; за результатами нецільових атак – фішинг, sms-шахрайство, картинг, хактивізм; внаслідок цільових (таргетованих) атак – DDoS атаки, промислове шпигунство, криптолокерство (кіберздирництво); у випадку внутрішніх атак – викрадення конфіденційної інформації та відомостей, що становлять комерційну таємницю.

Основне страхове покриття може охоплювати: реагування на кіберінциденти, компенсацію витрат на послуги експертів безпосередньо задля припинення кібератак; відшкодування втраченого прибутку в результаті порушення IT-інфраструктури компанії, знищення та/ або крадіжки даних, тимчасової зупинки в роботі компанії після кібератаки; викупну суму, сплачену вимагачам за дешифрування заблокованої інформації; судові витрати, зокрема – задоволення позовних вимог від третіх осіб, які зазнали збитків в результаті інциденту. Додаткове страхове покриття може передбачати: компенсацію витрат на розслідування інциденту та проведення експертиз – технічної та юридичної для виявлення причин атаки та оцінки масштабів завданої шкоди; антикризовий PR та відновлення репутації після кібератаки; відновлення втрачених чи пошкоджених в результаті інциденту електронних даних; покриття штрафних санкцій, які накладено державою за недотримання компанією вимог законодавства щодо здачі звітності тощо.

Одночасно існують такі види кіберстрахування, як: страхування першої особи, яке покриває втрати компанії від кібератак (пошкодження даних, зупинка бізнесу); страхування третіх осіб з метою компенсування збитків, завданих клієнтам чи партнерам саме через кіберінцидент; перестрахування, яке використовується задля розподілу ризиків між страховими компаніями, що забезпечує фінансову стійкість страховиків; комплементарне страхування, що являє собою страхування від кіберризиків, яке поєднується із майновим страхуванням, наприклад, від вогневих ризиків чи стихійних лих тощо.

Механізм оцінки втрат суб'єктів господарювання внаслідок кібератак в США залежить від типу скоєної кібератаки, її масштабів та сектору економіки, який постраждав. Основні аспекти оцінки втрат базуються на комбінації стандартизованих методик, наявних даних компаній, страхових підходів та існуючої нормативно-правової бази. У переважній більшості випадків оцінка вразливостей в США здійснюється на підставі та за допомогою "RiskLens" — платформи для квантифікації кіберризиків, яка допомагає організаціям оцінювати вразливості, ймовірність атак і потенційні фінансові наслідки [15]. Ця платформа використовує стандарт FAIR (Factor Analysis of Information Risk) задля кількісного аналізу ризиків, що дозволяє приймати обґрунтовані рішення з метою пріоритизації заходів у сфері кібербезпеки. RiskLens ідентифікує критичні активи (наприклад, бази даних, мережеві ресурси) і пов'язані з ними вразливості, аналізує ймовірність експлуатації вразливостей на основі історичних даних, стану поточних засобів захисту та характеристик загрози (наприклад, зовнішній зловмисник чи інсайдер). При цьому використовуються дані, які перебувають у екосистемі безпеки та галузеві стандарти для оцінки слабких місць. RiskLens розраховує потенційні втрати (Probable Loss Magnitude, PLM) у фінансових термінах, зміст яких охоплює: прямі втрати, які включають витрати на реагування на кіберінцидент, штрафи, втрату даних; непрямі втрати: шкода репутації, втрата клієнтів, простої в роботі.

Так, наприклад, для розробки ймовірного загрозливого сценарію витоку даних, платформа RiskLens може оцінити втрати від $150,000 до $700,000 за один кіберінцидент, враховуючи прямі та непрямі витрати. Агрегація сценаріїв дозволяє оцінити річний очікуваний збиток (Annualized Loss Exposure, ALE), наприклад, у розмірі $75,000–$350,000 за умов систематичного проведення фішингових атак. При цьому, важливим аспектом залишається пріоритизація та аналіз ефективності засобів захисту. RiskLens пропонує порівняння різних варіантів реагування на кіберризики (Risk Treatment Analysis), оцінюючи, які засоби захисту (наприклад, DLP-інструменти) можуть забезпечити найбільше їхнє зниження ризику за найменших витрат. За результатами аналізу представляється звіт, який містить інформацію про ймовірність перевищення межі втрат.

Саме завдяки платформі RiskLens здійснюється швидка оцінка кіберризиків, проводиться детальний аналіз вразливостей, визначається порівняння варіантів реагування з метою зниження розміру та масштабів втрат. Використовуючи вказану методологію за підрахунками експертів США середня вартість кібератаки для компаній у цій державі в 2023 році коштувала близько $4,45 млн [16]. Таким чином, ринок кіберстрахування в США є одним із найрозвиненіших. Одночасно спостерігається розвиток законодавства з метою врегулювання цієї сфери та встановлено обов'язок страхових компаній проводити аудит кібербезпеки перед видачею будь-яких полісів страхування, який регулюється, у свою чергу, міжнародними стандартами кібербезпеки, такими як NIST та Cybersecurity Framework

Канада. Кіберстрахування в цій країні є відносно новою сферою, але швидко зростаючою галуззю, яка допомагає державі, бізнесу і фізичним особам захиститися від фінансових втрат, пов'язаних із кіберзлочинами, такими як: витік даних, кібератаки, кібершантаж, вимагання (ransomware) та порушення конфіденційності даних. Кіберстрахування, зазвичай, включає захист від витоку даних, що передбачає витрати на сповіщення клієнтів, відновлення даних і юридичні послуги; кібершантажу та вимагання (ransomware): компенсація за викуп або витрати на відновлення систем; перерви в бізнесі: відшкодування втраченого доходу через збої в роботі, спричинені кібератаками; юридична відповідальність: покриття судових витрат, штрафів і компенсацій через порушення конфіденційності даних; кризове управління: витрати на PR та відновлення репутації після інциденту. Деякі страхові поліси також пропонують послуги з кібербезпеки, такі як моніторинг, консультації, технічна підтримка після кіберінциденту. Вартість послуг із кіберстрахування залежить від: розміру компанії та її доходу; галузі (наприклад, фінансовий сектор або охорона здоров'я мають вищі ризики); наявного рівня кібербезпеки; обсягу страхового покриття.

Згідно з даними Канадського центру кібербезпеки (Canadian Cyber Security Centre), у 2023 році кількість кібератак на канадські компанії зросла на 25% порівняно з попередніми роками [17]. Одночасно діють жорсткі вимоги щодо захисту даних, які визначені спеціальним законом Канади — PIPEDA (Personal Information Protection and Electronic Documents Act), відповідно до положень якого компанії мають зобов'язання повідомляти про будь-які витоки даних і компенсувати збитки [18]. Так середня вартість збитків за результатами витоку даних для канадських компаній у 2023 році склала близько 4,8 млн канадських доларів.

Механізми оцінки втрат у Канаді базуються на рекомендаціях Канадського центру кібербезпеки (CCCS) [19], які розроблені спеціально для оцінки кіберризиків, та включають аналіз активів, вразливостей і фінансових втрат. Страхові компанії (наприклад, Intact Insurance) використовують моделі оцінки, що враховують витрати на відновлення, штрафи за порушення даних і втрати, які несе бізнес спільнота у певному випадку настання страхової події. Кіберстрахування покриває витрати на відновлення, юридичну підтримку та компенсаційні виплати клієнтам.

Останнім часом уряд Канади розглядає можливість посилення вимог до кібербезпеки, що у свою чергу, може вплинути на внесення змін до умов та правил проведення кіберстрахування, надає сприяння страховикам на фоні зростаючого попиту у зв'язку із збільшенням кількості кібератак. Загалом ринок кіберстрахування Канади представлений такими страховиками, як: страхова компанія "Chubb", яка пропонує комплексні поліси для бізнесів, включаючи захист від кібершантажу та перерв у діяльності; "AIG Canada", яка спеціалізується на кіберстрахуванні для великих корпорацій із фокусом на захисті даних; "Intact Insurance", яка пропонує страхові продукти для малого та середнього бізнесу, включаючи покриття витрат на відновлення після кібератак; "Beazley Canada" відома спеціалізованими полісами щодо кіберризиків, включаючи підтримку в управлінні кризами. Проте в Канаді кіберстрахування ще не покриває усі типи кіберризиків, наприклад, державно-спонсоровані атаки чи системні збої в інформаційних системах.

Кіберстрахування в Канаді має низку особливостей, зумовлених специфікою ринку, законодавством та зростаючим рівнем кіберзагроз, до яких відносяться:

- широке покриття ризиків, у зв'язку з чим поліси страхування, зазвичай, охоплюють: витоки даних, кібершантаж та вимагання (ransomware), перерви в бізнесі, юридичну відповідальність і витрати на кризове управління (PR). Деякі страховки навіть

включають проактивні послуги, як-от: моніторинг кіберзагроз чи консультації з кібербезпеки. Адже кібератаки є динамічними, що значно ускладнює точну оцінку втрат, особливо репутаційних;

- жорсткі вимоги законодавства: закон PIPEDA (Personal Information Protection and Electronic Documents Act) зобов'язує компанії повідомляти про будь-які витоки даних і удосконалювати механізм компенсування збитків, що робить кіберстрахування важливим інструментом дотримання встановлених нормативних вимог, при цьому запроваджені штрафи за порушення, які можуть становити значні суми покриваються страховими полісами;

- високий рівень кіберзагроз: відповідно до звітних матеріалів Канадського центру кібербезпеки у 2024 році кількість кібератак зросла на 25%, порівнюючи із 2023 роком, при цьому найпоширеніші — фішинг, ransomware і порушення даних. Найвищі ризики мають сектори охорони здоров'я, фінансів і роздрібної торгівлі, тому поліси для цих галузей значно дорожчі, а 43% кібератак припадає на малий бізнес. У свою чергу, через збільшення кількості кібератак страхові компанії підвищують премії та посилюють вимоги до клієнтів (наприклад, наявна обов'язковість використання на постійній основі сучасних антивірусів, вимога щодо регулярного оновлення ПЗ тощо).

Австралія. Кіберстрахування в Австралії є відносно новим, але швидкозростаючим сегментом страхового ринку, що відображає глобальні тенденції у сфері кібербезпеки. Зростання кіберзагроз, таких як витоки даних, атаки програм-вимагачів та порушення безпеки, сприяють підвищенню попиту на страхові продукти, які захищають державу, бізнес і приватних осіб від фінансових й репутаційних втрат. В сучасних умовах лише 50% великих підприємств та інших суб'єктів господарювання беруть участь в програмах кіберстрахування. У цій країні немає окремого закону про кіберстрахування, але відповідний ринок регулюється через загальне страхове законодавство та рекомендації Австралійського центру кібербезпеки (ACSC) [20]. Національне законодавство, наприклад Privacy Act 1988 [21], регулює питання захисту даних і формує попит на послуги у сфері кіберстрахування з метою попередження правопорушень, за наслідками вчинення яких відбувається покриття штрафів і компенсація поточних витрат на відновлення. З 2021 року урядом Австралії встановлена нормативна вимога, відповідно до якої страховики зобов'язані звітувати перед Австралійською адміністрацією регулювання індустрії фінансових послуг (APRA) [22] про усі укладенні кіберстрахові поліси, що сприяє розвитку страхового ринку та формує його прозорість.

Стандарти оцінки кіберризиків в Австралії базуються на низці національних і міжнародних рамок, спрямованих на виявлення, оцінку та управління кіберзагрозами. Основні аспекти включають: національні стандарти та рекомендації, зокрема Австралійського центру кібербезпеки (Australian Cyber Security Centre (ACSC), який розробив *Essential Eight* – набір із восьми ключових заходів для зниження кіберризиків, таких як використання багатофакторної автентифікації, регулярне оновлення програмного забезпечення та резервне копіювання даних; австралійський стандарт "ISO/IEC 27001", адаптований цією країною для здійснення управління інформаційною безпекою, який включає методології оцінки ризиків, такі як ідентифікація активів, аналіз загроз і планування заходів реагування; Information Security Manual (ISM) – основний документ, який визначає стандарти кібербезпеки для урядових організацій, проте досить широко використовується і в приватному секторі, охоплюючи оцінку ризиків, управління вразливостями та захист даних.

Через постійне зростання кібератак страхові премії в Австралії зростають, що може ускладнювати доступ до кіберстрахування для невеликих компаній. Одночасно ринок кіберстрахування потребує кваліфікованих андеррайтерів, здатних оцінювати кіберризики, що є потужним викликом для цієї галузі. Один із способів, які активно вживають страховики - багатофакторна аутентифікація, яка стає ключовою вимогою під час укладання договорів кіберстрахування поряд з вимогами щодо наявності захищених та зашифрованих резервних копій даних, управління привілейованим доступом до мереж та систем. Оскільки відбувається еволюція кіберризиків, яка передбачає поширення нових технологій, такі як штучний інтелект і хмарні сервіси, що створюють нові виклики для страховиків, які змушені адаптувати свої страхові продукти до нових реалій.

На відміну від США та Канади, де кіберстрахування є більш розвиненим, австралійський страховий ринок перебуває у стадії свого динамічного розвитку. Проте Австралія активно переймає міжнародний досвід, зокрема від США та Канади, адаптуючи страхові продукти у відповідності до місцевих регуляторних вимог. Сучасні тенденції кіберстрахування в Австралії відображають глобальне зростання кіберзагроз і локальні особливості регулювання та економіки, до яких відносяться: очікуване зростання попиту на кіберстрахування, що пов’язано із значним збільшенням кібератак, таких як: програм-вимагачів, фішингу і витоку даних; зростання страхових премій через зростання частоти та серйозності кібератак, останнім часом страхові премії зросли на 20–30% у 2023–2024 роках (згідно з даними Insurance Council of Australia); страховики посилюють вимоги до клієнтів, наприклад, обов’язкове впровадження двофакторної автентифікації чи регулярних аудитів безпеки з метою зменшення ризиків; впровадження розширеного страхового покриття, зокрема комплексних полісів, що включає покриття витрат на реагування на кіберінциденти (юридичні, PR, відновлення даних), штрафи за порушення законодавства і навіть втрати через перерви в бізнесі.

Також слід вказати, що спостерігається тенденція підвищення попиту на кіберстрахування, оскільки воно стає важливою частиною стратегії управління ризиками, що стимулює розвиток національного страхового ринку.

Висновки. В сучасних умовах існують різні технологічні платформи, захисні системи, сучасне програмне забезпечення та інші інструменти, які розробники намагаються поєднати із кіберстрахуванням, щоб зменшити або нівелювати потенційні кіберзагрози та кіберризики. Історично склалося, що ринок кіберстрахування вважався “м’яким”, що надавало можливість компаніям та іншим суб’єктам господарювання отримувати страхове покриття за відносно низькими тарифами. Проте зростання кіберризиків та експоненціальне зростання кібератак, широке поширення програм-вимагачів призвело до необхідності уточнення умов, порядку та особливостей здійснення кіберстрахування, адаптації страхового ринку під них. У разі виникнення будь-якого кіберінцідента страховик (страхова компанія) компенсує завдані збитки в результаті претензій третіх осіб і претензій, пов’язаних із порушенням функціонування безпеки системи. Також страхове покриття включає витрати на технічну експертизу і відновлення даних і систем, компенсацію судових витрат і витрат на інформування уповноважених суб’єктів. Таким чином, страхування кіберризиків – це можливість суттєво знизити ризики негативних наслідків у сфері кібербезпеки та мінімізувати наслідки від кіберінцидентів, які вже сталися. Сучасний сервіс у сфері кіберстрахування допомагає не тільки захистити інформацію, але і скоротити можливі витрати, зберегти ділову репутацію. У той самий час до типових кіберризиків, окрім кібератак

відносяться: витік даних, DDoS-атаки, фішинг, кібершантаж та вимагання, зловмисне ПЗ, інсайдерські кіберзагрози тощо.

У страхуванні кіберризиків надзвичайно важливим аспектом є методологія оцінки кіберзагроз. Завдання такої оцінки полягають в тому, щоб: виявити загрози, які спрямовані на активи; визначити та спрогнозувати якомога більш точно наслідки реалізації кіберризиків; виявити вразливі місця для кібер-загроз в інформаційній безпеці організації; проаналізувати наявні методи контролю ризиків та визначити той, який дозволить мінімізувати виявлені загрози; оцінити ймовірність виникнення та реалізації кіберризиків.

На підставі проведеного аналізу цілком логічно виділити 5 основних тенденцій подальшого розвитку ринку кіберстрахування: 1) збільшення попиту на відповідні страхові продукти у зв'язку із поширенням кількості кіберінцидентів, оскільки кіберстрахування може виступати у якості інструменту мінімізації фінансових втрат; 2) посилення умов страхування та розширення кількості виключень із страхового покриття; 3) зростання середнього розміру страхових премій за рахунок збільшення страхових тарифів, що пов'язано з тим, що дисбаланс попиту та пропозицій на глобальному ринку кіберстрахування призвів до стрімкого зростання ставок страхових внесків; 4) безпосередній вплив контролю з боку страхувальників та зростання премій, спрямованих на страхове покриття; 5) збільшення рівня утримання кіберризиків: у той час як страховики вимагають виконання стандартних умов за договорами кіберстрахування, деякі страхувальники погоджуються на більш високі відсоткові ставки з метою звести до мінімуму розмір нарахованих страхових премій.

У проаналізованих державах (США, Канада, Австралія) ринок кіберстрахування демонструє перспективи, які характеризуються зростанням премій та капіталу страховиків й перестраховиків. Предметом кіберстрахування є інформація, інформаційно-телекомунікаційні системи, технології, бази даних, репутаційні ризики, які є немайновими об'єктами права власності, а також витрати, пов'язані з їхньою оцінкою, як немайнових об'єктів інтелектуальної власності.

Механізми оцінки втрат від кібератак та їх відшкодування найбільш розвинені в США та Канаді, трохи менше в Австралії. Ці провідні країни світу мають розвинений ринок кіберстрахування, активно впроваджують стандарти оцінки ризиків (наприклад, NIST, ISO/IEC 27001) і забезпечують розвиток ринку кіберстрахування через регуляторні акти та спеціальні програми. Законодавство, яке безпосередньо регламентує порядок та умови здійснення кіберстрахування, є відносно новим і не в усіх країнах існують нормативно-правові акти навіть на рівні федерального законодавства, які присвячені питанням кіберстрахування. У зв'язку з цим кіберстрахування переважно регулюється загальним страховим законодавством, національними законами про кібербезпеку або захисту даних.

В Україні окреслені механізми перебувають у стадії свого логічного розвитку, з акцентом на вдосконалення вітчизняного законодавства та подальшу співпрацю з міжнародними партнерами з метою адаптації кращих практик зарубіжного досвіду у сфері кіберстрахування. Також спостерігається низька обізнаність бізнесу про умови та порядок здійснення кіберстрахування та його переваги, особливо в умовах правового режиму воєнного стану; існуюча захмарна вартість оцінки ризиків та страхових продуктів через складність прогнозування спектру кіберзагроз, обмежена кількість страховиків (страхових компаній), які пропонують послуги у сфері кіберстрахування, недостатній досвід актуарних розрахунків для кіберризиків тощо. У тому числі, недостатня нормативно-правова база, яке регламентує сферу кіберстрахування. Так,

Закон України “Про страхування” 2021 року [23] регламентує питання страхування фінансових ризиків, але не деталізує поняття та умови щодо кіберризиків. На жаль, в нормах чинного законодавства все ще відсутнє визначення поняття “кіберризик”. На сьогоднішній день, в юридичній літературі також не було сформовано єдиного підходу до класифікації кіберризиків. Оскільки кіберстрахування в України перебуває на початковому етапі свого становлення, під час розроблення методологічних підходів щодо його подальшого розвитку, доцільно використовувати сучасні надбання та позитивний досвід провідних у цій галузі країн світу (США. Канади, Австралії), який переконливо засвідчує позитивні аспекти диверсифікації спектру послуг у сфері кіберстрахування, використання полісів страхування як потужний запобіжний захід від наслідків кіберзлочинів, хакерських кібератак та надійний механізм компенсації та покриття збитків.

Розвитку вітчизняного ринку кіберстрахування передбачає, у першу чергу, схвалення відповідних законодавчих актів у сфері забезпечення кібербезпеки на рівні держави, внесення змін до закону України “Про страхування” з метою чіткого визначення сутності, змісту та особливостей здійснення кіберстрахування. Діапазон кіберзлочинів достатньо широкий і коливається від отримання доступу до інформаційних баз даних, об’єктів інтелектуальної власності, втручання в діяльність комп’ютерних систем до отримання фінансової вигоди. З одного боку, необхідність кіберстрахування виникає у зв’язку із потужним розвитком інформаційних технологій та інноваційних продуктів у різних сферах економічної діяльності, що викликає появу різноманітних кіберризиків, з іншого – кіберзлочини переважно відбуваються шляхом крадіжки інновацій або новітніх технологій. З огляду на це можна зробити висновок, що в основі розвитку кіберстрахування і зростання кіберзлочинів, особливо у фінансовій сфері, є технології і питання тільки в тому, хто скоріше ними скористується і з якою метою. У цьому аспекті при розвитку системи страхування кіберризиків необхідно практично повністю виключити вплив людського фактору на розкриття інформації про страхувальників, створивши відповідні служби інформаційної безпеки і встановивши обмежений доступ працівників до їхніх баз даних з персональною відповідальністю виконавців. Також на законодавчому рівні вбачається доцільним посилити кримінальну відповідальність, зокрема і працівників страхових компаній, за розкриття або несанкціоноване поширення інформаційних баз даних клієнтів, розкриття конфіденційної інформації. До основних шляхів державної підтримки у сфері кіберстрахування слід віднести: розробку сучасних моделей ризику на основі зібраних даних; структурування премій страховими компаніями з метою стимулювання поведінки, що знижує ризики, і впровадження кращих світових практик у свою діяльність; стимулювання або впровадження обов’язкового кіберстрахування для державних та фінансових установ (купівлю полісів кіберстрахування), які відповідають мінімальним стандартам тощо.

Запровадження окреслених підходів у поєднанні із забезпеченням прозорості та розширенням меж взаємодії і співробітництва страхових компаній сприятиме диверсифікації страхових послуг і розвитку вітчизняного кіберстрахування. Саме тому запровадження системи страхування від кіберризиків в Україні потребує комплексного підходу, включаючи вдосконалення законодавства, розробку методик оцінки втрат, підвищення обізнаності бізнесу та співпрацю з державними органами. Механізм оцінки втрат має базуватися на аналізі критичності кіберінцидентів, кількісному підході до збитків та врахуванні прямих і непрямих втрат. Відшкодування через страхування першої та третьої особи, а також перестрахування, може забезпечити фінансову

стійкість суб'єктів господарювання в умовах кіберзагроз, особливо в умовах правового режиму воєнного стану.

Використана література

1. Yahoo Says Hackers Stole Data on 500 Million Users in 2014. URL: https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html
2. Equifax Says Cyberattack May Have Affected 143 Million in the U.S. URL: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html
3. Cyber Insurance Market Outlook for 2024-2034: Coverage & Capital Managing. URL: https://beinsure.com/cyber-insurance-market-outlook
4. Приказнюк Н., Гуменюк Л. Доржня карта впровадження кібер-страхування в Україні. *Innovation and Sustainability*, 2021. №1. С. 64-72. https://doi.org/10.31649/ins.2021.1.64.72
5. Пікус Р.В., Бабенко Ю.Л. Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава.* 2022. №2. С. 134–140.
6. Партин Г.О., Гребенюк А.В. Перспективи розвитку кібер-страхування в Україні, та перешкоди його становлення. *Модернізація економіки у контексті інноваційного розвитку: напрями та пріоритети*: матеріали міжнар. наук.- практ. конф. (Дніпро, 17 листопада 2018 р.). Дніпро, 2018. С. 32–33.
7. Шолойко А.В. Актуалізація кіберстрахування в умовах цифровізації економіки. *Науковий вісник Одеського національного економічного університету*. 2023. №9. С. 98-106.
8. Пацурія Н., Заярний О. Кіберстрахування як засіб забезпечення господарського правопорядку в інформаційній сфері: поняття, механізм та умови реалізації. *Право України.* 2021. №7. С. 13-30.
9. Олійник І.О. Загальні проблеми захисту кібернетичного простору України. *Актуальні проблеми управління інформаційною безпекою держави*: зб. тез наук. доп. наук.-практ. конф. (Київ, 26 березня 2021 р.). Київ: НА СБУ, 2021. С. 294–296.
10. Ксьонжик І., Жовта Н., Павліна А. Страхування ризиків кібербезпеки діяльності суб'єктів господарювання в сучасному інформаційному просторі. *Економіка та суспільство.* 2021. Вип. 34. DOI: https://doi.org/10.32782/2524-0072/2021-34-90
11. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
12. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України від 01 лютого 2022 року № 37/2022. URL: https://www.president.gov.ua/documents/372022-41289.
13. Cyber insurance entering a new phase of development as non-US territories set to capture 54% of growth up to 2030, according to new Howden report. URL: https://www.howdengroup.com/is-en/news/cyber-insurance-entering-a-new-phase-of-development-as-non-us-territories-set-to-capture-54-of-growth-up-to-2030
14. Two States Enact Insurance Data Security Laws. URL: https://www.hunton.com/privacy-and-information-security-law/two-states-enact-insurance-data-security-laws
15. RiskLens. URL: https://www.risklens.com/resource-center/topic/news
16. What is the Cost of a Data Breach in 2023? URL: https://www.upguard.com/blog/cost-of-data-breach
17. National Cyber Threat Assessment 2025-2026. URL: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026.

18. Personal Information Protection and Electronic Documents Act. URL: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/.

19. Canadian Centre for Cyber Security. URL: https://www.cyber.gc.ca/en.

20. Australian Cyber Security Centre (ACSC). URL: https://www.cyber.gov.au/.

21. Privacy Act 1988. URL: https://www.legislation.gov.au/C2004A03712/2019-08-13/text

22. Australian Prudential Regulation Authority. URL: https://www.apra.gov.au.

23. Про страхування: Закону України від 18 листопада 2021 року № 1909-IX. URL: https://zakon.rada.gov.ua/laws/show/1909-20#n2320.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~