ГОСПОДАРСЬКЕ ПРАВО, ГОСПОДАРСЬКО-ПРОЦЕСУАЛЬНЕ ПРАВО

УДК 004.056:339.138
DOI https://doi.org/10.32782/TNU-2707-0581/2024.4/03

Волинець В.В.
Київський університет туризму економіки і права

РОЛЬ КІБЕРСТРАХУВАННЯ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ДАНИХ В ОНЛАЙН ТОРГІВЛІ

Стаття присвячена питанню ролі кіберстрахування у забезпеченні безпеки даних в онлайн торгівлі. Встановлено, що розвиток інноваційних технологій і зростання популярності онлайн торгівлі підсилило необхідність у захисті безпеки даних суб'єктів бізнесу та споживачів. Шахрайські схеми з кожною кібератакою завдають чималих збитків сектору онлайн торгівлі, оскільки відразу досить важко відслідкувати несанкціонований вплив злочинців. Зважаючи на це, особливо актуальним залишається питання захисту персональної і фінансової інформації, яка міститься або передається через цифрові платформи.

В статті здійснено огляд того, що останнім часом почастішали випадки неправомірного втручання у безпеку даних, оскільки злочинні наміри в кіберпросторі постійно еволюціонують, удосконалюються і провокують нові проблеми, пов'язані із заволодінням конфіденційною та фінансовою інформацією. Зважаючи на це, часті випадки порушення безпеки даних несуть в собі загрозу в настанні серйозних фінансових витрат, зниженні репутації компаній, провокації негативного впливу на довіру споживачів.

З'ясовано, що оскільки сектор онлайн торгівлі сам по собі містить чимало ризиків за принципом «кіт в мішку», важливо продовжувати працювати над удосконаленням захисту безпеки даних від кібератак, підсилюючи таким чином довіру споживачів. В рамках дослідження визначено, що одним із таких механізмів захисту є кіберстрахування – спосіб захисту від атак, пов'язаних з кіберзлочинами. Кіберстрахування є доцільним інструментом для онлайн-бізнесу, оскільки забезпечує фінансовий захист від витрат, пов'язаних з кіберінцидентами, та допомагає відновитися після атаки. Окрім того він забезпечує не лише компенсацію збитків, але й доступ до спеціалізованих послуг з реагування на інциденти, пов'язані з кібербезпекою.

У висновках підсумовано, що забезпечення безпеки даних в онлайн торгівлі є надзвичайно важливим питанням, оскільки дозволяє оцінити ефективність кіберстрахування за мінімізації ризиків та забезпеченні надійного захисту інформації. Зважаючи на це, швидка адаптація страхових продуктів до нових кіберзагроз, зміни в регуляторних вимогах є важливим питанням, що потребує детального опрацювання. Отже, дослідження ролі кіберстрахування в забезпеченні безпеки даних матиме на меті покращити існуючі механізми захисту від кібератак і виробити нові стратегії задля ефективного подолання кіберзагроз в онлайн торгівлі.

Ключові слова: *онлайн торгівля, кібератаки, кібербезпека, фінансові збитки, конфіденційна інформація, репутація.*

Постановка проблеми. Цифрові технології вплинули на розвиток онлайн-торгівлі. Все більше з'являється сайтів, які пропонують якісні товари, швидке оформлення замовлень і зручну оплату. Цей процес змушує заощаджувати час і кошти. Однак із зростанням обсягів онлайн торгівлі і розвитку цифрових технологій виникають нові виклики, пов'язані із забезпеченням безпеки даних в мережі Інтернет. Кіберзлочинці з кожним разом шукають все нові і нові методи ошукати громадян чи компанії, зібрати необхідну інформацію і завдати якомога масштабніших збитків.

Зважаючи на систематичність і обсяг завданої шкоди, останнім часов дедалі більшої ваги набуває

питання кіберстрахування, як важливий інструмент захисту від можливих збитків. В порівнянні зі звичайним цивільним страхуванням, кіберстрахування окрім відшкодування збитків надає низку послуг, пов'язаних із вирішенням питань у сфері кіберзахисту.

Важливо наголосити, що ефективність кіберстрахування у забезпеченні безпеки даних в онлайн торгівлі ще недостатньо досліджена, а відтак, впроваджена в реалізацію. Тому, дослідження ролі кіберстрахування в контексті безпеки даних є важливим питанням, яке сприяє формуванню ефективних стратегій захисту інформації в умовах постійних нових атак і загроз.

Аналіз останніх досліджень і публікацій. Теоретичні та прикладні аспекти дослідження ролі кіберстрахування у забезпеченні безпеки даних в онлайн-торгівлі розглядаються у працях таких вчених, як В. П. Ільчук, О. М. Парубець, Д. О. Сугоняко [2], Н. В. Приказюк та Л. С. Гуменюк [3], Р. В. Пікус та Ю. Л. Бабенко [4], Н. Г. Нагайчук, Н. М. третяк та О. Ткаленко [5]. Однак незважаючи на розробленість даної теми, питаня залишається не вирішеним і потребує доопрацювання.

Постановка завдання. Метою статті є визначення ролі кіберстрахування у забезпеченні безпеки даних в онлайн-торгівлі.

Виклад основного матеріалу. Інтернет-торгівля є зручним механізмом для прискореного ведення бізнесу, оскільки має чималий спектр можливостей для швидкого задоволення власних потреб у сфері купівлі товарів онлайн. Широкий асортимент товарів і послуг, економія часу, детальне ознайомлення з характеристиками товару сприяє розвитку цієї сфери, підсилюючи її практичність. Попри позитивні причини скористатися онлайн-торгівлею, деяких споживачів лякає думка про те, що оплачуючи товари в мережі Інтернет, їх конфіденційними даними можуть заволодіти треті особи, і, як результат, завдати чималих збитків.

Кібератаки можуть завдати значної шкоди репутації компанії, призвести до втрати даних, фінансових збитків і спричинити перебої в роботі. Згідно з даними дослідження Identity Theft Resource Center 2022 Data Breach Report, у 2023 році хакери здійснили 2365 атак, жертвами яких стали 343 338 964 особи. Середня світова вартість витоку даних у 2023 році становила $4,45 млн, що на 15% більше порівняно з показниками трирічної давнини [1].

З цією метою все частіше компанії одна за одною впроваджують у свою діяльність кіберстрахування. Основне завдання кіберстрахування полягає в захисті від масштабних хакерських атак. Цей вид страхування формує фінансовий механізм для відновлення після значних збитків, допомагаючи підприємствам відновити нормальну діяльність, зберегти стабільність, платоспроможність та знизити втрати, спричинені перервами у виробництві. На думку групи дослідників В. П. Ільчук, О. М. Парубець та Д. О. Сугоняко, особливістю кіберстрахування є те, що його попит зазвичай формується внаслідок виникнення кіберзагроз або після кібератак. Пропозиція на ринку кіберстрахування залежить від специфічних умов, які супроводжують кожен кіберінцидент, зокрема характеру загрози, вартості страхових послуг, фінансових можливостей страховиків, а також можливості відшкодування збитків після настання страхових випадків. На формування пропозиції впливають можливості укладення страхових договорів через Інтернет (онлайн-поліси). Ринок кіберстрахування відзначається консервативною моделлю, що має на меті завоювати довіру клієнтів у сфері онлайн-бізнесу [2].

Поліс кіберстрахування є багатокомпонентним продуктом, оскільки містить у собі страхування майна, відповідальності та фінансових ризиків. Основні страхові випадки охоплюють збитки, що виникають в процесі порушення функціонування комп'ютерної мережі або її систем безпеки страхувальника через втручання третіх осіб. Загалом кіберстрахування поділяється на два види: страхування першої особи та третьої особи, що відповідає захисту організації та даних її клієнтів відповідно. В Україні кіберстрахування є новим і малопоширеним явищем. Незважаючи на те, що керівники підприємств усвідомлюють необхідність його впровадження, відсутність достатніх фінансових резервів деяких компаній не дають цього зробити. Попри низький попит, в Україні дві страхові компанії пропонують страхові поліси, які частково покривають кіберризики. Наприклад, страхова компанія «UPSK» надає повний комплекс покриття ризиків, а страхова компанія «АСКА» пропонує індивідуальний підхід з можливістю вибору необхідних ризиків залежно від специфіки господарської діяльності [3].

Згідно з дослідженнями Р. В. Пікус та Ю. Л. Бабенко, головним об'єктом кіберстрахування є кіберризик. Поняття «кіберризики» відзначається наступними ознаками, до яких відносять:

– будь-які ризики, що виникають в результаті використання та передачі електронних даних,

зокрема за допомогою Інтернету та телекомунікаційних мереж;

– фізичні збитки, спричинені кібератаками;

– шахрайство, яке виникає внаслідок неправомірного використання даних;

– неправомірний доступ до конфіденційної електронної інформації, що стосується фізичних осіб, компаній або уряду.

Загалом кіберризик – це ймовірність виникнення певних страхових подій, що впливають на функціонування ІТ-систем та кібербезпеку організації внаслідок стороннього втручання через цифрові та інші електронні технології, що призводить до завдання збитків і руйнування даних [4, с. 135].

Досліджуючи питання кіберстрахування варто звернути увагу на сферу застосування сучасних технологій, за яких застосовується поняття «страхування кібервідповідальності», «страхування кібербезпеки» та «страхування кіберризиків». На думку Н. Нагайчука, кіберстрахування – це страховий продукт, що захищає компанію від ризиків, пов'язаних з використанням Інтернету, та ризиків, пов'язаних з інформаційними технологіями, ІТ-інфраструктурою та діяльністю підприємства у кіберпросторі [5, с. 100].

У сучасному інформаційному просторі «кіберстрахування» визначається як страховий продукт, що передає певні фінансові ризики третій особі – страховику кіберпослуг. Цей процес допомагає суб'єктам господарювання зменшити вплив ризику шляхом компенсації витрат, пов'язаних із руйнівними наслідками кіберзлочинів, та забезпечення захисту від збитків, що виникають чи можуть виникнути внаслідок порушення безпеки та конфіденційності, спричиненої кібератакою.

Кіберстрахування покриває збитки, пов'язані з пошкодженням або втратою інформації з ІТ-систем та мереж. Окрім того кіберстрахування надає допомогу суб'єктам комерційної діяльності, сприяючи послідовному і ефективному вирішенню проблем, спричинених кібератакою, захистом репутації, а також примусовому вирішенню спорів.

Нині існує два підходи щодо вирішення кіберризиків шляхом кіберстрахування, зокрема:

– страхування кібервідповідальності;

– майнове страхування кібератак.

Стахування кібервідповідальності полягає у стахуванні відповідальності за ризики, які несе кібератака на сферу онлайн торгівлі. Тобто суб'єкти комерційної діяльності, здійснюючи онлайн торгівлю, вже на підсвідомому рівні прагнуть захистити свої дані та дані клієнтів від неправомірного впливу, спричиненого кібератакою. Разом з цим покриття кібервідповідальності третьої особи (страхової компанії) містить витрати, які комерційна компанія безпосередньо зазнає внаслідок порушень. До компетенції страхових компанії, що займаються кіберстрахуванням входить інформування клієнтів про хакерські атаки, розгляд претензій від фізичних та юридичних осіб, які зазнали збитків внаслідок дій кіберзлочинців.

Другий підхід до формування покриття кіберстрахування зосереджений на видах кібератак та кіберінцидентів, які відбуваються з компаніями та об'єктами, на які вони безпосередньо впливають. Зважаючи на цей підхід особливу увагу приділяють аналізу ризиків, пов'язаних із різними типами кіберзагроз, зокрема загрозливими програми, фішингом, DDoS-атаками, витоком даних, тощо. Страхові поліси кіберстаховиків має враховувати можливість пошкодження або втрати важливих даних, значним чином впливаючи на операційну діяльність компанії.

Досліджуючи сучасну практику угод страхування провідних європейських, американських та українських компаній, доцільно зосередити увагу на кількох основних напрямках подальшого розвитку кіберстрахування, зокрема й онлайн торгівлю. Серед головних напрямків кіберстрахування важливо створити страхові поліси, які б покривали збитки, пов'язані з відновленням даних, відшкодовували витрати на юридичні послуги, а також передбачали компенсацією втрат через простої в роботі систем і обмеження діяльності онлайн-платформ. Наразі процес із відшкодування збитків, викликаних простоєм через кібератаки, працює неналежним чином. Більшість компаній на свій страх і ризик намагаються якнайшвидше всіма зусиллями відновити роботу компаній, зазнавши при цьому мінімальних збитків.

Зважаючи на це, головною умовою майнового кіберстрахування насамперед має стати покриття витрат, повязаних із залученням експертів з кібербезпеки для аналізу та усунення наслідків інциденту, встановлення шкоди і програмою відновлення втраченої інформації. Важливою частиною страхових полісів є забезпечення інформаційної підтримки клієнтів та партнерів, постраждалих від кіберінцидентів.

Майнове кіберстрахування передбачає комплексний підхід до захисту активів компанії, враховуючи не тільки прямі збитки, але й непрямі втрати, пов'язані з репутаційними ризиками. Вказаний підхід дозволяє зменшити фінансовий

вплив кіберзлочинів на діяльність підприємства та забезпечити його стабільність в найближчому майбутньому.

Кіберстрахування, яке ґрунтується на різних видах кібератак, включає оцінку ймовірних та потенційних наслідків кожного типу загроз. Це дозволяє компаніям краще зрозуміти свої вразливі місця та вжити необхідних заходів для їх мінімізації. Перспективні страхові поліси з майнового кіберстрахування охоплюють різноманітні аспекти діяльності компаній, від забезпечення безперервності бізнес-процесів до захисту інтелектуальної власності. Вони спрямовані на надання всеосяжного захисту та підтримки у випадку кіберінциденту. Вивчення сучасних процесів кіберстрахування визначило важливість адаптації страхових продуктів до специфіки кожної окремої компанії. Це дозволяє створити більш ефективні та релевантні поліси, що відповідають конкретним потребам бізнесу.

Сучасний стан розвитку страхового ринку України дозволяє визначити кілька факторів, які перешкоджають впровадженню та розвитку страхування кіберризиків. По-перше, відсутня довіра до стандартних страхових послуг, і такий інноваційний продукт, як кіберстрахування, ще не знайшов достатнього споживчого кола. По-друге, не існує конкретних видів кіберстрахування; натомість, доступні лише комплексні продукти, спрямовані на страхування різних об'єктів від одного типу небезпеки, наприклад, кібератак.

Особливістю страхування кіберризиків є те, що попит на нього формується в процесі виникнення кібератак або потенційних кіберзагроз. Пропозиція на ринку страхових послуг залежить від специфіки кіберінцидентів у страхувальників, вартості полісу, прибутковості страховиків та їхньої здатності оформляти онлайн-поліси. Ринок кіберстрахування будується на консервативній моделі, де страховикам необхідно удосконалювати пропозиції в сфері інформаційної безпеки, будувати репутацію серед страхувальників та аналізувати новинки на кіберринку для надання актуальних послуг.

Кіберстрахування в онлайн сфері має підкріплюватися вдосконаленої нормативно-правовою базою. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як захищеність життєво-важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Цей процес передбачає забезпечення сталого розвитку інформаційного суспільства та цифрового комунікативного середовища, а також своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі [6].

Станом на 2024 рік нормативно-правове забезпечення інноваційного сегменту страхового ринку – кіберстрахування, знаходиться на стадії формування як в Україні, так і в усьому світі. Європейська Директива щодо мережевої та інформаційної безпеки ЄС (NIS) є першим законодавчим актом про кібербезпеку, прийнятим у всіх країнах ЄС. Основною метою Директиви NIS є підвищення кібербезпеки в Євросоюзі шляхом встановлення загального рівня безпеки мережевих та інформаційних систем. Ця директива позитивно впливає на розвиток ринку кіберстрахування в Україні, особливо для інтернет-ринків, пошукових систем, та хмарних обчислень, і може стати основою для відповідного законодавства в країні.

Українські страхові компанії все ще не мають достатніх ресурсів для розробки власного підходу до оцінки кіберризиків, а потенційні клієнти поки що не проявляють значного інтересу до цього відносно нового виду страхування. Проте, поточні оцінки і прогнози вказують на те, що попит на кіберстрахування щорічно зростає. Наразі, страхових компаній, які б пропонували якісні кіберстрахові продукти з високими відсотками на належним покриттям, адекватними страховими преміями, можуть зайняти чільну роль в онлайн бізнесі.

Прогнозується, що кіберстрахування з кожним роком лише зростатиме, а разом з цим і зростатиме сфера кіберзагроз. Після рекордного зростання в 2023 році, глобальний ринок кіберстрахування значно розширився. Подібні очікування прогнозуються і на 2024 рік. Таке зростання пояснюється активним впровадженням кіберстрахування у різні бізнес-сектори. Крім того, з кожним роком дедалі активніше розвиваються галузі, які впроваджують кіберстрахування, сприяючи розвитку цій сфері захисту.

Ринок кіберстрахування продовжує приваблювати як існуючі компанії, так і нових інвесторів, завдяки значним можливостям для зростання та отримання прибутку. Компанії все активніше застосовують сфері кіберстрахування у своїй діяльності, оскільки це ще один важіль безпеки в цифровому онлайн бізнесі [7].

Отже, зважаючи на дані, опрацьовані в процесі дослідження, важливо наголосити, що попит кіберстрахування невпинно зростатиме й надалі,

зокрема і в сфері інтернет-торгівлі. Це, головним чином визначається специфікою інтернет бізнесу та його вразливістю до різних типів кібератак. Для підвищення захисту онлайн-торгівлі необхідно працювати над обізнаністю працівників про можливі кіберризики, забезпечуючи таким чином конфіденційність корпоративної інформації щодо захисту даних. Важливо також сприяти підвищення ефективності роботи інформаційних систем, мінімізуючи взаємодію з зовнішніми джерелами. Впровадження кіберстрахування сприятиме фінансовій захищеності та підвищенню загального рівня безпеки сектору онлайн-торгівлі.

Такі заходи повинні сприяти захисту від кібератак в сфері онлайн-торгівлі. Важливо, щоб бізнес і ІТ компанії працювали разом над питаннями, які виникають у сфері кіберзахисту та кіберстрахування. Від цих важливих кроків залежатиме стабільність і надійність електронних операцій, зменшення фінансових втрат від потенційних кібератак, збереження репутації компаній на ринку. Спільна робота дозволить вчасно виявляти вразливі сторони та вжити заходів для їх усунення. Крім того, впровадження ефективних програм навчання для співробітників сприятиме підвищенню їх обізнаності щодо сучасних кіберзагроз та методів їх запобігання. Належна інтеграція кіберстрахування забезпечить додатковий рівень захисту, компенсуючи збитки у разі кібератак.

Систематичне оновлення програмного забезпечення та систем безпеки, а також проведення аудиту ІТ-інфраструктури допоможе підтримати високий рівень захищеності безпеки даних онлайн. Тісна співпраця між бізнесом і ІТ компаніями сприятиме розвитку інноваційних рішень для кібербезпеки, і тим самим, забезпечить не лише захист від кібератак, але й підвищить довіру клієнтів до онлайн-бізнесу. Таким чином, комплексний підхід у сфері кіберстрахування стане запорукою стабільного та безпечного функціонування онлайн-бізнесу в сучасних умовах.

Висновки. В процесі проведеного дослідження встановлено, що кіберстрахування відіграє значну роль у забезпеченні безпеки даних в онлайн-торгівлі. Кіберстрахування стимулює компанії до постійного вдосконалення своїх систем безпеки та впровадження новітніх технологій для запобігання інцидентам. Разом з тим, кіберстрахування допомагає підвищити рівень обізнаності працівників щодо потенційних загроз і методів їх запобігання. Співпраця між страховими компаніями та онлайн-бізнесом дозволяє розробляти індивідуальні плани захисту, які б враховували специфіку кожної компанії та її вразливість до зовнішніх загроз.

Забезпечення належного рівня кібербезпеки через кіберстрахування допоможе підвищити довіру клієнтів до онлайн-торгівлі, що є ключовим фактором для успішного ведення бізнесу. У разі кіберінциденту, страхування дозволяє швидко відновити діяльність і мінімізувати негативні наслідки для репутації компанії. Таким чином, кіберстрахування є важливим інструментом для захисту даних та забезпечення стабільності онлайн-торгівлі в умовах постійно зростаючих кіберзагроз. Це дозволяє компаніям не лише захищатися від кібератак, але й активно працювати над зменшенням ризиків та підвищенням рівня кібербезпеки.

Список літератури:

1. Хакери зламали компанію Cisco, щоб шпигувати за урядами країн. 2024. URL: https://speka.media/xakeri-zlamali-kompaniyu-cisco-shhob-spiguvati-za-uryadami-krayin-v5w1kz (дата звернення 15.08.2024).

2. Ільчук В. П., Парубець О. М., Сугоняко Д. О. Інноваційні підходи до розвитку ринку кіберстрахування в Україні. *Електронне наукове фахове видання «Ефективна економіка.* 2018. № 5, 2018. URL: http://www.economy.nayka.com.ua/pdf/5_2018/5.pdf (дата звернення 15.08.2024).

3. Приказюк Н. В., Гуменюк Л. С. Кіберстрахування як важливий інструмент захисту підприємств в умовах цифровізації економіки. Електронне науково-фахове видання «Ефективна економіка». 2020. № 4. URL: http://www.economy.nayka.com.ua/pdf/4_2020/8.pdf (дата звернення 15.08.2024).

4. 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 (дата звернення 15.08.2024).

5. Нагайчук Н.Г., Третяк Н.М., Ткаленко О. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. Фінансовий простір. 2019. № 1 (33). С. 97–111. URL: 10.32702/2307-2105-2020.4.6 (дата звернення 15.08.2024).

6. Про основні засади забезпечення кібербезпеки України: Закон України від 21.06.2018 за № 2469-VIII / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 15.08.2024).

7. Глобальний ринок кіберстрахування очікує ще один рік зростання в 2024 році. URL: https://forinsurer.com/news/24/03/25/43600 (дата звернення 15.08.2024).

Volynets V.V. THE ROLE OF CYBER INSURANCE IN ENSURING DATA SECURITY IN ONLINE TRADE

The article is devoted to the question of the role of cyber insurance in ensuring data security in online trading. It has been determined that the development of innovative technologies and the growing popularity of online commerce have strengthened the need to protect the security of data of business entities and consumers. Fraudulent schemes with each cyber attack cause considerable damage to the online trading sector, since it is quite difficult to track the unauthorized influence of criminals at once. In view of this, the issue of protecting personal and financial information that is contained or transmitted through digital platforms remains especially relevant.

The article provides an overview of the recent increase in cases of unlawful interference with data security, as criminal intentions in cyberspace are constantly evolving, improving and provoking new problems associated with the seizure of confidential and financial information. In view of this, frequent cases of data security violations carry a threat of serious financial costs, a decrease in the reputation of companies, and provocation of a negative impact on consumer confidence.

The conclusions summarize that ensuring data security in online trading is an extremely important issue, since it allows assessing the effectiveness of cyber insurance to minimize risks and ensure reliable information protection. Given this, the rapid adaptation of insurance products to new cyber threats, changes in regulatory requirements is an important issue that requires detailed study. Therefore, the study of the role of cyber insurance in ensuring data security will aim to improve existing mechanisms of protection against cyber attacks and develop new strategies for effectively overcoming cyber threats in online commerce.

Key words: *online trade, cyber attacks, cyber security, financial losses, confidential information, reputation.*