Шифр «Кіберстрахування 2020»

РОЗВИТОК КІБЕРСТРАХУВАННЯ ЯК СЕГМЕНТУ ГЛОБАЛЬНОГО СТРАХОВОГО РИНКУ

ЗМІСТ

ВСТУП

Актуальність дослідження. З поширенням цифрових послуг відповідальність бізнесу за зберігання, обробку, використання, контроль за конфіденційністю персональних даних істотно збільшилася. Помилки в роботі з великими обсягами персональних даних обертаються величезними штрафами, витратами на відновлення, захист ділової репутації. Перехід економіки до цифрового типу включає в себе як позитивні, так і негативні моменти, які в першу чергу пов'язані з інформаційною безпекою. І Україна не є виключенням у списку країн, яким характерні кіберінциденти, і до цього часто виявляються не готові ні влада, ні бізнес.

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

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. Кондратьєва, Й. Малкотра, Л. Мамаєвої, Т. Моташко, О. Парубець, С. Перцової, Н. Приказюка, Т. Ротової, Д. Сугоняко, К. Хейєса, Ю. Шевченко, С. Шекелфорда.

Розрізненість підходів до формування поняття кіберстрахування у вітчизняній та зарубіжній практиці, законодавча невизначеність основних понять, що входять до його складу зумовлюють необхідність проведення подальших досліджень у напрямку обґрунтування підходів до розвитку кіберстрахування як сегменту глобального страхового ринку.

Сучасне глобальне взаємопов'язане бізнес-середовище посилює імовірність кіберзагроз для організацій. Для зменшення ризиків і оптимізації нових можливостей організації мають бути захищеними, пильними і гнучкими. Саме тому, **метою дослідження** є комплексне вивчення тенденцій розвитку

кіберстрахування як сегменту глобального страхового ринку та обґрунтування підходів до його розвитку в Україні.

Для досягнення поставленої мети дослідження сформульовано та вирішено такі **завдання**:

- розкрити теоретичні аспекти кіберстрахування як сегменту глобального страхового ринку;

- проаналізувати сучасні тенденції розвитку кіберстрахування;

- обґрунтувати підходи до розвитку кіберстрахування в Україні.

В роботі було використано методи порівняльного аналізу - при порівнянні обсягів витрат та доходів від кіберстрахування та кількості компаній які придбали поліси кіберстрахування за різними країнами; контент-аналізу - для вивчення нормативно-правової бази з досліджуваної проблематики та узагальнення - для обґрунтування підходів до розвитку кіберстрахування як сегменту глобального страхового ринку.

Результати дослідження опубліковано у науковій статті.

1. ТЕОРЕТИЧНІ АСПЕКТИ КІБЕРСТРАХУВАННЯ ЯК СЕГМЕНТУ ГЛОБАЛЬНОГО СТРАХОВОГО РИНКУ

Кіберзлочинність в останні роки стає практично буденним явищем. У новинах щоразу чутно про зникнення великих сум з рахунків найбільших світових банків або про затримання чергового хакера.

Кіберризик - 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, в системах інтернет-торгівлі і в промислових системах управління. Також це ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних [1; 2, с. 422].

Кіберстрахування- явище нове не тільки для України, а й для всього світу. За даними Munich Re за 2018 рік, подібний захист пропонують в цілому 60 страхових компаній в різних країнах. У той же час страхуванням покрито лише 5% кіберризиків [3].

Проте швидке зростання загроз з боку хакерів стимулює розвиток цього напрямку, і за оцінками страхової групи Allianz, ринок кіберстрахування зростає на 25-50% щороку [4].

Провідний дослідник у галузі страхування С. Ванг вважає, що активізувати роль кіберстрахування у зменшенні кіберризиків та підвищенні кіберстійкості необхідно не просто шляхом передачі ризику від компаній до страховиків, а пом’якшенням вимог органів нагляду за страховою діяльністю на продукти кіберстрахування, розвиваючи при цьому взаємовигідне партнерство між страховими компаніями та організаціями, які профілюються на безпеці інформаційних технологій у напрямку надання інтегрованих послуг зі зменшення ризику та страхового захисту, що ґрунтується на угодах розподілу доходів у сферах надання консультаційних послуг зі страхування ризику, розслідування випадків та розгляду претензій, відшкодування збитків [5].

Лідером кіберстрахування по праву можна вважати США з їх потужною IT-інфраструктурою, де були відзначені перші в світі серйозні кіберзагрози для бізнесу та де діє жорстка законодавча база по захисту персональних електронних даних.

Кіберстрахування є динамічним сегментом глобального ринку страхових послуг. Безсумнівно, даний вид страхування розглядається як метод управління ризиками та захисту від різних загроз, що виникають при здійсненні електронної комерції.

До основних ризиків можна віднести:

- крадіжку таємної і конфіденційної інформації персоналом організації;
- крадіжку номерів кредитних карт;
- розкрадання фінансових коштів з депозитів;
- втрату носіїв інформації;
- фішинг;
- кібервимагання;
- порушення роботи комп'ютерної мережі внаслідок хакерських атак.

Але головним завданням кіберстрахування залишається захист від великомасштабних хакерських атак.

Свою популярність в розвинених країнах кіберстрахування отримало завдяки розумінню, що при впровадженні новітніх рішень у сфері кібербезпеки та проведенні постійної роботи з персоналом завжди залишається 1% ризику компрометації системи, який неможливо передбачити і реально оцінити [6].

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 [7].

Укладення договору страхування кіберризиків пов'язане з комплексною оцінкою клієнта та його систем. Оцінюється економічний стан компанії, канали

продажів, безпека комп'ютерних мереж, ступінь захисту персональних даних клієнтів. Чим більше у страхувальника доступу до конфіденційної інформації користувачів, тим дорожче буде ціна страхової програми. Також впливає фізична охорона серверних даних, доступ до них, наявність ключів доступу, регулярність резервного копіювання даних [8, с.177].

Кіберризик - дуже нагальна проблема, але щоб вирішити її за допомогою страхових інструментів, необхідно створити умови. Це вимагає законодавчої бази, технічних можливостей та готовності клієнтів співпрацювати зі страховиком для створення системи корпоративної кібербезпеки [9].

Збитки від кіберризиків можна розділити на три групи:

1. Безпосередньо збитки самого страховика. Відновлення втрачених (недопущених вигідних) від переривання діяльності та затримки на відновлення пошкодженої інфраструктури (наприклад, при прибутковому новому комп'ютерному обладнанні) та про введення в дію прогалин в системах кібербезпечного страхування, які стають причиною виникнення інцидентів.

2. Збитки перед третіми особами. У даному випадку покривається відповідальність в рамках матеріальної шкоди, морального збитку, порушення прав інтелектуальної власності та ін. Страхування відповідальності перед третіми особами у сфері IT особливо актуальне для IT-провайдерів, хостінг-центрів, розробників програмного забезпечення.

3. Витрати на кризовий менеджмент. Страхова компанія закладає витрати на залучення експертів до IT-безпеки, консультантів, юристів для усунення та мінімізації втрат в кібернетичній атаці.

Найчастіше договори страхування кіберризиків покривають перші дві групи збитків. Тобто втрати страхувальника та шкоду, завдану третім особам.

У додатковому покритті деяких страхових програм страхових компаній є послуга, яка покриває витрати на кризовий менеджмент і на відновлення репутації компанії після кібератаки

Основна складність при страхуванні кіберризиків - це фіксація збитків і доказ причинно-наслідкового зв'язку між страховим випадком і заявленим

збитком. Крім того, суму збитків потрібно якось підрахувати і документально підтвердити. Так, наприклад, найскладніше застрахувати масиви даних, які важко оцінити. Зовсім не просто встановити скільки коштує витік даних невеликої фірми або конкретної приватної особи та яким чином оцінювати такий збиток [10].

Якщо збитки понесла безпосередньо компанія-страхувальник, проводиться експертиза, завдання якої - довести або спростувати вторгнення третіх осіб в комп'ютерну систему, чиї дії спровокували псування майна та простої у виробництві.

При страхуванні відповідальності перед третіми особами факт настання страхового випадку підтверджується рішенням суду, при цьому страховик не несе відповідальність за грубі порушення співробітниками компанії-страхувальника вимог з кібербезпеки, за шахрайські дії страхувальника і дії його співробітників, які викликані їх недостатньою кваліфікацією.

Таким чином, договір страхування кіберризиків допомагає захиститися від загроз, в результаті яких може статися витік даних, вихід з ладу різного обладнання і збитки, які через ці події несе страхувальник. Найчастіше попит компаній на дане покриття задовольняється через покупку додаткових розширень в договорах майна, відповідальності. Але покриття за кіберризиками в таких договорах, з огляду на специфіку даних видів страхування, досить обмежена [8, с. 177].

Тому договір кіберстрахування - це, як правило, комплексний продукт, який включає в себе страхування майна, відповідальності та фінансових ризиків. Основний страховий випадок - збитки, які виникли в результаті порушення роботи комп'ютерної мережі (або її систем безпеки) страхувальника через вторгнення третіх осіб.

Прикладами наслідків такого вторгнення можуть бути: надання несанкціонованого доступу до комп'ютерних систем компанії; зміна, видалення або передача електронних даних, програмного забезпечення; використання ресурсів комп'ютерної системи і т. д. У свою чергу, несанкціоноване

вторгнення зазвичай має на увазі використання будь-яких засобів деактивації і обхід систем захисту комп'ютерної мережі (включаючи віруси і шкідливі програми, фішинг) і DoS / DDoS-атаки.

Основними видами кіберризиків у сучасних умовах виступають кріптовіруси, хакерські атаки на інформаційні системи об’єктів критичної інфраструктури, фінансово-кредитних установ, державних інституцій, крадіжки персональних даних, несанкціоновані транзакції, DDoS–атаки на DNS-сервери тощо.

Це призводить до збільшення витрат суб’єктів господарювання на вдосконалення захисту інформаційних систем, які, на жаль, не завжди можуть протистояти та відбити можливі кібератаки. У цьому випадку зменшити рівень втрат від настання кібератак можливо за допомогою кіберстрахування.

Наявні проблеми становлення і функціонування кіберстрахування можна поділити за класифікаційними ознаками (табл.1).

Таблиця 1

Проблеми становлення і функціонування кіберстрахування за класифікаційними ознаками

№ з/п	**Класифікаційна ознака**	**Сутність класифікаційної ознаки**
1	2	3
1.	Інституційна	відсутність законодавчо-нормативної бази регулювання кіберстрахування, діяльності страхових компаній, які можуть надавати послуги зі страхування кіберризиків
2.	Фінансова	недостатній обсяг фінансових ресурсів, що вкладаються у сферу забезпечення кібербезпеки на державному, регіональному, локальному рівнях; відсутність ефективних фінансових інструментів і важелів розвитку національної системи кіберстрахування
3.	Інформаційна	помилки в розробці й підтримці інформаційних систем страховиків і страхувальників; розвиток кібершпіонажу; перенесення персоналом підприємств, установ, організацій комерційної інформації в соціальні мережі
4.	Організаційна	відсутність кваліфікованого персоналу у сфері страхування кіберризиків; довіри юридичних і фізичних осіб до діяльності страхових компаній і ринку кіберстрахування; тимчасовий характер страхових відносин

Продовження табл. 1		
1	2	3
5.	Маркетингова	низький попит на продукти кіберстрахування через їх високу вартість; небажання клієнтів надавати необхідний для виявлення страхових випадків доступ до своїх інформаційних систем; відсутність досвіду страхових компаній з врегулювання ситуацій настання страхових подій, пов'язаних з втручанням в інформаційний простір держави, суб'єктів господарювання і населення; відсутність рекламування в засобах масової інформації, соціальних мережах переваг страхування кіберризиків у порівнянні з можливими збитками від кібератак; низький рівень конкуренції в сегменті кіберстрахування
6.	Науково-методична	відсутність наукового обґрунтування методики визначення показників оцінювання та розрахунку кіберризиків, стандартів оцінки збитків від настання кібератак та суми їх відшкодування страхувальниками

Джерело: систематизовано та побудовано автором за даними [6;9]

Особливістю кіберстрахування є те, що попит на нього формується в процесі виникнення кіберзагроз або після кібератак. Пропозиція залежить від індивідуальних особливостей настання кіберінцидентів у страхувальників, вартості страхових послуг, розміру прибутку страховиків та відшкодування збитків від настання страхових випадків, можливістю останніх укладати страхові договори через систему Інтернет (онлайн-поліси).

Отже, з розвитком кіберзагроз та кібератак страхування стає вагомим інструментом ризик-менеджменту для підприємств як державної, так і недержавної форми власності. Це перспективний напрям розвитку страхового бізнесу, оскільки створення страхових програм захисту крім безпосереднього відшкодування збитків, значною мірою охороняє від таких ризиків та не дозволяє припинити або знищити бізнес.

2. СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРСТРАХУВАННЯ

Як явище, значуще в світовому масштабі, факт кіберзлочинності відзначають як найбільші бізнесмени й економісти світу в на форумах так і найбільші консалтингові компанії. Зокрема, Pricewaterhouse Coopers випустили Всесвітній огляд економічних злочинів, де відзначили вибухове зростання кібератак в останні роки [11].

Кіберінциденти здатні наносити серйозний фінансовий та репутаційний збиток компаніям і економікам країн. Яскравим прикладом уразливості вітчизняного інформаційного сектору став вірус Petya, який масово атакував підприємства країни в 2017 році. Через атаку вірусу Petya влітку 2017 року вітчизняна економіка зазнала втрат на 0,4-0,5% від річного ВВП. Ця ситуація чітко показала: абсолютно будь-яка компанія вразлива до кібертероризму, незалежно від розміру, специфіки та технічного обладнання [12, с.26].

Статистика свідчить про те, що втрати світової економіки внаслідок кібератак збільшуються з кожним роком. І ці невтішні дані все частіше призводять керівництво компаній до думки про необхідність страхування кіберризиків.

Основними видами хакерських атак, які здійснили найбільш потужний негативний вплив на вітчизняну економіку стали:

1. У 2014 році здійснена DDoS-атака призвела до злому сайта Центральної Виборчої Компанії під час Президентських виборів в Україні.

2. Наприкінці 2015 року потужна хакерська атака вивела з ладу об’єкти критичної інфраструктури в Прикарпатті, Києві, Чернівцях.

3. У грудні 2016 року було здійснено декілька хакерських атак, спрямованих на втручання до інформаційних систем Міністерства фінансів України, Державної казначейської служби, Пенсійного фонду, а також сайту Укрзалізниці та підстанції Північної компанії Укренерго.

4. Влітку 2017 року відбулася найбільш масштабна за наслідками і рівнем збитку хакерська атака за допомогою вірусної програми Petya, яка порушила роботу системи органів виконавчої влади, державних і приватних підприємств, банківських установ, мобільних операторів, засобів масової інформації.

5. У жовтні 2017 року була здійснена чергова атака на Міністерство інфраструктури України, Одеський аеропорт і київське метро з використанням нового вірусу-шифрувальника, який вимагав викуп у біткоїнах [13].

Одним з можливих методів захисту від кібератак і компенсації негативних наслідків від них може виступати кіберстрахування.

Страхування як фінансовий інструмент набув поширення на міжнародному ринку ще у 2010 році. За оцінками Munich Re, обсяги доходів від кіберстрахування у 2020 році складуть $8-9 млрд проти $3,4-4 млрд у 2017 році. Щорічні втрати світової економіки від кіберзлочинності надзвичайно великі, так у 2017 році вони перевищили $400-600 млрд і склали 0,8% світового ВВП, що на 35% більше порівняно з 2015 роком [3].

Тільки атака вірусів WannaCry і Petya в 2017 році торкнулася 150 країн і завдала збитків більш ніж на $ 12 млрд. Тому компанії витрачають на кіберзахист все більше коштів. У дослідженні агентства MarketsandMarkets йдеться, що за підсумками 2018 року витрати бізнесу на захист від хакерів склали майже $ 153 млрд, а в 2023-му вони перевищать $ 248 млрд [11].

Під час щорічного дослідження глобальних ризиків від Allianz Global Corporate & Specialty AGCS), яке проведено 2415 експертами з 86 країн (включаючи топ-менеджерів компаній, страхових експертів, брокерів і ризик-менеджерів), кіберризики (кіберзлочинність, збої у роботі IT-систем, вразливість даних, штрафи), ставлять кіберризики на друге місце серед глобальних ризиків підприємств та фінансового сектора у 2019 році [14].

З цими оцінками складно не погодитися. Особливо якщо подивитися на те, з якою швидкістю цифрові технології накривають планету. За даними компанії Herjavec Group, яка спеціалізується на консалтингу в сфері кібербезпеки, зараз в світі більше 4 млрд користувачів інтернету, в 2022 році їх число зросте до 6

млрд, а у 2030-му - до 7,5 млрд. А за прогнозами Ericsson, до 2023 року кількість підключених до глобальної мережі пристроїв досягне 30 млрд [11].

Дані, зібрані виданням Insurance Journal, показують, що на кінець 2017 року 51% американських компаній не мають полісів кіберстрахування, а 27% не планують купувати його в майбутньому. Заперечення в значній мірі пов'язані зі структурою витрат і передбачуваною недостатньою прозорістю в галузі кіберстрахування [15].

Порівнюючи річні результати кількості компаній, які придбали поліси кіберстрахування у світі, можна побачити, що в цих країнах відсоток організацій, що мають страхування від кіберризиків, зріс з 62% до 75% у 2018 році (рис.1).

Аналізуючи окремі країни, можна побачити деякі цікаві цифри: так у Великобританії відсоток застрахованих компаній підскочив на 29%, при цьому загальна кількість компаній, які інвестують в страхування від кіберризиків становить 90% у 2018 році. В даний час у Великобританії найвищий рівень страхування серед усіх опитаних країн. У США спостерігалося аналогічне підвищення рівня страхування: на 27% більше організацій застраховано в 2018 році, ніж в 2017 році.

Для порівняння: в країнах Північної Європи спостерігається більш повільне поширення, в Швеції відсоток компаній, що мають страхування від кіберризиків, збільшився лише на 1%, і це країна з найнижчими рівнями - тільки 57% мають страхування від кіберризиків.

До опитування проведеного FICO було додано 5 країн, які вперше опитали у 2018 році; 76% організацій мають певний рівень страхування від кіберризиків [16] (рис. 1).

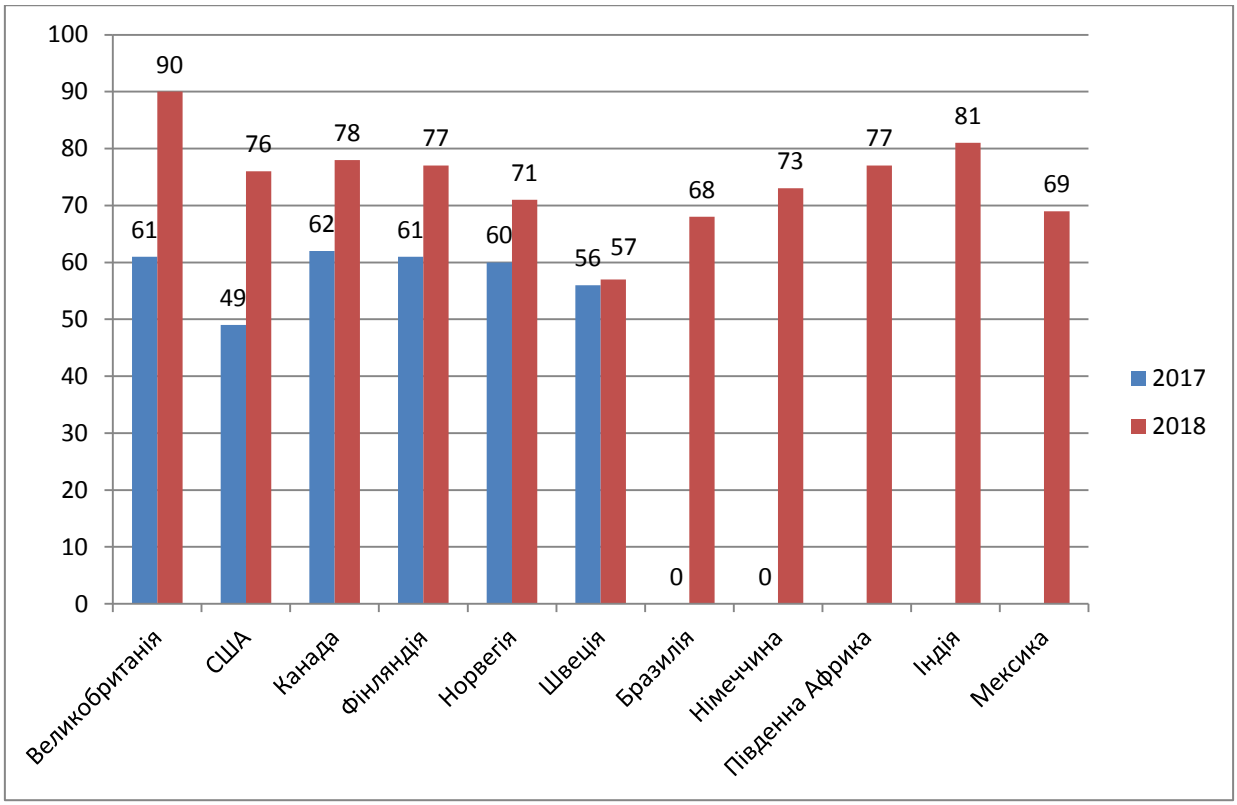

Рис. 1. Кількість компаній, які придбали поліси кіберстрахування у світі у 2017-2018 рр., %

Джерело: побудовано автором за даними [16]

Доцільно відмітити, що у Топ-10 страхових компаній, які займали 69,5% глобального ринку страхування в 2018 році, визначені п'ять провідних кіберстраховиків:

1. Chubb $ 325,8 млн. (16% ринку; 98% покриття)
2. AXA 255,9 млн. Дол. США (12,6% ринку; 100% автономно)
3. AIG $ 232,6 млн. (Частка ринку 11,4%; автономна 99,9%)
4. Мандрівники $ 146,2 млн. (7,2% ринку; 77,2% автомно)
5. Beazley $ 110,9 млн. (5,5% ринку; 90,9% автономно) [17].

Від зазіхань хакерів страждають навіть більшою мірою не рядові користувачі, а великий бізнес, який втрачає колосальні гроші. Найбільш привабливими для кіберзлочинців є фінансово-кредитні установи, особливо банки, які широко використовують сучасні IT і реєстроутримувачі цінних паперів. У зоні ризику також будь-яка компанія, що зберігає інформацію щодо

клієнтів в електронному вигляді: аудитори, рітейлори, брокерські, туристичні, транспортні, страхові компанії, заклади сфери розваг [8, с. 178]. Так, несанкціоновані втручання в діяльність систем Інтернет-Клієнт-Банк та Інтернет-банкінгу, кіберкрадіжки даних із банківських рахунків та платіжних карток клієнтів є наслідком значної кількості кіберзлочинів у фінансовій сфері. За даними Національного банку України, у 2017 р. сталося 77,6 тисячі випадків шахрайства з банківськими картками, що призвело до втрати коштів на суму 163,7 млн грн. [18].

Саме за рахунок перелічених втручань в банківську систему, інститут банківської таємниці стає більш вразливим і спричиняє втрату ділового іміджу й довіри фізичних і юридичних осіб до банківської системи країни загалом. На заваді ефективної взаємодії банківських установ і страхових компаній у напрямі зменшення негативного впливу кіберзлочинів постає низький рівень фінансової грамотності населення стосовно гарантування безпеки власних банківських рахунків і можливостей страхування від різного роду кіберризиків, що у випадку їх настання дасть змогу повернути значну суму коштів у вигляді страхового відшкодування за укладеними договорами [9].

Це зумовлює необхідність створення сумісних інформаційно-просвітницьких ресурсів, завдяки яким клієнти могли б чітко побачити, з яким банком співпрацює та чи інша страхова компанія і який спектр страхових послуг у сфері кіберстрахування надає.

Розвиток внутрішнього кіберстрахування потребує також удосконалення інституційного механізму управління діяльністю страхових компаній, який враховує вплив ендогенних і екзогенних факторів та поєднує інструменти державної підтримки диверсифікації інноваційних продуктів страхування з ринковими. Основними проблемами державного регулювання зазначеного ринку є недосконаліть нормативно-законодавчої бази, відсутність державних стандартів функціонування та державної фінансової підтримки.

Про формування повноцінного сектору кіберстрахування в Україні говорити поки зарано: інтерес до послуги почав формуватися у 2017 році, коли компанії розраховували збитки та втратили прибуток через напад вірусу Petya.

Крім того, основна інфраструктура, необхідна для розвитку цього виду страхування, лише формується. Так, Закон "Про основні засади забезпечення кібербезпеки України" набув чинності у травні 2018 року [19], а Державний центр реагування на кіберзагрози був створений лише у лютому 2018 року.

В українських реаліях далеко не завжди можливо навіть провести перевірку перед аудитом інформаційної системи клієнта, і для цього є багато причин. Як результат, не всі страховики готові надавати повноцінні програми страхування кіберризиків в Україні. Страховими компаніями, які працюють над розробкою і впровадженням таких програм страхування в Україні є «PZU Україна», «ВУСО», «АСКА», «Global Garant», «Українська страхова група», «ІНГО Україна»,

Факторами, що стримують розвиток страхування кіберризиків в Україні є наявність неякісної ІТ-інфраструктури, у багатьох компаній неліцензійне програмне забезпечення та потреба у доведенні підприємством саме факту кібератаки. Не всі із постраждалих від кібератак бажають повідомляти про витоки даних та проломи у системі безпеки. Перешкодою є й висока вартість страхових програм, оскільки страховики працюють із недостатньою страховою статистикою, а відтак важко правильно розрахувати страхові тарифи [8, с. 177].

Кіберстрахування характеризується консервативною моделлю побудови, і страховим компаніям, насамперед, треба завоювати довіру страхувальників до страхових продуктів у сфері інформаційної безпеки.

Розвиток кіберстрахування потребує об’єднання зусиль страхових компаній, Департаменту кіберполіції, Національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації задля протидії кіберзагрозам. У Законі «Про основні засади забезпечення кібербезпеки України» зазначено, що «державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом: періодичного проведення національного саміту з

професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки [8, с.178].

Важливим напрямом також є розвиток мережевої взаємодії національних страхових компаній між собою та страховиками інших країн з метою обміну позитивним досвідом у сфері страхування кіберризиків. Зазвичай збитки від кіберзлочинів становлять значну суму, і страхові компанії об'єднують свої зусилля шляхом перестрахування.

Сфера застосування кіберстрахування, як ефективного інструменту відшкодування значної суми збитків у результаті настання кібератак, у майбутньому розширюватиметься завдяки використанню біометричних методів ідентифікації в процесі здійснення фінансових, зокрема, страхових операцій; розширення сфери застосування чат-ботів суб'єктами страхової, банківської та бізнес сфер; збільшення кількості хакерських атак на провайдерів хмарних технологій та їхніх клієнт-серверних мереж [10].

З метою захисту прав страхувальників необхідно створити інститут страхових омбудсменів, що сприятиме покращенню якості і прозорості надання послуг на ринку кіберстрахування.

Перший крок до створення такого інституту було здійснено у 2015 році, коли була створена громадська спілка «Український страховий омбудсмен» (УСО) [20], головною метою діяльності якої є надання безплатної консультаційної допомоги у вирішенні спірних питань між страхувальниками і страховиками щодо виплати страхового відшкодування в основному за полісами «автоцивілки». Рішення омбудсмена є обов'язковими для страхових компаній, що входять до складу УСО, для інших страховиків вони мають рекомендаційний характер.

Впровадження страхових продуктів на ринку кіберстрахування потребує впровадження інформаційних технологій страховиками. Для того щоб страхувати різноманітні кіберризики та відповідати зростаючим вимогам клієнтів, до складу яких можуть входити високотехнологічні компанії,

підприємства критичної інфраструктури, телекомунікаційні фірми, фінансово-кредитні установи, бізнес-структури тощо, страхові компанії повинні тісно співпрацювати з постачальниками телематичного обладнання, мобільними операторами, провайдерами хмарних сервісів і т. ін.

При цьому треба враховувати той факт, що страхові компанії, які надають послуги з кіберстрахування, також можуть стати об'єктами кібератак у випадку недостатнього забезпечення їхньої інформаційної безпеки.

Несвоєчасне виявлення та затримка нейтралізації витоку конфіденційної інформації, втрата інтелектуальної власності можуть спричинити більш глобальні наслідки, пов'язані із зростанням недовіри до страхового ринку, масового розірвання укладених договорів страхування, виплати страховиками значної суми коштів у вигляді страхового відшкодування наслідків кіберкрадіжки.

Виходячи з цього, страхові компанії, що здійснюють страхування кіберризиків, повинні забезпечити надійне зберігання конфіденційної інформації, що міститься на паперових або електронних носіях, створивши відповідні служби інформаційної безпеки.

До функцій останніх необхідно передати ідентифікацію внутрішніх і зовнішніх загроз, які можуть призвести до випадкових або зловмисних витоків інформації.

Для забезпечення стійкості від кіберзагроз необхідно налагодити тісну співпрацю між службами безпеки страховиків і страхувальників на основі застосування сучасних технологій та пристроїв запобігання витоку даних з їхніх інформаційних систем, мінімізувавши вплив людського фактору.

Без суттєвої державної фінансової підтримки, розробки державних стандартів, індикаторів та граничних значень оцінки інформаційної безпеки у сфері страхування забезпечити надійний захист інформації на практиці дуже складно.

Розвиток кіберстрахування потребує прискорення інформатизації послуг зі страхування кіберризиків. Нині дуже складно знайти інформацію про

страхові компанії, що пропонують укладання полісів кіберстрахування, спектр їхніх послуг, розмір відшкодування збитків та ін. Зважаючи на це, необхідна чітка регламентація механізмів взаємодії між страховиками і страхувальниками.

Конкурентну перевагу на ринку кіберстрахування отримають страхові компанії, які при розробці методології визначення страхових тарифів і ризиків кіберстрахування будуть застосовувати актуарне моделювання на основі використання персоналізованого маркетингу, що забезпечить індивідуальний підхід до кожного клієнта за допомогою використання інтерактивних комунікацій.

Тому прийняття кіберризиків на страхування неможливе без застосування індивідуального андеррайтингу, який включає комплекс заходів, спрямованих на збалансування інтересів страхувальника і страховика в напрямку проведення експертної оцінки таких ризиків, прогнозування ймовірності розміру потенційних збитків від настання кіберінцидентів, визначення умов страхування, розміру страхового покриття і премій.

3. ОБҐРУНТУВАННЯ ПІДХОДІВ ДО РОЗВИТКУ КІБЕРСТРАХУВАННЯ В УКРАЇНІ

Основним завданням розвитку кіберстрахування є захист від наслідків великомасштабної хакерської атаки. Цей вид страхування забезпечує фінансовий механізм відновлення після великих збитків, допомагаючи підприємствам повернутися до нормального функціонування, збереження стабільності, платоспроможності та зниження втрат у результаті перерви у виробництві.

Крім того, страхові компанії пропонують такі додаткові умови: відшкодування витрат на розслідування кіберзлочинів, антикризовий піар з метою якого євідновлення репутації, витрати на захист у суді й відновлення роботи IT-систем [7].

Розрізненість теоретичних підходів до формування ринку кіберстрахування у вітчизняній і зарубіжній практиці та законодавча невизначеність основних понять, що входять до його структури зумовлюють необхідність обґрунтування підходів до його розвитку з урахуванням сучасних тенденцій зростання кіберзагроз.

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» [21], Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [22], Закон України «Про основи національної безпеки України» [23] та Закон України "Про основні засади забезпечення кібербезпеки України" [19].

Крім того, діють стратегічні та міжнародні документи, такі як: Стратегія національної безпеки України [24] та «Конвенція про кіберзлочинність» [25].

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, на нашу думку, доцільно

виділити три основні проблеми, які ускладнюють боротьбу з кіберзлочинами в Україні:

- по-перше, відсутність визначень ключових термінів та категорій у науковій та фаховій літературі;

- по-друге, неузгодженість чинних нормативно-правових документів у сфері протидії кіберзлочинності;

- по-третє, відсутність державної системи протидії кіберзлочинам, у т.ч. шляхом страхування кіберризиків.

Зауважимо, що однією з основних причин розвитку кіберзлочинності як виду кримінального бізнесу, є значна прибутковість при незначних вкладеннях та виробничих витратах.

Іншою причиною росту кіберзлочинності можна вважати незначні ризики при складності оперативно-пошукових та слідчих заходів у разі скоєння кіберзлочину. Крім того, на думку М. Гудмана та С. Бреннера, існує психологічний аспект кіберзлочинності: злочинці не знають об'єкти злочину (жертви) особисто, що припускає відсутність у них прояву почуття провини та стримування [26].

У той же час, як свідчить досвід зарубіжних країн, істотно знизити можливі збитки від дії кіберзлочинців можливо шляхом страхування кіберризиків.

Розглянемо характерні види кіберризиків і напрями кіберстрахування (табл.2).

З метою зменшення банківських ризиків провідні страхові компанії зарубіжних країн створили та впроваджують комплексні програми страхування банківських ризиків, що в сукупності застрахованих ризиків банківської діяльності передбачають страхування від комп'ютерних злочинів [27].

Необхідно зауважити, що поліс страхування від кіберзлочинів створено для забезпечення захисту банку від зростаючого ризику несанкціонованого доступу до інформації автоматизованих систем, які використовуються для обслуговування клієнтів.

Таблиця 2

Характерні види кіберризиків і напрями кіберстрахування

Види кіберризиків	**Напрями кіберстрахування**
Ризик втрати інформації та порушення роботи систем при зламі пароля доступу або внаслідок DDoS-атаки	За сутністю відноситься до кіберризику втрати інформації та порушення роботи комп'ютерних систем. Кіберстрахування відшкодує витрати на поновлення діяльності інформаційної технології, наприклад, web-сайту.
Ризик фінансових втрат через порушення роботи комп'ютерних систем	За сутністю відповідає ризику втрати вигоди в offline-страхуванні. Напрям страхування захищає IT-підприсмства від втрат з вини кіберзлочинців у разі порушення роботи комп'ютерних систем. Напрям страхування є доцільним для захисту online-магазинів, медіа-кінотеатрів, систем трекер-торентів.
Ризик фінансових втрат за регрес-позовами при викраденні, розголошенні або використанні персональної інформації	Сутність полягає в ризику втрат від регрес-позовів власників даних при викраденні, розголошенні та використанні кіберзлочинцями їх персональної інформації. Цей напрям страхування відшкодовує збитки підприємств за регрес-позовами власників персональної інформації.
Ризик фінансових втрат за здирницгвом при вірусному блокуванні комп'ютерних систем	Сутність полягає в кібервимаганні (здирництві) через примушення до сплати (наприклад, шляхом SMS) за розблокування інформаційних систем або інформації при попередньому блокуванні вірусом програм комп'ютерів або баз даних. Кіберстрахування покриває витрати на розблокування інформаційних систем при доведенні витрат та фіксації кіберзлочину для страхувальника.
Ризик фінансових втрат на відновлення програмного забезпечення та (або) інформації внаслідок дії кіберзлочинців	За сутністю є аналогом майнового страхування та відноситься до кіберризику фінансових втрат при пошкодженні програмного забезпечення та (або) інформації внаслідок дії кіберзлочинців. Кіберстрахування відшкодовує витрати на відновлення програмного забезпечення та (або) інформації.

Джерело: авторська розробка

При цьому, поліс кіберстрахування в комплексних страхових продуктах для банків та інших фінансових установ за формою є доповненням до полісу комплексного страхування від загроз кримінальних ризиків банку. З метою уникнення або скорочення втрат банківських установ від дії кіберзлочинців

страхові організації зарубіжних країн створили комплексні страхові продукти, наприклад, страхування від комп'ютерних злочинів – CCI (computer crime insurance) та страхування від атак хакерів – HI (hacker insurance).

Сутність цих страхових продуктів полягає в покритті збитків банку в результаті несанкціонованого доступу до комп'ютерних і комунікаційних систем фінансової організації, введення неправомірних даних або команд, знищення інформації та програм вірусами. У світовій практиці ризики комп'ютерних злочинів та атак хакерів, як правило, приймаються на страхування як додаток до основного полісу комплексного банківського страхування – BBB (banker's blanket bond) [26].

Особливістю страхових полісів "Computer Crime Insurance" та "Hacker Insurance" є те, що при настанні страхового випадку страхова компанія відшкодовує як збитки, заподіяні банку, так і шкоду, заподіяну третім особам (клієнтам банку).

Отже, кіберстрахування в банківській сфері демонструє потенціальні можливості розвитку, оскільки розроблені і використовуються найкращі зарубіжні практики, підходи та меодики. В той же час, 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.

Уряд не має можливості для проведення програм оцінки рейтингу ризику, але він добре підходить для надання інформації та аналізу тенденцій загроз з боку суб'єкта, організації та галузі. Мета повинна полягати в тому, щоб поглибити розуміння громадськістю ризику та виробляти кращі рішення з управління ризиками.

Хоча минулі кіберзагрози не можуть бути основою для всебічних прогнозів загроз завтрашнього дня, вони можуть надати історичні дані для інформування прогнозних моделей. Покращені набори даних, в кінцевому

рахунку, є найкращим способом побудови нових більш ефективних моделей для оцінки кіберризиків. Більш досконалі набори даних дозволять в рамках моделей страхування оцінювати кіберстрахування, оцінювати дані про втрати за претензіями, розуміти кіберризики і зіставляти прогнозні сценарії з відповідними кіберпокриттями.

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

Страхові компанії потребують достовірної інформації про ефективність заходів щодо зниження ризику, щоб встановлювати надбавки до цін, які спонукають компанії бути відповідальними за кібердії. Так, американська компанія Marsh & McLennan оголосила про ініціативу «Cyber Catalyst» в березні 2019 роки для виявлення та оцінки кращих практик та продуктів, які знижують кіберризик. У співпраці з іншими страховими компаніями Marsh надасть інформацію, яка допоможе споживачам «орієнтуватися на переповненому ринку кібербезпеки» [28].

Такі зусилля виходять за рамки платформ обміну інформацією, спрямованих на надання даних про загрози фахівцям з кібербезпеки та спрямовані на те, щоб дозволити приватним суб'єктам найбільш ефективно витрачати свої кошти на кібербезпеку. В кінцевому рахунку, такі зусилля швидко покажуть свій результат - позитивний чи негативний, шляхом прогнозування продуктів кібербезпеки, які забезпечують значущі та вимірні покращення. Хоча жоден продукт не застрахований від атак, деякі з них більш безпечні, ніж інші.

Страховики повинні використовувати спільні програми або аналогічні зусилля (спільні бази даних за кібератаками та кіберризиками), щоб стимулювати компанії брати участь в діях щодо зниження ризиків і впроваджувати програмне забезпечення для кібербезпеки з доведеною захисною цінністю. Така стратегія вже успішно використовується в інших галузях страхування, таких як охорона здоров'я, автомобілі та пожежна безпека.

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

Уряд має забезпечити, щоб політика, якою керуються підприємства, заохочувала найкращі практики кібербезпеки. Зокрема, політики повинні мати достатні межі охоплення і область дії (визначені шляхом аналізу прогнозованих витрат на кібератаки) і повинні забезпечувати оцінку премій для стимулювання поведінки, що знижує ризики, особливо у державному та фінансовому секторі. Компанії в приватному секторі можуть потім звернути увагу на ці поліпшені страхові пропозиції і прийняти рішення про придбання кіберстрахування, якщо вони не зробили це раніше.

4) Уряд за підзвітністю має надати засновані на даних оцінки витрат на зобов'язання оборонних підприємств купувати кіберстрахування.

Перш ніж доручити (або стимулювати) всю оборону галузь на придбання кіберстрахування, уряду необхідно зрозуміти, які витрати такі дії можуть накласти на ці компанії і, в кінцевому підсумку, на платника податків, який, ймовірно, буде нести тягар, оскільки компанії переносять витрати за рахунок збільшення ціни на їх товари та послуги. Подібно до того, як моделі ризиків, засновані на даних, сприятимуть розвитку індустрії кіберстрахування і будуть стимулювати використання передових методів через структури преміальних витрат, державна політика повинна також ґрунтуватися на таких даних.

Отже, для ефективного розвитку кіберстрахування у вітчизняній практиці, важливою є державна підтримка та ініціатива у цьому сегменті страхового ринку. Тільки державне втручання в змозі надати поштовх розвитку кіберстрахування як сегменту глобального страхового ринку.

ВИСНОВКИ

В результаті проведеного дослідження з'ясовано, що інформаційні технології, що стрімко проникають в економічні й соціальні процеси, зумовлюють необхідність змін на ринку страхування України і розвитку такого його сегмента, як кіберстрахування, який забезпечує необхідний страховий захист і відшкодування суми збитку в розмірі, необхідному для компенсації витрат, пов'язаних із втратою баз даних страхувальників та їх подальшим відновленням у разі виникнення масштабних кібератак.

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

Поштовхом для розвитку зазначеного ринку стане прийняття відповідних законодавчих актів у сфері забезпечення кібербезпеки на рівні держави та окремих суб'єктів господарювання, чітке визначення в Законі України «Про страхування» сутності кіберстрахування, з віднесенням його до добровільного або обов'язкового виду страхування. 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 з 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.

На законодавчому рівні необхідно посилити кримінальну відповідальність, зокрема і працівників страхових компаній, за продаж інформаційних баз даних клієнтів, розкриття конфіденційної інформації.

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 (купівлю полісів кіберстрахування), які відповідають мінімальним стандартам; компенсацію витрат на зобов'язання оборонних підприємств купувати кіберстрахування.

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кібер-ризик. *Вікіпедія.* URL: uk.wikipedia.org › wiki › Кібер-ризик.

2. Братюк В. П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. 2015. № 9. С. 421-427.

3. Підсумки 2018. URL: https://cyberpolice.gov.ua/results/2018/.

4. Барометр рисков. Allianz назвал глобальные риски предприятий и финансового сектора на 2019 год. URL: https://forinsurer.com/news /19/01/16/36513?hl=%EA%E8%E1%E5%F0% F0%E8%F1%EA%E8

5. Shaun S. Wang. Integrated Framework for Information Security. *Investment and Cyber Insurance.* URL: https://papers.ssrn.com/sol3/papers.cfm? abstract_ id=2918674.

6. Перцева С.Ю. Киберстрахование в цифровой экономике. Современное состояние и перспективы развития рынка страхования: *Материалы III Международной научно-практической конференции.* 2018. С. 60-64.

7. Кібер-страхування: новий інструмент ризик-менеджменту URL: http://forbes.net.ua/ua/opinions/1426423-kiber-strahuvannya-novij-instrument-rizik-menedzhmentu.

8. Ротова Т.А., Шевченко Ю. Страхування як фінансовий інструмент захисту від кібер-ризиків. *Безпека соціально-економічних процесів в кіберпросторі : матеріали Всеукр. наук.-практ. конф.* Київ : КНТЕУ, 2019. 244 с. С. 177-178

9. Ільчук В. П., Парубець О. М., Сугоняко Д. О. Інноваційні підходи до розвитку ринку кіберстрахування в Україні. *Ефективна економіка*. 2018. № 5. URL: http://www.economy.nayka.com.ua/?op=1&z=6295.

10. Мамаева Л.Н. Кибер-страхование как способ обеспечения информационной безопасности. *Научно-практический журнал. Экономическая безопасность и качество*. 2018. № 1(30). С. 76 -79

11. Пігулка від хакерів: як бізнес захищає себе від кібератак. URL: https://mind.ua/publications/ 20192978- pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak

12. Cyber insurance in Ukraine and how it works.*Збірник тез доповідей Міжнародної науково0практичної конференції «Сучасний стан та перспективи розвитку економіки, фінансів, обліку та права».* Полтава. 2019. 61 с.

13. Найбільші кібератаки в Україні з 2014 року. Інфографіка. *Журнал Новое время.* URL:https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika1438924.html.

14. Forbes [2016], "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". URL: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by2019/#7885d6313a91.

15. Jay P. Kesan & Carol M. Hayes Strengthening Cybersecurity with Cyber Insurance. *Markets and Better Risk Assessment* 102 Minn. L. Rev. 191 (2017), University of Illinois College of Law Legal Studies Research Paper No. 17- 18.

16. Who has cyber risk insurance worldwide? URL: https://www.fico.com/blogs/who-has-cyber-risk-insurance-around-world

17. State of the Cyber Insurance Market. *Top Trends, Insurers and Challenges: AM Best* URL: https://www.insurancejournal.com/ news/national /2019/06/18 /529747.htm

18. Офіційний сайт Національного банку України URL: https://bank.gov.ua/

19. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL:https://zakon.rada.gov.ua/laws/ show/2163-19.

20. Український страховий омбудсмен URL: http://ombudsman.ua/.

21. Про інформацію: Закон України від 2.10.1992 №2657-XII зі змін. та допов. від 2.12.2010 №2756-VI URL: zakon.rada.gov.ua

22. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 №80/94-ВР зі змін. та допов. від 27.03.2014 №1170-VII URL: zakon.rada.gov.ua.

23. Про основи національної безпеки України: Закон України від 19.06.2003 №964-IV зі змін. та допов. від 12.02.2015 №186-VIII URL: zakon.rada.gov.ua.

24. Стратегія національної безпеки України: Указ Президента України від 12.02.2007 №105 зі змін. та допов. від 8.06.2012 №389/2012) URL: zakon.rada.gov.ua.

25. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001. Конвенцію ратифіковано із застереженнями Законом України від 07.09.2005 №2824-IV URL: zakon.rada.gov.ua.

26. Goodman, M.D., Brenner, S.W. (2012). The Emerging Consensus on Criminal Conduct in Cyberspace. UCLA J.L. & Tech., No 3 // www.lawtechjournal.com.

27. Сергієнкова О.В., Мелентьєва О.В. Проблеми та перспективи розвитку страхування банківських ризиків в Україні. URL: конференция.com.ua.

28. Leslie Scism. Insurers Creating a Consumer Ratings Service for Cybersecurity Industry. *The Wall Street Journal*. 2019 URL: https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service- for-cybersecurity-industry-11553592600)