

на інші фінансові послуги. Розвиток ресурсів даного типу є важливим кроком для поліпшення комунікації страхових компаній зі своїми потенційними клієнтами.

Згідно зарубіжного досвіду, рівень інноваційності страховика є одним із визначальних чинників підвищення його конкурентоспроможності. Потреба у реалізації інноваційних рішень на ринку страхових послуг обумовлюється необхідністю автоматизації бізнес-процесів, застосуванням цифрових технологій, наявністю альтернативних каналів збуту та використанням ефективних маркетингових ідей.

#### **Список використаних джерел**

1. Щоквартальний брифінг InsurTech 2 кварталу 2021 року. URL: <https://www.willistowerswatson.com/en-HK/Insights/2021/07/quarterly-insurtech-briefing-q2-2021> (дата звернення: 24.10.2021).
2. Офіційний сайт Metromile. URL: <https://www.metromile.com> (дата звернення: 24.10.2021).
3. Офіційний сайт Cuvva. URL: [www.cuvva.com](http://www.cuvva.com) (дата звернення: 25.10.2021).
4. Офіційний сайт Trov. URL: <https://trov.com> (дата звернення: 25.10.2021).
5. Офіційний сайт Money SuperMarket. URL: [www.moneysupermarket.com](http://www.moneysupermarket.com) (дата звернення: 25.10.2021).

**УДК 336.71**

***Т.Г. Іванова,***

к.е.н., доц., професор кафедри банківської справи та страхування,  
ДВНЗ «КНЕУ імені Вадима Гетьмана»,  
[t\\_ivanova\\_03@ukr.net](mailto:t_ivanova_03@ukr.net)

## **ПЕРСПЕКТИВИ РОЗВИТКУ РИНКУ КІБЕРСТРАХУВАННЯ В УКРАЇНІ**

Діджиталізація і цифрові технології все міцніше входять у всі аспекти нашого життя, та в будь-якій сфері діяльності цифровізація – це необхідна умова для ведення конкурентоспроможного бізнесу. Кібератаки є одним з найбільших ризиків для світової економіки та, на жаль, стають нормою в

постпандемічному житті, особливо в міру того, як все більше фінансово-кредитних установ (КФУ) пристосовуються до використання цифрових технологій. Існуючий стан в інформаційній сфері актуалізував перед державою та КФУ завдання з формування ефективних засобів протидії кіберризикам та запобіганню прояву їх негативних наслідків, тому правовим та економічним засобом мінімізації поширення кіберзагроз стає кіберстрахування.

Кіберстрахування (поліс страхування кіберризиків, cyber insurance) – страховий продукт для захисту бізнесу та фізичних осіб від ризиків, пов’язаних із користуванням інтернетом, зберіганням та обробкою даних в електронному вигляді, роботою з ІТ-інфраструктурами. Кіберстрахування також можна визначити, як метод управління ризиками. Це послуга, за допомогою якої ризики користувачів ІТ передаються страховику за страхову премію [1].

Під кіберризиком мається на увазі будь-який ризик що призводить до фінансових втрат, знищення або погіршення репутації КФУ у результаті виходу з ладу ІТ систем та систем інформаційної безпеки. Даний ризик матеріалізується наступними способами:

- навмисне та несанкціоноване порушення інформаційної безпеки, що призводить до отримання доступу до інформаційних систем КФУ з метою шпигунства, вимагання або нанесення шкоди їх репутації;
- ненавмисне або випадкове порушення інформаційної безпеки, яке може призвести до певних матеріальних та не матеріальних втрат;
- операційні ІТ-ризики за рахунок низької цілісності системи КФУ або інших факторів.

Страхування кібер-ризиків – це можливість знизити ризик негативних наслідків у сфері інформаційної безпеки та мінімізувати наслідки від інцидентів, що вже відбулися. Цей вид страхування забезпечує фінансовий механізм відновлення КФУ після завданих їм збитків, допомагає повернутися до процесу створення продукту та здійснення операцій, зберегти стабільність та

знизити втрати в результаті перерви у фінансово-господарській діяльності. Страхова сума здатна компенсувати збитки та витрати, спрямовані на відновлення бази персональних даних та розслідування того, що сталося.

Перспективи розвитку ринку кіберстрахування полягають у наступних тенденціях:

1) Ринок кіберстрахування зростатиме та є прибутковим. За даними Standard & Poor's Corp. у найближчому майбутньому страхові внески в цій сфері, які зараз складають близько \$5 млрд, збільшаться в середньому на 20-30 % на рік [2]. Використання нових технологій в бізнесі, таких як IoT (Інтернет речей), цьому всіляко сприяють. Валові страхові премії (GWP) з 2016 року збільшилися більш ніж удвічі (середньорічний темп зростання +22%), значно випередивши комерційний P&C-сектор. Аналогічні темпи зростання прогнозуються для глобального кіберринку в наступні кілька років (середньорічний темп зростання +23%), що до 2025 року наблизиться до 20 мільярдів доларів [3].

2) Зазначимо, що, як тільки кіберстрахування ставатиме більш зрілим продуктом на страховому ринку, правила страхування та управління кіберризиками посиляться. Високу планку задаватимуть регулюючі органи, які будуть прагнути забезпечити належні стандарти збору даних і регулярної звітності. В Україні відсутньо спеціальне правове регулювання відносин з кіберстрахування, натомість поширена практика включення до страхових полісів зі страхування майна та транспортних засобів окремих кіберризиків, що зумовило виникнення ряду концептуальних проблем, які потребують наукового дослідження і законодавчого вирішення та закріплення. Можливо кіберстрахування стане однією з обов'язкових вимог для фінансово-кредитних установ.

3) Стандартизація страховки. Через те, що ринок кіберстрахування ще у процесі формування, поліси кіберстрахування на страхових ринках суттєво відрізняються за лімітами, характеристикам, покриттям та умовами. Це викликає певні труднощі у страховиків, які можуть не розуміти, який поліс

підходить найкраще для певного клієнта. В подальшому умови полісів будуть переглянуті в бік стандартизації та виключена двозначність. Альтернативні умови поліса залишаються для більш досвідченого споживача страхових послуг та за додаткову плату.

4) Адаптивна кіберполітика. Дії КФУ можуть впливати на перегляд умов кіберстраховки. Згодом страхова галузь почне краще розуміти кіберзагрози та обирати підхід до клієнтів відповідно до їх ставлення до кібербезпеки. Наприклад, винагороджувати за адекватну поведінку під час кіберінцидентів або надавати додаткові оплачувані послуги з метою більш ефективного контролю безпеки.

5) Системний кіберризик є проблемою для страхових компаній, тому що стандартні універсальні страхові продукти, які вимірюють кіберризики, не достатньо враховують особливості діяльності даного конкретного КФУ, тому найближчим часом виникнуть альтернативні варіанти. Це сприятиме подальшому зростанню ринку кіберстрахування за рахунок розробки індивідуальних страхових продуктів для заповнення ринкових прогалин з метою задоволення попиту клієнтів СК. Так, майбутній договір кіберстрахування може бути заключений на дотримання повного обсягу кібербезпеки та її складових. При цьому клієнт обирає як один із стандартних універсальних страхових пакетів або скласти свій власний пакет з урахуванням особливостей бізнесу та індивідуальних потреб. Базові пакети поліса покривають ризики втрати та пошуку даних (включаючи віруси шифрувальники), програмне забезпечення, розголошення персональних даних та включають розслідування та діагностику кібератак. Крім базових страхових полісів, виникає попит на індивідуальні поліси, в яких передбачено страхування наступних ризиків: втрати інформації; розкрадання інтелектуальної власності; неправомірне використання обчислювальних ресурсів; здирництво; розкрадання коштів; порушення конфіденційності та розголошення персональних даних; заподіяння шкоди майну, життю та здоров'ю третіх осіб; збитки ділової репутації; втрата продукту, перерва у

діяльності. Вартість страхування визначається індивідуально в залежності від набору ризиків, страхової суми та франшизи, а також роду діяльності страхувальника та результатів оцінки ризикозахищеності.

б) Залучення кіберекспертів. Усвідомлення того, що одна масштабна кіберкатастрофа може призвести до величезних фінансових втрат, змушує страхові компанії міркувати над новими підходами до оцінки кіберризиків. Навіть з розвитком більш просунутих інструментів моделювання кіберризиків, страхові компанії будуть інвестувати у залучення кіберекспертів до своєї основної команди з управління ними.

Кіберстрахування, як галузь страхування надзвичайно слабо представлена в Україні та потребує вагомих зусиль, зважаючи на кількість кібер-злочинів за останні роки. Але, слід зазначити, що страхова компанія AIG першою із СК України розпочала страхувати юридичних осіб від кібер-ризиків. Так, СК AIG та міжнародний розробник антивірусного програмного забезпечення ESET з 2018 року представляють новий сервіс для корпоративних клієнтів «Гарантія антивірусного захисту». Програма поєднує антивірусне рішення зі страхуванням від кіберінцидентів. У разі виникнення кіберінцидента страхова компанія допоможе компенсувати збитки в результаті претензій третіх осіб і претензій щодо порушення системи безпеки. Також, в страхове покриття включені витрати на технічну експертизу та відновлення даних і систем, компенсація судових витрат і витрати на повідомлення суб'єктів даних. Даний сервіс допомагає не тільки захистити інформацію та скоротити можливі витрати, але також зберегти репутацію, оскільки СК AIG відповідає за дані своїх клієнтів [4]. Також, в Україні ще дві страхові компанії активно пропонують страхові поліси, що покривають частину кібер-ризиків. Наприклад страхова компанія «UPSK» надає повний комплекс покриття ризиків, у той час коли страхова компанія «АСКА» пропонує індивідуальний підхід з можливістю вибору необхідних ризиків залежно від специфіки господарської діяльності клієнтів [5, 6].

Отже, з переходом на цифрову модель ведення фінансового бізнесу пов'язують і подальший розвиток та вдосконаленням кіберстрахування. Найголовнішою проблемою страхування кіберризиків є відсутність даного виду страхування у більшості СК України, незважаючи на ефективну роботу кіберполіції та загальновідомих рекомендацій задля запобігання кібер-атакам та іншим ризикам. Також, проблемою розвитку кіберстрахування в Україні є відсутність алгоритмів оцінювання кіберризиків, оскільки для кожного виду кібер-злочину потрібно виокремити рівні заподіяної шкоди, оцінити їх та розробити заходи, щоб запобігти наступним атакам. Але, вважаємо, що кіберстрахування є динамічним сегментом глобального ринку страхових послуг та з огляду на безперервно зростаючу кількість кіберзагроз, в найближчому майбутньому воно стане невід'ємною частиною ведення страхового бізнесу в Україні.

#### Список використаних джерел

1. Киберстрахование. URL: <https://ru.wikipedia.org/wiki/> (дата звернення: 17.10.2021).
2. Кіберстрахування: чого чекати в найближчі 5 років? URL: <https://10guards.com/ua/articles/cyber-insurance-what-to-expect-in-the-next-five-years/> (дата звернення: 22.10.2021).
3. Стоимость киберстрахования на глобальном рынке выросла на 32 %. URL: <https://forinsurer.com/news/21/07/20/40054/> (дата звернення: 23.10.2021).
4. Страхування від кібер-ризиків стало ще доступнішим. URL: <https://parasol.ua/ua/news/strahovanie-ot-kiber-riskov-stalo-eshte-dostupnee/> (дата звернення: 24.10.2021).
5. Офіційний сайт страхової компанії UPSK. URL: <https://upsk.com.ua/service/corporate/cyberriskua> (дата звернення: 24.10.2021).
6. Офіційний сайт страхової компанії АСКА. URL: <https://aska.ua/ua/business-insurance/industry/> (дата звернення: 24.10.2021).