КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА СТРАХУВАННЯ, БАНКІВСЬКОЇ СПРАВИ ТА РИЗИК-МЕНЕДЖМЕНТУ

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

РОЗВИТОК КІБЕРСТРАХУВАННЯ В УКРАЇНІ

Студентки магістратури денної
форми навчання,
спеціальності 072 «Фінанси, банківська
справа та страхування»
освітньої програми «Фінансові інститути та
ризик-менеджмент»
Бабенко Юлії Леонідівни

Науковий керівник:
к.е.н., професор
Пікус Руслана Володимирівна

Засвідчую, що в цій дипломній
роботі немає запозичень із праць
інших авторів без відповідних посилань
Студент _____
(підпис)

Робота допущена до захисту в Екзаменаційній комісії рішенням кафедри страхування, банківської справи та ризик-менеджменту від «18» травня 2022 р., протокол № 11.

Завідувач кафедри страхування,
банківської справи та ризик-менеджменту,
доктор економічних наук, професор
Приказюк Наталія Валентинівна _____
(підпис)

Київ - 2022

АНОТАЦІЯ

Бабенко Ю. Л. Розвиток кіберстрахування в Україні.

Кваліфікаційна магістерська робота за спеціальністю 072 Фінанси, банківська справа та страхування. - Кафедра страхування банківської справи та ризик-менеджменту, економічний факультет, Київський національний університет імені Тараса Шевченка, Київ, 2022.

Метою роботи є удосконалення теоретичних основ та розробка практичних рекомендацій щодо розвитку кіберстрахування в Україні як інструменту фінансової безпеки юридичних та фізичних осіб.

У першому розділі роботи уточнено теоретико-методичні основи щодо визначення, змісту та витоків поняття «кіберризик» та «кіберстрахування», наведена авторська конструкція тлумачення змісту за обраними критеріями. Визначено зміст та основні завдання кіберстрахування як ефективного інструменту фінансування втрат за наслідками кіберризиків. Виокремлено два підходи до формування покриття кіберризиків в страхуванні: страхування кібервідповідальності і майнове страхування наслідків можливих кібератак. Охарактеризовано можливі варіанти страхового покриття кібервідповідальності з відокремленням покриття відповідальності першої і третіх осіб, а також кіберстрахування, як різновиду майнового страхування. Визначено, що Європейська Директива має позитивний вплив на розвиток ринку кіберстрахування, а саме інформованості щодо потенційних загроз, усвідомлення необхідності удосконалення системи кібербезпеки та забезпечення превентивних заходів через введені штрафи, особливо для інтернет-ринку, пошукових систем в Інтернеті, служби хмарних обчислень.

У другому розділі виявлені та проаналізовані особливості розвитку кіберстрахування в Україні та розвинених країнах світу. Зв'ясовано, що кіберзахист систем в сучасному інформаційному світі є надзвичайно важливим інструментом захисту суб'єктів господарської діяльності, а кіберстрахування є одним із інструментів його реалізації. На основі кореляційно-регресійного аналізу визначено, що попит та пропозиція на продукт кіберстрахування буде напряму залежати від індексу кібербезпеки. Досліджено, що, незважаючи на великий попит на продукти кіберстрахування, страхові компанії не готові його повністю покривати через ризиковість збиткової діяльності. Встановлено, що на противагу великому попиту, страховики збільшують страхові тарифи, вводять обмеження на покриття, або взагалі припиняють продавати поліси кіберстрахування. Досліджено основні моделі ціноутворення, які існують на страховому ринку, проведено їх критичний аналіз. Встановлено, що найбільш часто страхові компанії використовують принцип базової ставки. Виявлено, що оцінка ставок є важливою проблемою для продуктів кіберстрахування і виникає через недоступність актуарних даних та невизначеність нормативних стандартів кіберризиків. Серед страхових компаній досі не існує стандартизованого підходу до оцінки тарифів, тому можна спостерігати серед досліджень широкий спектр різних думок і підходів, які не завжди пов'язані одним з одним.

У третьому розділі визначено стримуючі фактори та перспективи розвитку кіберстрахування в Україні з метою захисту від кіберзагроз інтересів фізичних та юридичних осіб. Проаналізовано міжнародний досвід розвитку кіберстрахування, та на його основі визначено можливості його імплементації у вітчизняну практику, а саме як страхові компанії можуть заходити на ринок без великих втрат для свого бізнесу. Доведена необхідність використання перестрахування та катастрофічних облігацій для страхових компаній у новій галузі страхування.

Ключові слова: страховий ринок, страхова послуга, кіберризик, кіберстрахування, кібератака, кібербезпека, кібервідповідальність.

Список публікацій магістра:

1. XVIII Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених Київського національного університету ім. Тараса Шевченка «Шевченківська весна 2020». – Бабенко Ю.Л. Кіберстрахування: сучасний стан та перспективи розвитку.

Шевченківська весна 2020: Сучасні виклики економіки: матеріали XVIII Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених / За заг. ред. А.О. Вітренка: - К., [б.в.], 2020. Частина 1. – С. 5.

2. VIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень». - Пікус Р. В., Бабенко Ю. Л. Теоретичні основи кіберстрахування. / Київ, 2021. – 156 с.

3. The 2nd International scientific and practical conference "Eurasian scientific discussions" (March 13-15, 2022). – Pikus R., Babenko Yu. THE MAIN CYBER THREATS TO BUSINESS THAT A CYBER INSURANCE POLICY CAN COVER. / Editor Komarytskyy M.L. Barca Academy Publishing, Barcelona, Spain. 2022. 165 p.

4. Пікус Р. В., Бабенко Ю. Л. Кіберстрахування: нові можливості для страхового ринку України. Економіка та держава. 2022. № 2. С. 134–140. DOI: 10.32702/2306-6806.2022.2.134

Babenko Y. Development of cyber insurance in Ukraine.

Qualifying master's thesis in specialty 072 Finance, Banking and Insurance. - Department of Banking Insurance and Risk Management, Faculty of Economics, Taras Shevchenko National University of Kyiv, Kyiv, 2022.

The aim of the work is to improve the theoretical foundations and develop practical recommendations for the development of cyber insurance in Ukraine as a tool for financial security of legal entities and individuals.

The first section of the paper clarifies the theoretical and methodological foundations for the definition, content and origins of the concept of "cyber risk" and "cyber insurance", the author's construction of the interpretation of the content according to selected criteria. The content and main tasks of cyber insurance as an effective tool for financing losses due to cyber risks are identified. There are two approaches to the formation of coverage of cyber risks in insurance: cyber liability insurance and property insurance of the consequences of possible cyber attacks. Possible options for cyber liability insurance coverage with the separation of first and third party liability coverage, as well as cyber insurance as a type of property insurance are described. It is determined that the European Directive has a positive impact on the development of the cyber insurance market, namely awareness of potential threats, awareness of the need to improve cybersecurity and provide preventive measures through fines, especially for the Internet market, Internet search engines, cloud computing services.

The second section identifies and analyzes the features of the development of cyber insurance in Ukraine and developed countries. It was found that cybersecurity of systems in the modern information world is an extremely important tool for the protection of economic entities, and cyber insurance is one of the tools for its implementation. Based on correlation-regression analysis, it is determined that the supply and demand for the cyber insurance product will directly depend on the cybersecurity index. It is investigated that, despite the high demand for cyber insurance products, insurance companies are not ready to fully cover it due to the risk of unprofitable activities. It has been established that, in contrast to high demand, insurers are increasing insurance rates, imposing restrictions on coverage, or even ceasing to sell cyber insurance policies. The main pricing models that exist in the insurance market are studied, their critical analysis is carried out. It is established that most often insurance companies use the principle of the base rate. It has been found that rate estimation is an important issue for cybersecurity products and arises from the unavailability of actuarial data and the uncertainty of cyber risk standards. There is still no standardized approach to the assessment of tariffs among insurance companies, so there is a wide range of different opinions and approaches among studies that are not always related to each other.

The third section identifies the deterrents and prospects for the development of cyber insurance in Ukraine in order to protect against cyber threats to the interests of individuals and legal entities. The international experience of cyber insurance development is analyzed, and on its basis the possibilities of its implementation in domestic practice are determined, namely how insurance companies can enter the market without great losses for their business. The necessity of using

reinsurance and catastrophic bonds for insurance companies in a new field of insurance has been proved.

Keywords: insurance market, insurance service, cyber risk, cyber insurance, cyber attack, cybersecurity, cyber responsibility.

List of master's publications:

1. XVIII International scientific-practical conference of students, graduate students and young scientists of Kyiv National University. Taras Shevchenko's "Shevchenko Spring 2020". - Babenko Y. Cyber insurance: current status and prospects. Shevchenko Spring 2020: Modern Challenges of the Economy: Proceedings of the 18th International Scientific and Practical Conference of Students, Postgraduates and Young Scientists / For the general. ed. A.O. Vitrenko: - K., [b.v.], 2020. Part 1. - P. 5.

2. VIII All-Ukrainian scientific-practical conference of students, graduate students and young scientists "United by science: prospects for interdisciplinary research." - Pikus R., Babenko Y. Theoretical foundations of cyber insurance. / Kyiv, 2021. - 156 p.

3. The 2nd International scientific and practical conference “Eurasian scientific discussions” (March 13-15, 2022). - Pikus R., Babenko Y. THE MAIN CYBER THREATS TO BUSINESS THAT A CYBER INSURANCE POLICY CAN COVER. / Editor Komarytskyy ML Barca Academy Publishing, Barcelona, Spain. 2022. 165 p.

4. Picus R, Babenko Y. Cyber insurance: new opportunities for the insurance market of Ukraine. Economy and state. 2022. № 2. S. 134–140. DOI: 10.32702 / 2306-6806.2022.2.134

ЗМІСТ

ВСТУП

Актуальність. Глобальна пандемія, яка розпочала нову еру віддаленої роботи, продемонструвала, що людство як ніколи є надзвичайно вразливим до кібератак, особливо тоді, коли все більше людей та компаній впроваджують використання нових технологій. Компанія, що має цифрові активи, є потенційною жертвою атаки програмою-здирником, злому інформаційних систем, зараження шкідливим програмним забезпеченням або фішингом та інших кібератак. Наслідки кібератак, наприклад, витік даних з серверів, можуть бути дуже істотними і не обмежуються прямими витратами на відновлення пошкодженої техніки.

У зв'язку зі зростанням масштабності кіберзлочинів ризик-менеджмент компаній повинен ввести до свого списку додаткову загрозу, якій раніше не приділяв значної уваги і, як наслідок, розпочати пошук шляхів оптимізації кібербезпеки серед яких - технологічна безпека, ознайомча робота із протидією та профілактикою кіберзлочинів, а також кіберстрахування. Даний вид страхування забезпечує фінансовими можливостями компанію щодо відновлення після великих втрат, повернення попередньої ефективності, дозволяє зберегти платоспроможність та знизити рівень витрат внаслідок простою виробництва, викликаного різного роду кіберзагрозами.

Підвищена зацікавленість та попит у підприємств і бізнесу щодо ринкових інструментів фінансування кібервтрат, особливо в умовах коли Україна і світ все частіше потрапляють під масовий вплив кібератак, актуалізує кіберстрахування, як особливий різновид страхового продукту і для страхових компаній. Тому реагуючи на потреби ринку серед страхових компаній постало завдання відпрацювати сучасну практику кіберстрахування, сформувати перелік страхових продуктів, які можуть виступити такими інструментами фінансування.

Серед досліджень присвячених кіберстрахуванню існують різні напрями, які безпосередньо стосуються мети наукової роботи, її завдань, предмета та об’єкта. До авторів робіт, які безпосередньо досліджували розвиток кіберстрахування в різних країнах світу, в тому числі і в Україні можна віднести наступних вчених: Антоніо Ю. [44], Бем Р. [17], Берк Д. [18], Братюк В. [1], Гудзь. О. [4], Волосович С. [2], Зеллер Г. [31], Кафенбергер Л. [32], Нагайчук Н.[6], Мак А. [15], Мірсанова О. [36], Моді С. [37], Приказюк Н.[7], Третяк Н. [6], Романовський С. [39]. В роботах вказаних авторів, досліджувались питання, які безпосередньо пов’язані із аналізами складових компонентів страхових тарифів, розширенням можливостей для компаній у забезпечені своєї кібербезпеки, аналізах страхових портфелів тощо. Серед українських вчених переважають роботи щодо можливостей та перспектив впровадження нового виду страхування. Практика кіберстрахування в Україні є доволі новою темою дослідження, залишається чимало питань, які вимагають подальших наукових досліджень.

Актуальність вирішення вказаних проблем та недостатній рівень їх теоретико-методичного обґрунтування обумовили вибір теми, мети та завдань дипломної роботи.

Метою роботи є удосконалення теоретичних основ та розробка практичних рекомендацій щодо розвитку кіберстрахування в Україні як інструменту фінансової безпеки юридичних та фізичних осіб.

Для досягнення поставленої мети в роботі були поставлені наступні **завдання**:

- уточнити зміст та еволюцію категорій «кіберризик» та «кіберстрахування»,
- розкрити зміст та основні завдання кіберстрахування,
- виокремити характеристи нормативно-правової бази функціонування кіберстрахування;
- виявити та охарактеризувати особливості ринку кіберстрахування;

- визначити основні тенденції функціонування ринку кіберстрахування на основі його фінансового аналізу;
- узагальнити особливості та виокремити характеристики продукту кіберстрахування;
- охарактеризувати міжнародну практику кіберстрахування та надати пропозиції щодо її реалізація в Україні;
- визначити перспективи впровадження кіберстрахування як фінансового інструменту захисту фізичних та юридичних осіб.

Об'єктом дослідження є ринок кіберстрахування в Україні

Предметом дослідження є теоретичні основи, сучасні тенденції та перспективні напрямки розвитку кіберстрахування в Україні.

При написанні роботи використовувалися наступні **методи**: абстрагування і конкретизація – при уточнені наукових підходів до визначення кіберризиків та їх класифікації; критичний аналіз літературних джерел та наукова абстракція – при розкритті змісту та основних завдань кіберстрахування; системний підхід – при виокремленні нормативно-правової бази функціонування ринку кіберстрахування; аналіз і синтез, порівняльний аналіз – при виявленні особливостей ринку кіберстрахування; економіко-статистичний та графічний – при проведенні фінансового аналізу сучасного стану ринку кіберстрахування в Україні; економіко-математичне моделювання та регресійний аналіз – при узагальнені особливостей та виокремлені характеристик продукту кіберстрахування; аналогія та логічне узагальнення - при узагальненні міжнародного досвіду кіберстрахування та надання пропозиції щодо його реалізації в Україні; абстрагування і конкретизація, оптимізація – при обґрунтуванні напрямів подальшого розвитку та ефектів впровадження кіберстрахування фізичними та юридичними особами.

Інформаційну базу дослідження становили статистичні матеріали Національної асоціації страхових комісарів NAIC [33], Fitch [38], Visiongain [21], Ponemon Institute та IBM Security [19], сайти консалтингових компаній Marsh [24], Woodruff Sawyer [18], сайти міжнародних страхових компаній Allianz [16],

AXA [46], Helvetia Insurance [47], AIG та відповідні наукові статті вітчизняних та зарубіжних вчених.

Практичне значення отриманих результатів. Основні висновки та рекомендації роботи мають практичну цінність, оскільки вони можуть застосовуватися страховими компаніями для просування свої страхових продуктів з кіберстрахування та створення нових конкурентних переваг на ринку страхування.

Апробація результатів дослідження:

1. XVIII Міжнародна науково-практична конференція студентів, аспірантів та молодих вчених Київського національного університету ім. Тараса Шевченка «Шевченківська весна 2020». – Бабенко Ю.Л. Кіберстрахування: сучасний стан та перспективи розвитку. *Шевченківська весна 2020: Сучасні виклики економіки:* матеріали XVIII Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених / За заг. ред. А.О. Вітренка: - К., [б.в.], 2020. Частина 1. – С. 5.
2. VIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Об'єднані наукою: перспективи міждисциплінарних досліджень». - Пікус Р. В., Бабенко Ю. Л. Теоретичні основи кіберстрахування. / Київ, 2021. – 156 с.
3. The 2nd International scientific and practical conference "Eurasian scientific discussions" (March 13-15, 2022). – Pikus R., Babenko Yu. THE MAIN CYBER THREATS TO BUSINESS THAT A CYBER INSURANCE POLICY CAN COVER. / Editor Komarytskyy M.L. Barca Academy Publishing, Barcelona, Spain. 2022. 165 p.
4. Пікус Р. В., Бабенко Ю. Л. Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава*. 2022. № 2. С. 134–140. DOI: 10.32702/2306-6806.2022.2.134

Обсяг основного тексту кваліфікаційної роботи складає 49 сторінки. Список використаних джерел містить 47 найменувань. Робота містить 11 таблиць та 14 рисунків.

Дана робота має таку **структуру**: вступ, три розділи, два підрозділи, висновки, список використаних джерел.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ РОЗВИТКУ КІБЕРСТРАХУВАННЯ

У сучасному технологічному світі кожне підприємство використовує комп'ютери для надсилання, отримання або зберігання електронних даних. Такі дані можуть включати прогнози продажів, податкові записи та іншу інформацію, що належить вашому бізнесу. Якщо дані будуть втрачені, викрадені або пошкоджені через порушення безпеки, заміна або відновлення їх може завдати значних витрат підприємству.

Кожна комп'ютерна система також може містити конфіденційні дані, які належать іншим сторонам, таким як клієнти, працівники або продавці. Якщо хакером викрадені або зламані такі дані, їх власники можуть подати позов до компанії за збитки. Компанія також може понести значні витрати на сповіщення про загрозу даним. Тому підприємства починають захищати свій бізнес від витрат, пов'язаних зі зломом даних, купуючи поліс кіберстрахування.

Головним об'єктом кіберстрахування є кіберризик. Визначення сутності поняття «кіберризик» наведено в роботах різних авторів і вирізняється, насамперед, цілями і підґрунтям. Відповідно до Chief Risk Officer Forum (групи професійних менеджерів з ризику зі страхової галузі) поняття «кіберризики» охоплює наступні позиції:

- будь-який ризик, що виникає внаслідок використання та передачі електронних даних, включаючи такі технологічні засоби, як Інтернет та телекомунікаційні мережі;
- фізичні збитки, які можуть бути завдані кібератаками;
- шахрайство внаслідок неправильного використання даних;
- неправовий доступ до конфіденційної електронної інформації, пов'язаної з фізичними особами, компаніями або урядом [20].

Українські дослідники наводять своє розуміння даної категорії. Наприклад, С. Волосович визначає, що кіберризик – це операційний ризик, який

полягає в отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі [2], а Н. Приказюк розуміє під кіберризиком ймовірність виникнення збитків через збій у системі інформаційних технологій організації [7].

В трактуванні категорії «кіберризик» наведеними науковцями відсутні або результат, або зміст явища, що не має в собі повноцінного описання вказаної категорії. При формуванні власної категорії, ми маємо звернути увагу на суть явища, а саме, що це, як зазначає Н. Приказюк, ймовірність настання, але не збитків, а подій; зміст явища, який докладно описують Chief Risk Officer Forum і полягає в тому, що кіберризики вражають роботу ІТ-систем та кібербезпеку організації через стороннє втручання цифрових та інших електронних технологій; та на результат = настання кіберризику призводить до отримання збитків, руйнування цифрових активів та можливої втрати репутації організації.

Можемо підсумувати, що кіберризик – це ймовірність настання подій, які вражають роботу ІТ-систем та кібербезпеку організації через стороннє втручання цифрових та інших електронних технологій, що призводить до отримання збитків, руйнування цифрових активів та можливої втрати репутації організації.

При з'ясуванні сутності кіберстрахування (або іноді називають такими поняттями як: «страхування кібервідповідальності», «страхування кібербезпеки» або «страхування кіберризиків») науковці звертають увагу на сферу діяльності сучасних технологій. Наприклад, за визначенням Нагайчук Н. кіберстрахування – це страховий продукт, що захищає компанію від ризиків, пов'язаних з використанням мережі Інтернет, а також із ризиками, що відносяться до інформаційних технологій, ІТ-інфраструктури та діяльності підприємства у кіберпросторі [6]. Такої ж думки дотримується і Гудзь О., який характеризує кіберстрахування як страховий продукт, який захищає економічні суб'єкти від ризиків, що відносяться до інформаційно-комунікаційних технологій, використання Інтернет-мережі, ІКТ-інфраструктури та діяльності у кіберпросторі [4].

Німецькі дослідники Р. Бем і Г. Шварц під страхуванням кіберризиків розуміють передачу фінансового ризику, пов’язаного з мережевими та комп’ютерними інцидентами, третіх сторін [17].

У наведених трактуваннях відсутні результати таких категорій, що призводить до неповноцінного прочитання суті поняття. Потрібно звернути увагу на те, які наслідки несуть за собою використання описано виду страхування та який від цього результат. Компанії самостійно несуть відповідальність за свою кібербезпеку, але коли вони застраховані і у випадку кібератаки покриття кібервідповідальності забезпечить вирішальну підтримку, щоб допомогти вашому бізнесу продовжити нормальне функціонування [1].

Порівнявши описані визначення, «кіберстрахування» можна визначити як страховий продукт, який пов'язаний з передачею фінансового ризику третій стороні, тобто страховій компанії для того, щоб допомогти державі, суспільства, суб’єктам господарювання та людині зменшити вплив ризику шляхом компенсації витрат, пов’язаних із потенційно руйнівними наслідками кіберзлочинів, забезпечити захист від збитків, що виникають внаслідок порушення безпеки та конфіденційності [45].

Кіберстрахування покриває збитки, пов'язані з пошкодженням або втратою інформації з ІТ-систем та мереж. Політика, як правило, включає значну допомогу та управління самим інцидентом, що може бути суттєвим при зіткненні з репутаційними збитками або примусовим регулюванням.

Можна виділити два підходи до формування політики покриття кіберризиків.

1) страхування кібервідповідальності;

2) майнове страхування можливих кібератак.

Перший із з них базується на тому, що відповідальність за ризики може покриватися для першої і третьої (тобто сторонньої особи). Покриття кібервідповідальності третьої особи оплачує витрати, які компанія безпосередньо зазнає внаслідок порушення, наприклад, інформування клієнтів про хакерську атаку і застосовуються до претензій, які націлені на об’єкта від

людей або компаній, які отримали збитки внаслідок дій або бездіяльності об’єкта (табл. 1.1). Наприклад, клієнт подає до суду за халатність після того, як хакер викраде його особисті дані з комп'ютерної системи та випустить їх в загальний доступ в Інтернеті [45].

Таблиця 1.1

Можливі варіанти страхового покриття кібервідповідальності

Страхування відповідальності першої особи	**Страхування відповідальності третьої особи**
Витрати на відновлення даних	Мережева безпека та відповідальність за конфіденційність
Втрата доходу або додаткові витрати	
Кібервикрадення / кібершантаж	Електронна відповідальність за медіа
Витрати на реагування (IT-розслідування, сповіщення клієнтів)	Нормативне провадження
Мінімазація репутаційного збитку	Судові збори, штрафи
Юридична допомога: консультація і захист від вимог третіх осіб	

Джерело: складено автором на основі [25, 41].

Другий підхід до формування покриття кіберстрахування базується на видах кібератак та кіберінцидентів, які можуть трапитися із компанією та об’єктами, на які вони впливають. Проаналізувавши угоди про страхування топових європейських, американських та українських компанії, а також практики в наукових роботах, можна виокремити можливі страхові поліси з майнового кіберстрахування (табл 1.2).

В табл. 1.2 подано одним із додаткових покриттів технічна заміна, що включає вартість заміни технічного обладнання. Даний вид покриття підпадає під класифікацію майнового страхування. Проте на страховому ринку відбувається дискусія стосовно включення даного покриття у страховий поліс. Так, як даний тип збитків може бути спричинений операційними помилками незалежно від того, чи вони спричинені технічними збоями, як випадкові, чи шкідливими загрозами, які можуть спричинити кінетичну шкоду. Тому страхові компанії на власний розсуд вирішують необхідність включення даного покриття в страховий поліс, при тому значно збільшуючи вартість покриття [45].

Таблиця 1.2

Поліси майнового кіберстрахування

Поліси кіберстрахування	**Покриття, які забезпечують поліси**
Перерва в процесі виробництва	1.збитки та відшкодування втрачених прибутків в результаті порушення в роботі IT-системи, мережі та веб-сайтів з причини кібератаки (припинення роботи).
Крадіжка активів	1.відшкодування викупної суми, сплаченої вимагачам, за дешифровку заблокованої інформації підприємства; 2. витрати, які понесла компанія, відновлюючи інформацію.
Знищення або шкода будівлям/обладнанню або іншому майну	1. витрати у випадку збою безпеки мережі, які можуть витік даних, зараження зловмисним програмним забезпеченням: юридичні витрати, IT-криміналістика, відновлення даних, експертиза зв'язків з громадськістю. 2. порушення безпеки комп'ютерної системи (Dos- та DDos-атаки, ураження вірусами, знищення, модифікація або видалення інформації).
Соціальна інженерія (нецільова атака)	збитки від втрати грошових коштів і активів страхувальника, що сталися в результаті застосування технологій фішингу, картингу (нецільові атаки).
Технічна заміна	вартість заміни технологічного обладнання, яке стає непридатним при атаці зловмисного програмного забезпечення.

Джерело: складено автором на основі: [18, 25, 41].

Кіберстрахування – це інструмент передачі ризику, який не потрібно розцінювали як забезпечення комп'ютерної безпеки для компанії. Між поняттям «кіберстрахування» та «кібербезпека» існує суттєва різниця. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України»: «кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [10].

Кіберстрахування можна вважати запобіжним заходом кібербезпеки, але за жодних обставин це не повинне розглядатися, як заміна міцної бази безпеки, яка вимагає сучасних технологій кібербезпеки, навчених команд та перевірених

процедур. Якщо не досягти необхідного рівня безпеки, страхувальники можуть відмовитися укладати договір страхування, або підвищити вартість премій.

Зі збільшенням кількості додатків, програмного забезпечення, пристроїв організація стає більш вразливою до кібератак. Так само, як підприємства страхують свій бізнес від фінансових ризиків, стихійних лих та фізичних ризиків, їм також необхідно страхувати кіберризики.

Кіберстрахування може відігравати ключову роль у підтримці бізнесу будь-яких розмірів, воно може забезпечити стійкість бізнесу до порушень кібербезпеки, а в найгіршому випадку допомогти відновити бізнес після масштабних кібератак.

Термін «кіберстрахування» зародився в США і такий продукт в основному зосереджувався на зобов'язаннях третьої сторони, які пов'язані з порушенням даних та конфіденційності, включаючи витрати на сповіщення. Такий акцент обумовлений порушенням законів про сповіщення, прийняті у більшості штатів США, які передбачають, що бізнес повинен повідомити про загрози лише постраждалих сторін, якщо є докази, які обґрунтовано припускають, що їх особисті дані будуть використовуватися зловмисно.

Історично це відрізняється від Європи, де натомість на першому місці зосереджено покриття витрат на переривання бізнесу внаслідок кіберінцидентів.

Однак ця невідповідність за останні кілька років зменшилась і і тепер регулюється положенням про захист даних General Data Protection Regulation (GDPR) [28], прийнятим Європейським союзом, який почав діяти 25 травня 2018 року. Цей Регламент захищає основні права та свободи фізичних осіб і, зокрема, їхнє право на захист персональних даних.

У 2016 році в рамках стратегії кібербезпеки ЄС Європейська Комісія запропонувала директиву щодо мережевої та інформаційної безпеки ЄС (NIS: Directive on security of network and information systems). Директива NIS є першою частиною законодавства про кібербезпеку в усьому ЄС. Метою є підвищення кібербезпеки. NIS призначений для встановлення загального рівня безпеки мережевих та інформаційних систем.

NIS розшифровується як «Правила мережевих та інформаційних систем 2018». Вони випливають із європейського права і реалізують Європейську директиву 2016/1148 щодо високого загального рівня безпеки мережевих та інформаційних систем по всьому Європейському Союзу [27].

NIS стосується безпеки мережевих та інформаційних систем та цифрових даних всередині них, тоді як GDPR стосується обробки персональних даних.

Дані директиви мають позитивний вплив на розвиток ринку кіберстрахування, а саме інформованості щодо потенційних загроз, усвідомлення необхідності удосконалення системи кібербезпеки та забезпечення превентивних заходів через введені штрафи, особливо для тих галузей, які чітко визначені у директиві NIS: 1) інтернет-ринок; 2) пошукова система в Інтернеті 3) служби хмарних обчислень [27].

Оскільки Україна не входить до ЄС, Директива NIS не є зобов'язуючою, однак вона служить настановою з питань належної практики. Деякі з її положень були добровільно впроваджені в українському законодавстві, проте інші залишаються без уваги.

У 2005 році Україна ратифікувала Будапештську конвенцію - перший міжнародний договір, який прагне вирішити питання кіберзлочинності шляхом гармонізації національного законодавства, вдосконалення методик розслідування та посилення співпраці між країнами [8].

Окрім цього, у 2016 році було прийнято Стратегію кібербезпеки України, яка визначає пріоритети та напрямки кібербезпеки і є важливим структурним елементом для формування політики у сфері кібербезпеки, яка відповідатиме світовому рівню [11]. Для реалізації Стратегії кібербезпеки Парламент України ухвалив Закон «Про основні засади забезпечення кібербезпеки України» – основний законодавчий акт, що встановлює правові рамки для системи кібербезпеки [10]. Стратегія 2016 року була розрахована на п'ять років і несла в собі низку важливих положень, проте значно широкі формування, які не мають конкретно визначеної кінцевої мети та низька ефективність вказаних заходів не дали достатнього поштовху для активної її реалізації. Нова Стратегія

кібербезпеки України від 26 серпня 2021 року [12] має вирішити основні проблемні завдання попередньої стратегії і звернути увагу на сучасні тенденції (виклики) ринку, а саме:

- увага до кібербезпеки у міжнародній конкуренції;
- швидкі прогресуючі зміни інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;
- вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинило стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;
- упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою [14].

Саме на ці тенденції потрібно звертати увагу страховикам, формуючи поліс кіберстрахування та при вирахуванні його вразливих моментів.

Кіберстрахування в своєму полісі містить також відповідальність за нерозголошення персональної інформації та збереження захисту даних. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [9] в своїх положеннях розмежовує обов’язки щодо захисту інформації власника систем і може бути використаний як основа для формування договору про кіберстрахування в розділі страхування захисту персональних даних.

Отже, кіберстрахування, на відміну від традиційного страхування, призначене для задоволення потреб компаній у цифрову епоху. Кожна компанія стикається з кіберризиками незалежно від їх розміру, але чим більші її розміри, тим більше й областей вразливості. Поліс кіберстрахування призначений допомогти організаціям пом'якшити вплив ризику шляхом компенсації витрат, пов’язаних із відновленням після порушень в кібербезпеці або подібних подій. Покриття кібервідповідальності може забезпечити вирішальну підтримку, щоб допомогти бізнесу залишатися на плаву.

РОЗДІЛ 2
СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРСТРАХУВАННЯ В УКРАЇНІ

2.1 Тенденції розвитку ринку кіберстрахування

У 2020 році кібератаки займають перше місце (39% опитаних респондентів) в барометрі Allianz Risk [16]. В 2019 році серед найбільших ризиків для компаній вони займали друге місце. Якщо порівняти це з 2013 роком, коли він зайняв 15 місце із лише 6% відповідей, стає зрозуміло як швидко зросла обізнаність про кіберзагрозу, обумовлену зростаючою залежністю компаній від своїх даних та IT-систем.

У 2021 класифікація ризиків різко змінила свою позицію, що пов'язано із виходом в топ-ризиків ризику Пандемічного спалаху, який до цього був на 17 місці за рейтингом 2020 року. Відповідно ризик кібератаки опинився на 3-ому місці, проте із більшим процентом (40%), порівнюючи із попереднім 2020 роком (39%). У 2022 році ризик кіберзагроз повернувся до своєї лідируючої позиції, так як фізичні і юридичні особи змогли більше пристосуватися до викликів пандемії Covid-19.

Дослідження Clark School в Університеті Меріленду було одним із перших, які змогли кількісно оцінити майже постійну швидкість хакерських атак на комп'ютери з доступом до Інтернету. В середньому кожні 39 секунд здійснюється певного роду кібератака [34]. Деякі з них успішно локалізуються, деякі повністю знешкоджуються, але велика кількість завдає значного збитку фізичним та юридичним особам. На рис. 2.1 відображено середню вартість завданих збитків від кіберзагроз. Як бачимо, з кожним роком вони тільки зростають і бізнес зазнає все значніших втрат. Одним із варіантів мінімізації цих втрат є кіберстрахування.

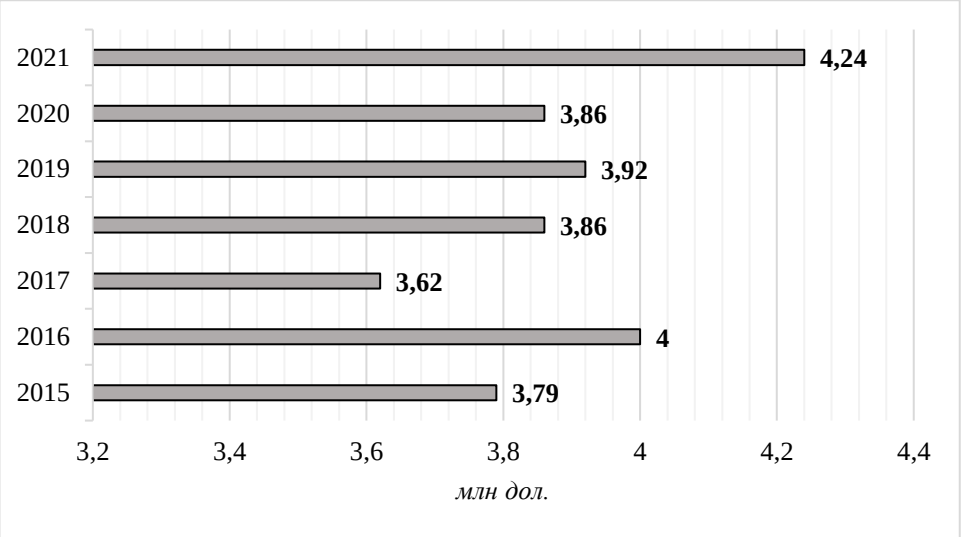

Рис. 2.1 Середня вартість злому даних, млн дол. [19]

За аналізом статистики кібербезпеки 2021 року від PurpleSec LLC кіберзлочинність зросла на 600% через пандемію COVID-19. Унаслідок спалаху COVID-19 кіберзлочинці підняли складні схеми електронної пошти для фішингу. Кіберзлочинці представляються як представники Центру з контролю та профілактики захворювань у США (CDC) або Всесвітньої організації охорони здоров'я (ВООЗ). Україна, в тому числі також ввійшла в список країн, на які найбільше були направлені кібератаки (6% успішного враження шкідливим програмним забезпеченням) (рис. 2.2).

Рис. 2.2 Рейтинг країн за цілеспрямованими кібератаками, %.

Джерело: складено автором на основі: [23]

На рис. 2.3 відображено прогноз розвитку кіберстрахування до 2030 року зроблений консалтинговою компанією Visiongrain. Найбільший приріст по відношенню до попереднього року відбудеться у 2023 році і тенденція буде постійно збільшуватись. Серед країн Європи найбільший розвиток припадає на Німеччину, Велика Британія поступиться їй другим місцем, а згодом і третім для Франції. Росія і Італія залишились аутсайдерами у дослідженні і їхній розвиток буде незначним.

Для того, щоб страхові компанії могли розвивати дану галузь страхування, вводити нові продукти, або розвивати існуючі, необхідно окрім прогнозованих тенденцій збільшення страхових премій і кібератак, зрозуміти прихильність компаній до посилення своєї кібербезпеки, в тому числі і передачі кіберризиків на страхування.

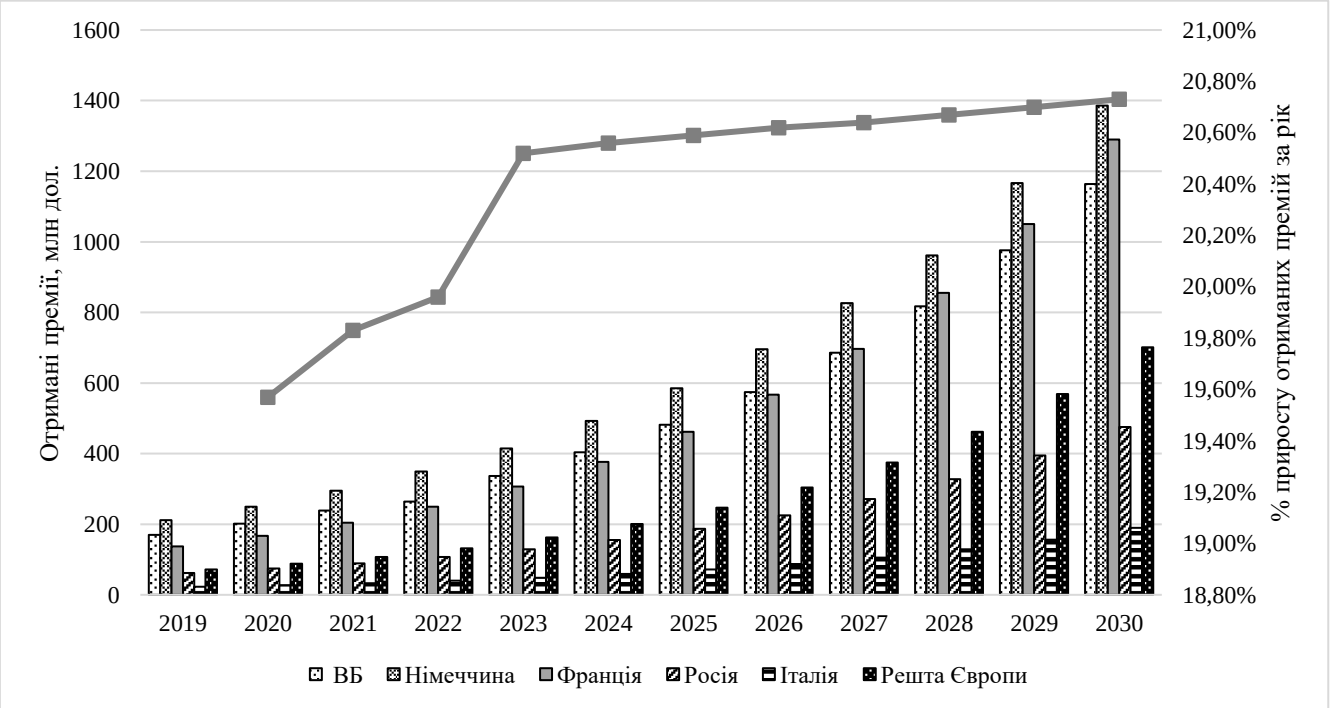

Рис. 2.3 Прогноз розвитку ринку кіберстрахування на 2020-2030 рр. [21]

Страхові компанії України також починають впроваджувати поліси страхування кіберризиків, проте рівень отриманих премій свідчить, що результати поки що не високі. Насамперед потрібно оцінити рівень сприйняття

компаніями і населенням країни такого типу страхування. Тенденція кількості кібератак та наслідків, які слідують за ними провокує компанії забезпечити захист свої діяльності, тобто застрахувати свої ризики. Тому для того, щоб дослідити сприйняття компаніями кібербезпеки необхідно побудувати модель, яка буде показувати тенденцію кіберзагроз.

Так, як дані по українському ринку кібербезпеки є обмеженими, а країни Європи починають їх розкривати у відповідності з Загальним регламентом про захист даних (General Data Protection Regulation, GDPR) для аналізу беремо 27 країн Європейського Союзу. В даній моделі не берем до уваги ринок США, так як тенденції їхнього розвитку набагато вищі і не актуальні для сьогоднішнього стану ринку України. Зі звіту Mordor Intelligence «Глобальний ринок кібербезпеки – зростання, тенденції, вплив Covid-19 та прогнози (2022–2027)» [29] Україна, як і вся Європа перебувають у середньому рівні розвитку своєї кібербезпеки, що додатково підтверджує подібність тенденцій ринку і необхідність їх цілісного аналізу.

Між динамікою показників кібератак та кіберстрахових покриттів існує пряма тенденція: зі збільшення кількості кібератак, збільшуються і пропозиції на ринку страхування кіберризиків. Проте страховим компаніям необхідно обережно поводитися з такими тенденціями, тому що ризик накопичення може спричинити тільки великі виплати для страхових компаній. Наприклад, одна масова кібератака, така як вірус Petya, може вивести із ладу ряд крупних компаній. Припустимо, що більшість із цих компаній були застраховані в одній страховій компанії. Тоді їм одночасно необхідно покрити масштабні страхові відшкодування.

Для того, щоб уникнути подібних ситуацій, компанії повинні забезпечувати засоби захисту своїх айті-систем. Такі умови є регламентованими на рівні законодавства країни і існують технічні вимоги до програмних забезпечень та служб захисту. Щоб оцінити готовність країн до запобігання реалізації фундаментальних кіберзагроз, управління кіберінцидентами,

злочинами та масштабними кіберкризами існує Глобальний індекс кібербезпеки GCI.

Тому для того, щоб компаніям можна було брати до уваги аналіз тенденцій кібератак, необхідно щоб показник кількості кібератак на країну корелював із індексом кібербезпеки. Перевірити можемо це за допомогою моделі кореляційно-регресійного аналізу.

Також перевіримо і кореляцію між такими показниками, як:

- VICTIM - компанії, що вже зазнали впливу кібератак (попередній період), адже в поточному кількість кібератак має бути менше, так як компанії повинні забезпечити якісніший захист своїх систем безпеки;
- Malware - середньорічний показник зараження зловмисним програмним забезпеченням (подібна тенденція впливу, як і з показником VICTIM);
- XNODE - кількість відкритих підключень до Інтернету в кожній країні (чим більш відкритих підключень, ти більша і кількість кібератак) - на цей показник особливо потрібно звернути увагу страховим компаніям при розрахунку вартості страхових премій.

На основі досліджуваних показників будуємо модель за допомогою кореляційно-регресійного аналізу програмному комплексі MS Excel. В результаті розв’язання поставленої мети факторного кореляційно-регресійного аналізу, було побудовано економіко-математична модель, яка має наступний вигляд:

$$Y = 50{,}14 + 0{,}25\ X1 - 0{,}24\ X2 + 0{,}26\ X3 - 0{,}27\ X4$$

Для перевірки зв’язку між досліджуваним показником (Y) та факторами, які на нього впливають (X) побудована кореляційна матриця (табл. 2.1). У роботі представлений кінцевий варіант матриці, показники якої мають вплив на Y. При аналізі було досліджено 8 факторів, проте 4 із них не мали впливу на кінцевий показник, тому були видалені з моделі.

Таблиця 2.1

Кореляційна матриця

	Attack	Victim	GCI	XNODE	Malware
Attack	1				
Victim	-0,58562	1			
GCI	-0,83651	0,6014	1		
XNODE	0,661461	-0,57461	-0,41123	1	
Malware	-0,61046	0,399686	0,176679	-0,35035	1

Джерело: складено автором на основі Додатку 1

Показники регресійного аналізу (табл.2.2) показують, що кореляціями між факторами є велика і показники пояснюють Y на 99%. Це можна пояснити тим, що деякі фактори мають прямий вплив на показник кібератак. За правилами побудови моделей такі фактори варто виключити, але через обмеженість даних для початкового аналізу їх можна врахувати, а з часом при вдосконаленні моделі варто виключити, або замінити іншими. Стандартна похибка менше 30%, отже модель є точною.

Таблиця 2.2

Показники регресійної статистики

Regression Statistics	
Multiple R	0,9977
R Square	0,9954
Adjusted R Square	0,9946
Standard Error	0,2995
Observations	27

Джерело: складено автором на основі Додатку 1

Показники дисперсії, значущості F ($F > F_c$) та показника F-статистики (<0.05) свідчить про достатній рівень достовірності результатів оцінювання (табл. 2.3).

Таблиця 2.3

Показники, що характеризують достовірність моделі регресії

	df	*SS*	*MS*	*F*	*Significance F*
Regression	4	454,6499079	113,6625	1266,356	1,34668E-26
Residual	23	2,064377785	0,089756		
Total	27	456,7142857			

Джерело: складено автором на основі Додатку 1

Всі коефіцієнти моделі підтверджують правило |tрозр |> tкритич (табл. 2.4). Модель також є надійною, так як всі Р-значення <0,05. Це означає, що модель є достатньо адекватною, статистично значимою і може використовуватися для прогнозування.

Результати дослідження свідчать про наявність кореляції вибраних факторів з основними дослідженими тенденціями розвитку кібератак. Отже, гіпотеза про можливість використання страховими компанія показника тенденції кібератак підтверджується.

Таблиця 2.4

Показники, що характеризують достовірність моделі регресії

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*
Intercept	50,14467831	0,590271223	84,95193	3,09E-30	48,92360925	51,36574737
Victim	0,245680396	0,020123476	12,20865	1,57E-11	0,204051813	0,287308979
GCI	-0,244335181	0,005620128	-43,475	1,38E-23	-0,255961302	-0,23270906
Malware	0,25959656	0,013880957	18,70163	2,08E-15	0,230881612	0,288311508
XNODE	-0,266484196	0,009036979	-29,4882	8,89E-20	-0,285178611	-0,247789781

Джерело: складено автором на основі Додатку 1

В цілому результати проведення регресійного аналізу факторів, що характеризують розвиток кібератак, можуть бути уточнені за рахунок розширення і забезпечення адекватності вхідних статистичних даних.

Отже, сприйняття населенням та компаніями кіберстрахування, як інструменту кібербезпеки напряму залежить від тенденції розвитку кіберзагроз. З кожним роком все більше компаній розуміють, що загроза бути атакованими

кіберінцидентами зростає в геометричному порядку, тому все більше компаній готові придбати поліси кіберстрахування. Страховики розуміючи збільшення попиту на ринку відразу готові такі послуги надавати.

2.2 Особливості функціонування ринку кіберстрахування

Зі збільшенням кількості та вартості кіберінцидентів у всьому світі все більше компаній визнають, що вони не застраховані від атак, і згодом бачать більшу користь у кіберстрахуванні. За даними Національної асоціації страхових комісарів (NAIC), кількість чинних полісів кіберстрахування зросла на 21,3% з 2019 по 2020 рік [33]. Зростання відбувалось, як за рахунок автономних премій, так і премій у складі інших видів страхування (найпоширеніший варіант – майнове страхування).

Зростання прямих премій з кіберстрахування значно пришвидшилося в 2020 році, і такий імпульс зберігся і в 2021 року (рис. 2.4). Автономні та прямі премії у пакетних полісах з кіберстрахування збільшились більш ніж на 22% у 2020 році приблизно до 2,7 мільярда доларів, згідно з даними, зібраними з аналізу полісів кіберстрахування поданих у статутних фінансових звітах страхових компаній [38].

Прямі премії за автономне кіберпокриття зросли за 2020 рік на 29%, а у 2021 році на 92%, що відображає зростаючий попит на конкретний кіберзахист та зацікавленість страховиків у зменшенні неоднозначності у покритті щодо кіберризиків, включених у пакетну політику. Попит зумовлений потребою у експертах з управління ризиками та страховому захисті фірмами будь-якого розміру внаслідок випадків вторгнення в мережі, крадіжки даних та інцидентів з вимогами, які значно зросли за останні два роки.

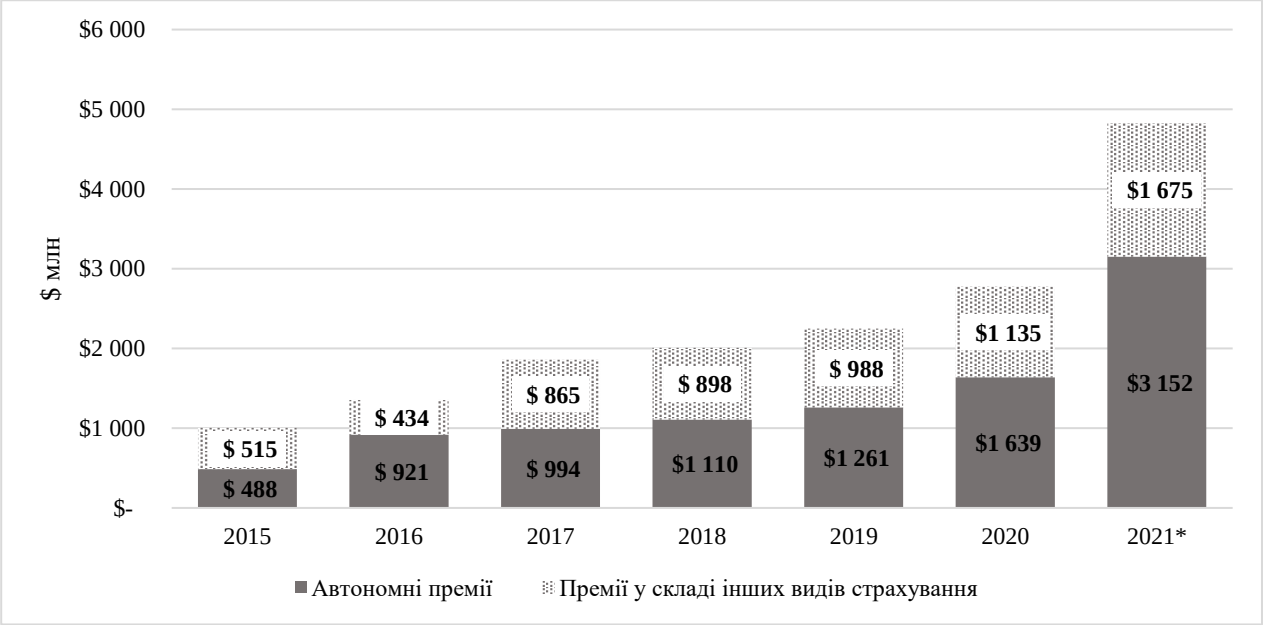

Рис. 2.4 Виплачені премії у галузі кіберстрахування, 2015-2021 рр.. [3]

***-** *дані можуть бути неповними по закриттю року*

Як бачимо, попит на кіберстрахування збільшується, що підтверджує і висунута нами гіпотеза у розділі 2.1. Проте, якщо детально проаналізувати ринок, де кіберстрахування вже протягом декількох років розвивалось, то тенденція свідчить, що незважаючи на те, що попит збільшується, пропозиція кіберстрахових полісів зменшується, оскільки страховики та перестраховики роблять крок назад і переоцінюють свої ризики. Зі збільшенням кількості кіберінцидентів і поданих претензій галузь стала менш прибутковою. За оцінками рейтингового агентства Fitch, виплати страхових компаній за претензіями, відомі як коефіцієнт прямих збитків, підскочили з 47 центів за кожен долар зароблених премій у 2019 році до 73 центів у 2020 році [38]. Тим не менш, у 2021 році зростання зробленої премії перевищило зміну понесених збитків, а коефіцієнт автономних кібервтрат покращився до 65% з 72% роком раніше (рис. 2.5).

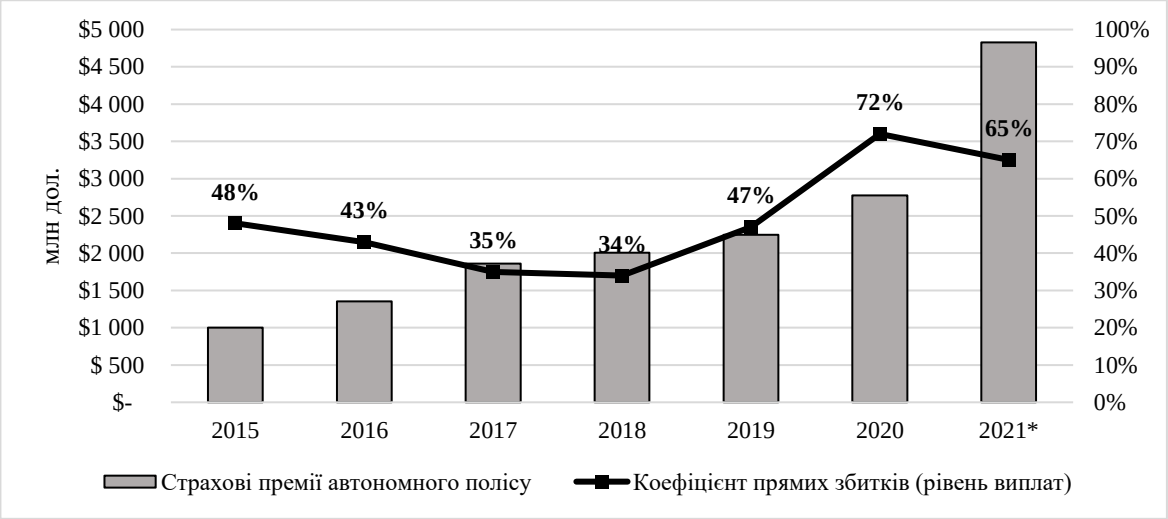

Рис. 2.5 Рівень виплат страхування кіберризиків, 2015-2021 рр.

***-** *дані можуть бути неповними по закриттю року*

Джерело: складено автором на основі: [3]

З таблиці 2.5 бачимо, що деякі страхові групи США, які перебувають в рейтингу найкращих страхових компаній за полісом кіберстрахування також підпадають під ризики втрат в зв'язку з значними загрозами кіберінцидентів. У таблиці виділені AMERICAN INTRNL GRP, CNA INS GRP, SOMPO GRP рівень втрат яких перевищує 100%, зо свідчить про те, що в даному виді страхування їх діяльність є збитковою і неефективною.

Таблиця 2.5

Рейтинг страхових груп США за підписаними преміями

2020 РАНГ	2019 РАНГ	НАЗВА ГРУПИ	ПРЯМІ ПРЕМІЇ, $	РІВЕНЬ ВИПЛАТ, %	ДОЛЯ РИНКУ
1	1	CHUBB LTD GRP	404 144 104	61%	14.7%
2	2	AXA INS GRP	293 025 192	98.2%	10.6%
3	3	AMERICAN INTRNL GRP	228 424 711	**100.6%**	8.3%
4	4	ST PAUL TRAVELERS GRP	206 817 208	85.5%	7.5%
5	5	BEAZLEY GRP	177 746 192	47.9%	6.5%
6	6	AXIS CAPITAL GRP	133 549 784	46.2%	4.8%
7	7	CNA INS GRP	119 612 168	**105.7%**	4.3%
8	10	FAIRFAX FINANCIAL	108 687 558	55.7%	3.9%
9	11	HARTFORD FIRE 7 CAS GRP	102 864 503	25.4%	3.7%
10	8	BCS INS GRP	86 582 699	59.1%	3.1%
11	14	TOKIO MARINE HOLDINGS INC GRP	78 160 355	51.1%	2.8%
12	12	SOMPO GRP	72 588 641	**114.1%**	2.6%
13	13	ZURICH INS GRP	64 430 818	40.4%	2.3%
14	9	LIBERTY MUT GRP	41 856 727	30%	1.5%

Продовження табл. 2.5

15	18	APOLLO GLOBAL MGMT GRP	39 338 993	29.6%	1.4%
16	15	BERKSHIRE HATHAWAY	37 366 878	25.8%	1.4%
17	19	MARKEL CORP GRP	29 736 405	38%	1.1%
18	28	EVEREST REIN HOL INC	28 173 404	48%	1%
19	17	CINCINATTI FNCL GRP	24 888 476	24.6%	0.9%
20	25	SWISS RE GRP	23 654 519	42.6%	0.9%

Джерело: [33].

Ставки премій для кіберпокриття різко зросли в 2020 році (рис. 2.6) у відповідь на погіршення досвіду по середніх ставках премій за поновлення кібербезпеки за попередні роки на 11% в порівнянні з аналогічним періодом. У 2021 році тенденція росту ставки тільки підвищилась, як реакція на збільшення загроз з боку кіберінцидентів. Дослідження Ради страхових брокерів та агентів передбачає, що таке тенденція буде продовжуватися і на наступні періоди [3].

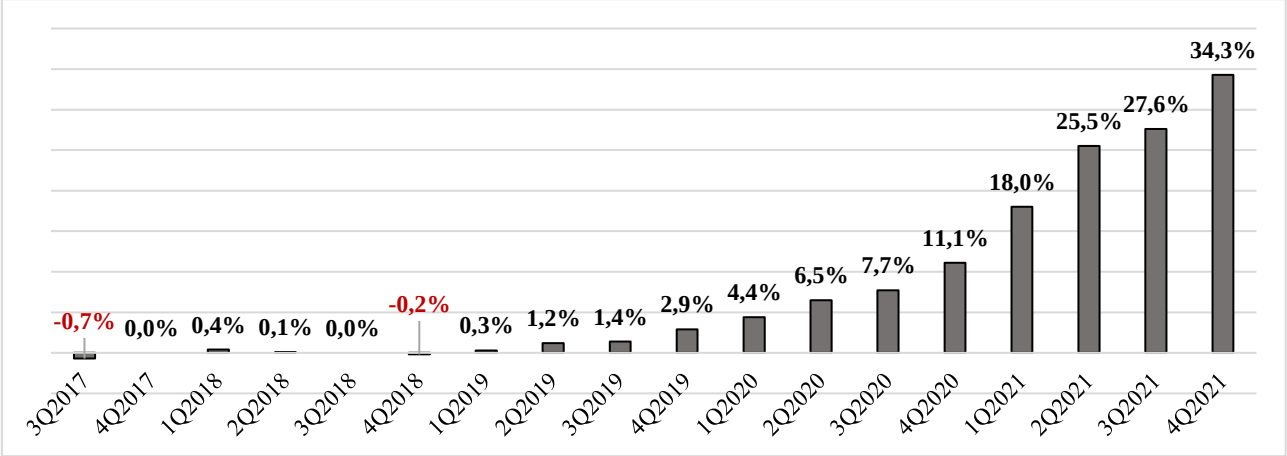

Рис. 2.6 Зміна страхових тарифів за поліси страхування кіберризиків 2017-2021 рр, %

Джерело: складено автором на основі: [3, 38].

Зменшення пропозиції на ринку кіберстрахування через значні рівні втрат страхових компаній містить в собі декілька причин.

Кіберризик не лише впливає на окремі фінансові установи, але має і важливий *системний вимір*. Всесвітній економічний форум (ВЕФ) визначає системний кіберризик як ризик того, що кіберподія (атака (-и) чи інші

несприятливі події) на окремий компонент критичної інфраструктури екосистеми спричинить значну затримку, зрив, порушення або втрати, такі, що впливають не тільки на початковий компонент, але і на наслідки, що також наступають на пов'язані (логічно та / або географічно) компоненти екосистеми, що призводить до значних негативних наслідків для здоров'я населення чи безпеки, економічної безпеки та національної безпеки [32].

Системний ризик виникає внаслідок концентрації ризику, кореляції ризику та посилення шоку. Наприклад, певні системи, включаючи центральні клірингові платформи (CCP) та системи передачі, такі як SWIFT (міжнародна міжбанківська система передачі інформації та здійснення платежів), є ключовими центрами фінансової системи. Хоча вони забезпечують стандартизацію та безпеку глобальних фінансових послуг, вони також створюють ризик концентрації через низьку зовнішню надмірність. Їхні послуги не можуть бути легко замінені іншими установами, оскільки, хоча системи фінансової інфраструктури є технічно надлишковими, їх функції не виконуються. Тривалість простою або дефолт може вплинути на оплату, кліринг та врегулювання фінансових операцій з негативними зовнішніми наслідками, піддаючи фінансові установи, ринки та учасників несподіваних потрясінь. Міжзв'язки, що охоплюють фінансову систему, дозволяють широко розповсюджуватись хакерським атакам та потенційно набувають системного характеру.

Так, прикладом такого інциденту була атака на український банк (назва якого не розголошується з міркувань конфіденційності) через систему SWIFT, про що повідомляється в телеграмі НБУ №56-0031/37708, в результаті якої банк втратив 10 млн доларів США [5].

Кіберстрахування продовжує представляти собою частину загального ризикового ризику для галузі страхування кіберризиків та окремих страховиків. Велика непередбачена кіберподія, така як масове вторгнення в хмарне середовище або атака на інфраструктуру, може призвести до значних фізичних збитків, які можуть спричинити тиск на рівні капіталу та індивідуальні рейтинги.

Оскільки кіберіндустрія все ще *є відносно новою сферою, якій бракує історичних даних*, так як загрози продовжують постійно розвиватися, страховикам важко виправдати збільшення премій. Наприклад, щодо природної небезпеки ми маємо історичні дані про погоду, які допомагають нам передбачити, що станеться з ураганом чи цунамі, тоді як для порівняння ми ледве маємо дані кіберстрахування за 10-12 років. Підсилюється небезпека тим, що кіберзагроза створена людиною та постійно розвивається. Крім того, існує багато рівнів підключених і взаємопов'язаних технологій, кожна з яких має свої особливості, як-от програмне забезпечення, апаратне забезпечення, Інтернет речей, віддалений моніторинг тощо.

Сьогодні, крім нормативних рекомендацій, *не існує остаточного методу розрахунку страхових премій* чи прозорості щодо того, як страховики виправдовують підвищення своїх премій, вартості перестрахування та інших надбавок. Наприклад, страховики, які оформили поліси кібервідповідальності на 5 мільйонів доларів минулого року, скоротили до лімітів від 1 до 3 мільйонів доларів у 2021 році, згідно зі звітом Служби розміщення ризиків (RPS) США. Так само, як повідомляє XL Net, багато компаній зіткнулися з підвищенням премії за кіберстрахування від 75% до понад 1000%.

З іншого боку, організації підприємств, які досліджують кіберстрахування, не знають про рівень ризику, з яким вони стикаються, і не можуть точно розрахувати фінансовий ризик, який вони потенційно можуть передати, порівняно з необхідною сумою страхування. Підприємства не визначили ні свою схильність до кіберризиків, ні рівень толерантності, оскільки вони ніколи *не вимірювали реального фінансового впливу* вторгнення в дані компаній, реагування на інциденти та пов'язані із цим перерви у бізнесі. На сьогоднішній день оцінки кібербезпеки покладалися на поточні, дезінтегровані та випадкові процедури або аудити, які дають сторінки суб'єктивних звітів, які мало хто може зрозуміти чи контекстуалізувати. Хоча ці звіти викривають уразливі місця та дають уявлення про потенційні індикатори компромісу, вони не інформують організацію про фактичний рівень кіберризику [37].

Вплив ризику суттєво змінився внаслідок *реакції на пандемію коронавірусу*. Широкий перехід до віддаленої роботи, а також посилення втручань від фішинг-листів та інших засобів додали напруги системам мережевої безпеки. Найслабшими ланками кібербезпеки є співробітники. Більшість атак спочатку ініціюються через фішинг, спробу потенційних хакерів поділитися особистою інформацією, як-от паролі, логіни та іншу інформацію через небажані електронні листи чи інші форми контакту. Якщо співробітник помилково відкриє один із цих листів, натисне шкідливе посилання або обмінюється особистою інформацією з кіберзлочинцем, то всю компанію можна швидко та легко зламати.

З рис. 2.7 ми бачимо, що чим більша компанія за кількістю працівників, тим вона вразливіша до кіберзагроз. Відповідно, власникам бізнесу необхідно це враховувати під час укладення договору кіберстрахування та вжиття превентивних заходів кібербезпеки. Але більшість зусиль щодо безпеки малих і середніх підприємств у кращому випадку є номінальними. Малі компанії працюють з обмеженими бюджетами, а продукти кібербезпеки не завжди в пріоритеті. Здебільшого вони використовують безкоштовні інструменти кібербезпеки, які не можуть належним чином захистити їхній бізнес.

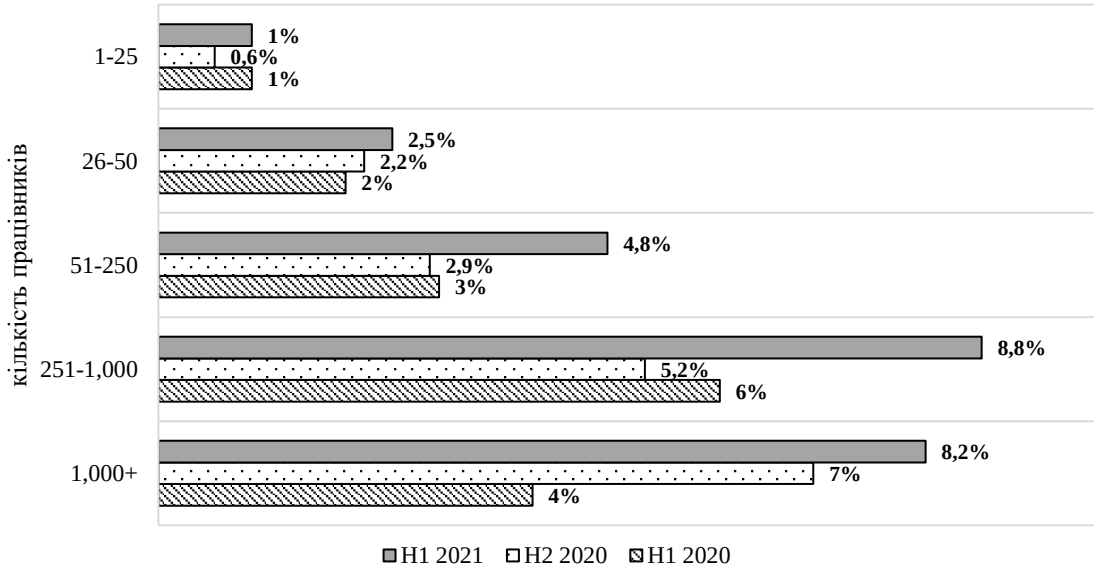

Рис. 2.7 Частота претензій страхових виплат за розміром компанії (кількість працівників), % [35]

З 2020 року організації були змушені продовжувати працювати у віддаленому робочому середовищі, в той час як суб'єкти кіберзагроз продовжували працювати, використовуючи притаманні недоліки безпеки даних. Ця проблема знайшла відображення в дослідженні Ponemon-IBM про вартість злому даних за 2021 рік, що показало кореляцію між збільшенням віддаленої робочої сили та збільшення вартості вторгнення в дані компаній (рис 2.9).

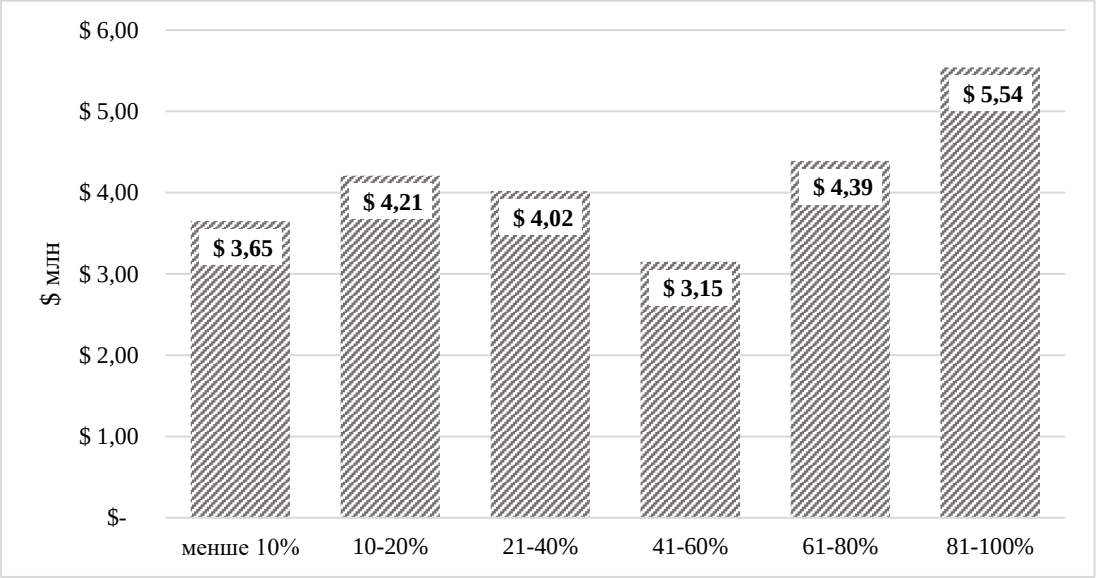

Рис. 2.9 Середня вартість кіберпорушень в залежності від частки співробітників, які працюють віддалено [23]

Отже, незважаючи на те, що попит на ринку кіберстрахування значно зростає з кожним роком, страхові компанії не поспішають перекладати на себе ризики. Фінансові наслідки при порушенні безпеки ведення бізнесу чи даних клієнтів можуть бути величезними. Виникає необхідність не лише захисних заходів для запобігання кібератакам, а й контролю за збитками, судовими зборами та управлінням ризиками після порушення. Зважаючи на такий широк спектр поставлених завдань для страхових компаній, вартість існуючого покриття кіберризиків на страховому ринку перевищує можливості своїх клієнтів.

2.3 Методи формування страхового тарифу кіберстрахування

З математичної та актуарної точки зору, вражає, що для кіберстрахування, нового та динамічного типу ризику, незрозумілі частота та серйозність можливих втрат від кіберподій. Не тільки відсутність даних є головною проблемою для страхових менеджерів та емпіричних дослідників, але динамічний характер кіберризику також несе в собі величезний ризик змін. Дані про кібервтрати обмежені, а сам ризик дуже динамічний. Тому не дивно, що не існує набору моделей, які б достатньо відображали властивості цього нового класу ризику. Розробка моделей кіберризиків не тільки допоможе компаніям вдосконалити управління кіберризиками, але й сприятиме появі вдосконаленого страхового ринку.

Дві проблеми, які часто постають перед страховиками - це: як можуть виглядати екстремальні кіберсценарії та яка структура залежності між кібервтратами. Багато експертів побоюються, що в деяких випадках кібервтрати є великими і дуже корелюються, наприклад, тому що всі компанії використовують одне і те ж програмне забезпечення. Такий ризик для страхових компаній називається «ризик накопичення». У разі кібератаки відразу не одна, а декілька компаній виставлять претензії до страхових компаній і їй необхідно їх виплатити.

Якщо кіберзбитки мають великі ризики, виникає питання про те, наскільки можлива диверсифікація кіберризиків або чи існує недиверсифікаційна пастка (як це зафіксовано для інших катастрофічних ризиків). Також варто відзначити, що сьогодні основна увага в базах даних приділяється порушенням даних та даних США; інформації щодо інших видів ризику чи інших країн є доволі мізерною.

Ця ситуація може покращитися в найближчі роки із впровадженням нових правил захисту даних в Європейському Союзі, які також включають обов'язкові вимоги щодо повідомлення про деякі кіберінциденти. Ці вимоги щодо сповіщення не лише створюватимуть можливість розширених даних для

актуаріїв та дослідників, але також можуть заохотити осіб, які приймають рішення, інвестувати кошти в кіберзахист та кіберстрахування.

Важливою проблемою страховиків є те, як в таких швидко розвиваючих подіях обрахувати вартість страхових премій та відсотки відшкодування, щоб вберегти свій бізнес від ризиків накопичення, некоректної оцінки та ідентифікації. Станом на сьогодні не існує стандартизованого розрахунку вартості кіберстрахування, актуарних таблиць або моделей, кожна із страхових компаній довіряє своєму власному досвіду.

Для розрахунку вартості страхових премій розрізняють «ціноутворення за фіксованою ставкою» та «ціноутворення за базовою ставкою». Підхід до ціноутворення за єдиною ставкою, як випливає з назви, забезпечує єдину ставку для всіх страхувальників, незалежно від їх розміру, або будь-якого конкретного контролю безпеки страхувальником, тоді як підхід до ціноутворення за базовою ставкою використовує низку таблиць і модифікаторів пошуку для обчислення премію (наприклад, ліміти, утримання, історія претензій тощо) та галузі заявника.

Більшість страхових компаній для розрахунку премій за страхування для кіберстрахування використовують модель ціноутворення базової ставки. Тобто базовий внесок оцінюється як функція щорічних доходів або активів страхувальника (або, за деякими нішевими продуктами, кількості працівників чи аутсорсингові проекти). Потім цей базовий внесок множиться на змінні, що стосуються стандартних страхових та галузевих факторів.

Остаточна премія =

(Базова ставка відповідальності 3 сторони) + (Базова ставка витрат 1 сторони)

x (Граничний коефіцієнт)

x (Фактор утримування)

x (Фактор класифікації даних)

x (Фактор інфраструктури безпеки)

x (Управління, ризик та коефіцієнт відповідності)

x (Фактор контролю платіжної картки)

x (Фактор управління медіа)

x (Фактор втрати комп’ютерної системи, якщо він застосовується)

x (Фактор претензії / Історія втрат) [39].

Фактор, який надає найбільший вплив на премію - це основна вартість активів або доходи фірми заявника. Наприклад, у табл. Б.1 наведено приклад того, як початкова політика спочатку визначає премії як функцію фірмового доходу (див. Додаток 2).

Стандартні фактори страхування включають такі змінні, як зміна лімітів або вирахування (утримання) полісу. Наприклад, чим більше ліміти тим більша буде премія, як показано в табл. Б.2 (див. Додаток 2).

Крім того, премія буде змінена на основі таких факторів, як співстрахування, затримка часу, попередні акти порушення, розширений звітний період та бізнес-переривання. Співстрахування коригує, чи страхує одна страхова компанія чи існує договір співстрахування. Історичні претензії стосуються кількості випадків, коли застрахований зазнав інциденту та подав позов за минулі роки. Премії зазвичай збільшуються приблизно на 10% за кожну подію. Проте існують мінімальні та максимальні значення, які забезпечують ряд модифікованих ціноутворень для страхових андеррайтерів на основі переліку міркувань, визначених у полісі, таких як: кількість та розмір претензій, що подаються щорічно, історія судових процесів проти страхувальника та будь-які вжиті коригувальні заходи, щоб обмежити повторне повторення одних і тих самих протиправних дій (див. Додаток 2).. Тобто, виходячи з таких ознак, андеррайтер може вибрати перемножити (або зменшити, або збільшити) премію на 0,85 до 1,7.

Поліси кіберстрахування також забезпечують страхування бізнесу від перебою виробничої діяльності. Для оцінки такого показника необхідно розуміти кількість годин можливої зупинки діяльності та % покриття (див. Додаток 2).

Наступним показником страхові компанії намагаються контролювати ризики для страхувальника на основі галузі, в якій він працює. Однак у даній політиці є декілька підходів до оцінки коефіцієнта (див. Додаток 2). Витрати на страхування бізнесу можуть сильно відрізнятися залежно від типу бізнесу. Тип галузі, публічна видимість, місцезнаходження підприємства та інші фактори також можуть сприяти витратам на страхування бізнесу [15].

Найбільш складний підхід враховує характеристики контролю інформаційної безпеки заявника при визначенні остаточного ціноутворення в преміях. Коригування, що базуються на дійсній позиції безпеки заявника, сильно різняться між політиками, починаючи від основних категорій ризику до більш детальних показників (див. Додаток 2). Проте незважаючи на просту оцінку ця конкретна політика не дає ніяких вказівок щодо того, як андеррайтер повинен оцінювати заявника на основі цих властивостей.

Більш детальніший і продуманий підхід представлений у табл. Б.8, який розмежовує загальну позицію фірми щодо безпеки на шість аспектів (факторів): класифікація даних, інфраструктура безпеки, управління, ризик та відповідність, контроль платіжних карток, контроль засобів масової інформації та переривання комп'ютерної системи (див. Додаток 2). Кожен фактор забезпечував чотири якісні варіанти (відмінно, добре, задовільно, погано) із зважуванням.

Перевага такого підходу щодо інших простіших або складніших підходів полягає в тому, що він забезпечує розумний компроміс між специфічністю та практичністю. Наприклад, інші поліси коригують премію на основі конкретних відповідей на анкети (чи використовує фірма двофакторну автентифікацію, стандартні брандмауери, належні кращі практики), малоймовірно, що будь-який страховик дізнається граничне зменшення ризику, які вони нададуть. Таким чином, такий підхід надає андеррайтеру можливість досліджувати контроль фірми та робити розумні оцінки.

На додаток до характера бізнесу, місцезнаходження та історії позовів, головним фактором у визначенні страхової премії буде вибраний рівень покриття. Чим вищі межі кіберпокриття, тим вищими будуть премії. Однак

додаткове покриття зазвичай коштує дешевше за долар покриття порівняно з базовим покриттям. Наприклад, перші 250 000 доларів США покриття коштують в середньому 739 доларів у прикладі нижче, тоді як наступні 250 000 доларів США покриття коштують лише в середньому 407 доларів, загальна вартість яких становить 1146 доларів [15].

У табл. 2.6 продемонстровано, як змінюється середньорічна премія за різні рівні покриття з різними франшизами на основі бізнесу з помірним ризиком у США. Фактичні ціни премій залежать від типу бізнесу, місцезнаходження та історії претензій.

Таблиця 2.6

Зміна премій страхування кіберризиків за різні рівні покриття

Межа кібервідповідальності	Франшиза	Середньорічна страхова премія
1 000 000 доларів	10 000 доларів	1588 доларів
500 000 доларів	5000 доларів	1146 доларів
250 000 доларів	2500 доларів	739 доларів

Джерело: [15].

Франшиза, що підлягає кіберстрахуванню, - це сума збитків, за яку відповідає компанія у випадку покриття злому, порушення даних або іншої події, покритої страхуванням кіберризиків. Типова франшиза для полісу в 1 мільйон доларів може становити 10 000 доларів, але можна вибрати більші чи менші франшизи залежно від ситуації у компанії. Вибір меншої франшизи означає, що компанія буде платити менше у разі порушення, але це також означає, що премії будуть вищими. Вибираючи франшизу, компанія повинна врахувати вплив збитків на бізнес та суму збитків, яку зможе покрити у разі кіберподії.

Такі типи обрахування страхових премій є найпростішими в системі ціноутворення кіберстрахування. Дослідники та науковці з різних країн світу в різний період часу висували свої теорії та моделі на основі математичного моделювання. У табл. 2.7 наведена класифікація моделей ціноутворення полісу кіберстрахування якими на даний момент користуються страхові компаній на європейському та американському ринках.

Таблиця 2.7

Класифікація моделей оцінки тарифів кіберстрахування

Cyber insurance ratemaking (CIRM)

Назва класифікації моделей	***Процесні моделі***	***Факторні моделі***	***Актуарні моделі***
Опис класифікаційної групи	Моделювання ланцюга операцій, процесів та знаходження ризику для кожного з етапів	Визначення рівню ризику в залежності від сукупності факторів	Визначення ймовірності втрати і оцінка суми збитків на основі історичних даних про кіберінциденти
Методи	- колективна модель ризику; - теорія екстремальних цінностей; - стохастичний процес.	- фіксована ставка з групами небезпеки; - базова ставка на основі опитувальників.	- фіксована ставка, - бета-біноміальна та однофакторна латентна модель - модель на основі копули (зв'язки).
Переваги	Відразу видно причину виникнення ризику	Можливий моніторинг та аналіз ситуацій за допомогою індикаторів	Математична обґрунтованість результатів
Недоліки	Труднощі із отриманням адекватної кількісної оцінки	Складність у визначенні причинно-наслідкових зв'язків	Труднощі із отриманням адекватної кількісної оцінки

Джерело: складено автором на основі [36, 39, 44].

Розподіл моделей оцінки страхових премій у табл. 2.6 був здійснений на основі переважаючого фактору. Тому, наприклад, теорія екстремальних цінностей має в своєму розрахунку VaR-методику, яку потрібно було б віднести до актуарної моделі, але побудова екстремальних сценаріїв розвитку подій для оцінки цієї моделі є більш значущим фактором. Тому вона відноситься до групи процесних моделей.

В недоліках відразу у двох моделях, процесних та актуарних, вказані труднощі із отриманням адекватної кількісної оцінки. Вони полягають в тому, що більшість даних не є у відкритому доступі для користувачів, актуаріїв, аналітиків. Страхові компанії не мають єдиних, або власне напрацьованих ефективних баз даних у розрізі кіберінцидентів. Це пов'язано з тим, що більшість фізичних та юридичних осіб не розкривають інформацію про кібератики, які

зазнають вони, або їхні підприємства та відповідно їх наслідки у грошовому вимірі втрат.

Математична оцінка кіберстрахування стосується не тільки обрахування страхових тарифів, вона також може застосовуватися до вирахування лімітів страхового покриття, франшиз. Наприклад, у табл 2.8 наведено мінімальні обов'язкові ліміти відповідальності страховика. Відповідно за різних лімітів страхових може мати три сценарії: песимістичний (високий ризик), оптимістичний (базовий ризик) та базовий (низький ризик). Всі показники ризику для страховика оцінюються на основі моделей CIRM.

Таблиця 2.8

Ймовірність настання ризику для страхових компаній за різних сценаріїв встановлення страхових лімітів

Ліміт покриття	Низький ризик	Базовий ризик	Високий ризик
=500	0,0977	0,4055	5,9530
=1 000	0,0437	0,1760	2,1016
=10 000	0,0033	0,0129	0,11335

Джерело: [31]

Моделі оцінки тарифів кіберстрахування відрізняються між собою математичною моделею, яка лежить в основі обрахунків та типами втрат, які зазнає страхувальник (табл. 2.9). Відповідно для кожного типу покриття, які можуть забезпечувати поліси кіберстрахування можуть бути свої моделі обрахунку страхових тарифів. Тому в теорії, якщо поліс є комплексним, він може включати в себе відразу декілька таких моделей. Проте на практиці актуарії схиляються більше до типових розрахунків із використанням одної моделі.

Таблиця 2.9

Порівняння авторських моделей CIRM

Автори / рік	Модель	Математична оцінка	Вхідні дані	Тип втрат
Бем і Катарія (2006)	Бета-біноміальна та однофакторна латентна модель	Внутрішня кореляція збоїв	Дані про кібератаки	Втрата виробничих функцій операцій

Продовження табл. 2.9

Герат (2011)	Модель на основі Copula (зв'язків)	Інтегроване моделювання на основі Copula	Кількість заражених комп'ютерів та їх загальна втрата	Пошкодження першої сторони через кіберпорушення
Мухопадхяй (2013)	Колективна модель ризику	Байєсівська мережа моделювання за допомогою Copula (CBBN)	Двадцять індикаторних змінних (втрата, оновлення системи тощо)	Загальні порушення кібербезпеки
Елінг і Вірфс (2015)	Теорія екстремальних цінностей	Value-at-Risk (VaR) і Tail Value-at-Risk (TVaR)	Дані про операційний ризик активів	Внутрішні та зовнішні помилки систем і людей
Фаренвальд (2018)	Стохастичний процес (модель SIS)	Позначений точковий процес і середнє значення поля	Топологія мережі, швидкість зараження та відновлення, початкові зараження	Втрати через кіберзараження
Хуа і Сю (2020)	Стохастичний процес/немарківський (Copula)	Монте-Карло моделювання кіберінфекції та процесу відновлення	Кількість вузлів і посилань, топологія мережі, швидкість зараження	Збитки через перерви в роботі та втрати, пов'язані з витратами на ремонт комп'ютерів

Джерело: складено автором на основі [36, 44]

Отже, встановлення тарифів на кіберстрахування — це процедура, яка використовується для встановлення ставок (або цін) на продукти кіберстрахування, що надаються страховими компаніями. Оцінка ставок є важливою проблемою для продуктів кіберстрахування. Ця проблема виникає через недоступність актуарних даних та невизначеність нормативних стандартів кіберризиків. Серед страхових компаній досі не існує стандартизованого підходу до оцінки тарифів, тому можна спостерігати серед досліджень широкий спектр різних думок і підходів, які не завжди пов'язані одним з одним.

РОЗДІЛ 3
ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРСТРАХУВАННЯ В УКРАЇНІ

3.1 Міжнародний досвід розвитку кіберстрахування та можливості його імплементації у вітчизняну практику

Зараз у світі існує понад 30 мільярдів підключених IT-пристроїв (наприклад, ПК, сервери, маршрутизатори, промислові системи керування, медичне обладнання та операційні технології). Ми живемо у світі, де датчики можуть виявляти жести, дотики та зміни навколишнього середовища, дані можуть передаватися за допомогою радіочастотних електромагнітних полів, де мікроелектромеханічні системи (МЕМ) можуть взаємодіяти з навколишнім середовищем (наприклад, мікросенсори) і змінювати спосіб здійснення платежів за допомогою мобільних пристроїв. пристроїв [43]. Так звані «додатки для Інтернету речей» впливають на всі сектори нашої економіки, наприклад:

• охорона здоров'я: моніторинг та передача даних про хронічні захворювання (наприклад, рівень глюкози), моніторинг фізичної активності;

• фінансові послуги: коли номери кредитних карток та банківських рахунків відкриті, успішні атаки можуть бути катастрофічними як установ, так і їхніх клієнтів [40];

• промисловість: розумні мережі, розумні міста, транспортні системи, аварійні служби, включають роздрібну торгівлю (відстеження відправлень і логістика, оптимізація ланцюгів поставок за допомогою датчиків на полицях);

• інформаційні технології: пристрої безпеки, мобільні пристрої, передові системи допомоги водієві (ADAS), моніторинг історії водіння;

• неприбуткові: школи, які зберігають електронні адреси, фізичні адреси та іншу інформацію про своїх вчителів та учнів у загальнодоступному списку в Інтернеті; державні організації піддаються впливу зараженого програмного

забезпечення, атак з боку програм-вимагачів, спрямованих на пошкодження адміністративних процесів, у тому числі податкових служб, систем соціального забезпечення та майнових служб;

• виробництво: відстеження роботи машин і моніторинг продуктивності (бездротове відстеження запасів, контроль виробничих процесів), відстеження потоків сировини та ланцюгів поставок [43].

На рис. 3.1 показані основні тенденції частоти претензій за галузями. Як бачимо, кожні півроку кожна галузь все частіше піддається кіберзагрозам, тому страховики збільшують свою активність. Лише некомерційні організації демонстрували тенденцію до зниження. Однак це тим більше, що влада дуже стурбована своєю кіберзагрозою, тому всі організації державного значення (некомерційні) почали активно впроваджувати основні методи боротьби з кіберзлочинністю.

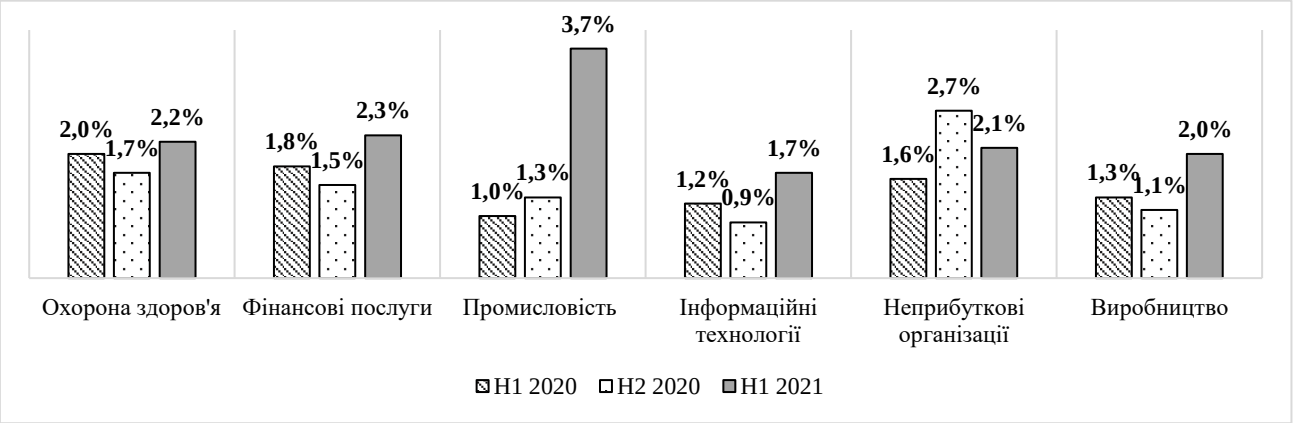

Рис. 3.1 Кіберстрахові претензії за галузями, % [35]

Страхові компанії на ринку України, на відміну від своїх іноземних колег, не поспішають активізувати свою діяльність у кіберстраховій сфері. Це пов’язано як з низьким попитом на ринку впринципі, так і побоюваннями страховиків щодо прибутковості ведення такого бізнесу. У розділі 2.2 ми могли спостерігати таку тенденцію, що попит на послуги зростає, але пропозиція на ринку навпаки спадає, так як для страховиків це виходить неприбутковою діяльністю, а іноді навіть і збитковою. Першу тенденцію, яку можна виділити для оновленого українського кіберстрахового ринку на основі міжнародного

досвіду – це диверсифікація страхувальників по галузях. В основному тенденція кібератак направлена на конкретний сектор, наприклад бюджеті установи, банки, крупних ретейлерів. Тому якщо диверсифікувати пакет страхувальників, можна уникнути системних ризиків. З рис. 3.1 бачимо, що галузь промисловості найбільше і з позитивною тенденцією страждає від кіберзагроз і відповідно до страховиків збільшується кількість претензій по полісах. Тому цю галузь на початковому етапі виходу на ринок, або утвердження на вже існуючому можна зменшити до мінімуму. Прибирати повністю зі свого пулу страхувальників її не варто, так як ймовірність там не є стовідсотковою. Більше того, такі сектори як охорона здоров'я та фінансові послуги можуть стати обов'язковими для страхування, так як цей сектор є критично важливим для функціонування бізнес-екосистем.

Таку диверсифікацію страхувальників можна проводити і за кількістю працівників (рис. 2.7) і за розміром компанії (рис. 3.2). На розмір компанії страховикам потрібно звернути особливу увагу. На малі підприємства по статистиці менш націленими є кіберзагрози, так як хакери розуміють, що ефективніше по їх доходах буде одна атака на велике підприємство, ніж декілька на малі. Тому малі підприємства перебувають у меншій зоні ризику (рис. 3.2). Відповідно страхові компанії, які тільки виходять на ринок і не впевнені в своїх силах, можуть націлюватися на страхування малого бізнесу. Відповідно згодом збільшувати структуру своїх страхувальників, якщо будуть забезпечені попередні фінансові цілі.

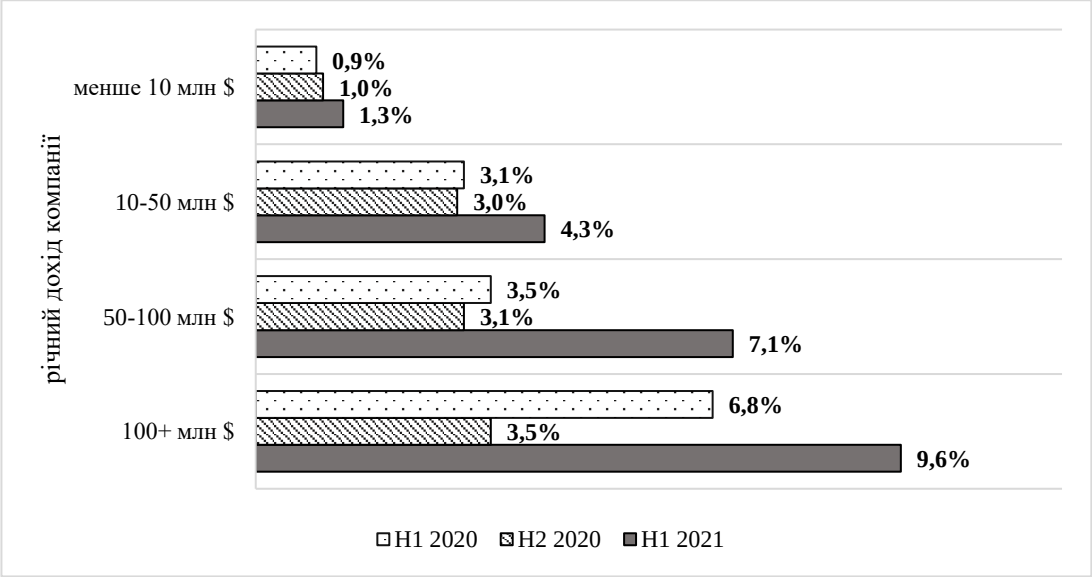

Рис. 3.2 Частота претензій страхових виплат за розміром компанії (прибуток компанії), % [35].

На багатьох сайтах міжнародних страхових компаній та страхових брокерів можна знайти калькулятори кіберстрахових премій. Страховим компанія України можна також розміщати такі попередні оцінки у якості маркетингової стратегії для того, щоб користувачі могли оцінити свої можливості. Міжнародна швейцарська група страхових компаній Helvetia Insurance, на нашу думку, рекомендує найбільш відповідний для ринку України калькулятор страхових премій (рис. 3.3). Такий тип калькулятора врахує всі особливості обрахунку страхових премій, які було описано у розділах вище.

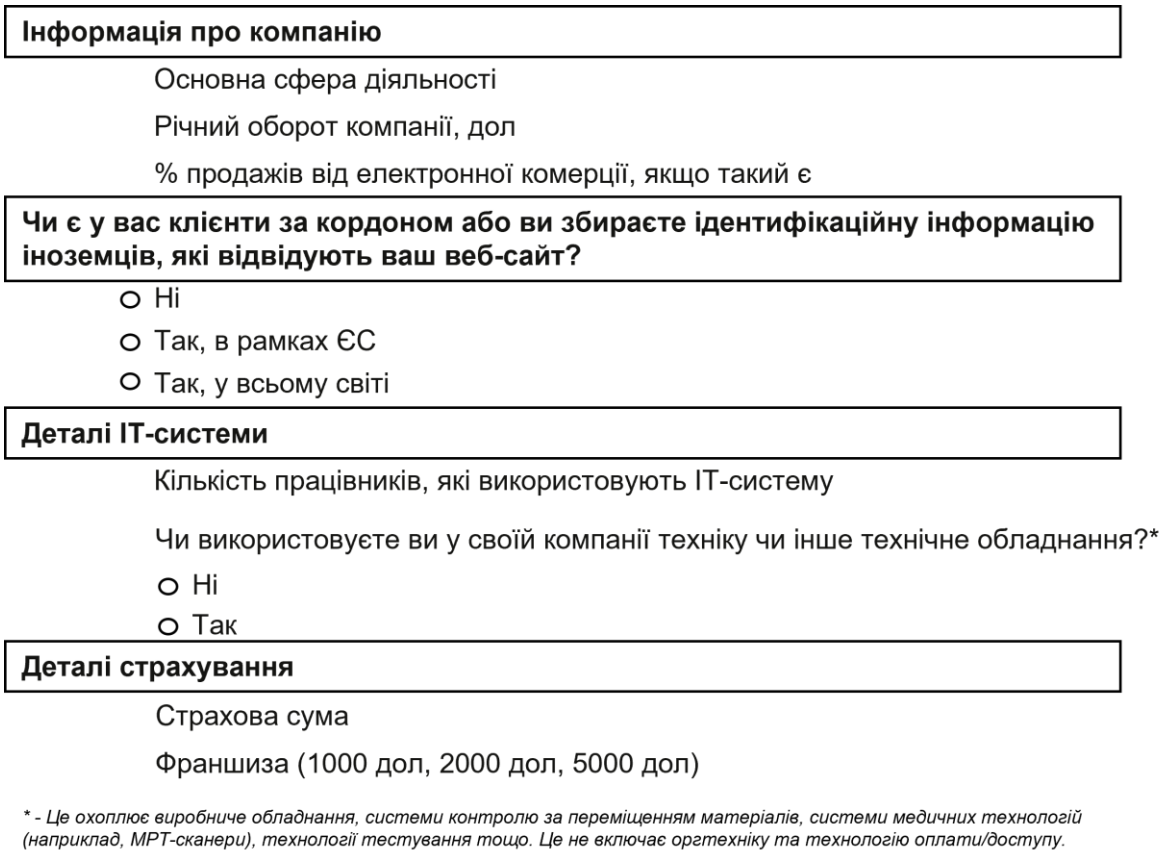

Рис. 3.3 Калькулятор страхових премій кіберстрахового полісу

Джерело: складено автором на основі [47].

Калькулятор страхових премій може пропонувати не тільки страхова компанія, але й брокери, або інші страхові агенти, які можуть розмістити таку інформацію публічно. Якщо попередні умови задовольняють страхувальника, то тоді страховик проводить більш розгорнутий аналіз такого «калькулятора» (рис. 3.4). В основному для якісного аналізу на даному етапі страховикам потрібно залучати кіберекспертів (власних або аутсорсинг). Можна проводити таке дослідження і за рахунок андерайтерів, але якщо в них немає достатніх знань про айті-середовище та кібербезпеку, то відразу збільшується ризиковість кожного такого укладеного договору.

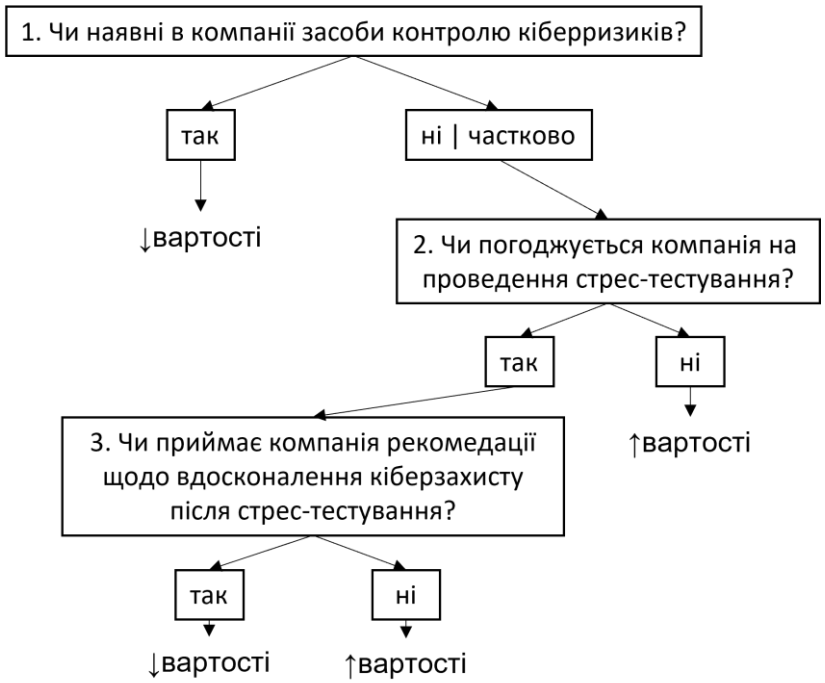

Рис. 3.4 Процес формування цінової позиції кібестрахового полісу

Джерело: розроблено автором на основі пропозицій міжнародних страхових компаній.

Засоби контролю кібербезпеки є основним фактором у визначені вартості кіберстрахового полісу. У розділі 2.3 ми бачили які фактори впливають на страхові премії у факторних моделях. Відповідно, чим нижчий рівень контролю кібербезпеки, тим вищими є премії. Основними засобами контролю для всіх груп підприємства є:

1. *Багатофакторна автентифікація (MFA):* вимагання принаймні двох доказів для підтвердження особи.
2. *Виявлення кінцевих точок і відповідь (EDR):* інтегрований центр для збору, кореляції та аналізу даних, а також для координації попереджень і реагування на безпосередні загрози.
3. *Захищені, зашифровані та перевірені резервні копії*.
4. *Управління привілейованим доступом (PAM):* необхідний рівень доступу для працівників для виконання своєї роботи.
5. *Фільтрація електронної пошти та веб-безпека* [24].

Перелік не кінцевий і може різнитися в залежності від специфіки бізнесу. Наприклад, якщо діяльність компанії пов'язана із обробкою великих обсягів конфіденційної інформації, то її неспроможність протидіяти кіберзагрозам підпадає під санкції, відповідно до документів, що регулюють поводження з даними, зокрема Загального регламенту про захист даних (GDPR). Відповідно до GDPR, на компанію можуть бути накладені штрафні санкції у розмірі 20 мільйонів євро або 4% від її річного обороту, залежно яка сума є більшою. Відповідно, чим вищий рівень потенційних штрафних санкцій за неспроможність захистити дані клієнтів, тим вищий відсоток від свого IT-бюджету компаніям слід спрямовувати на кібербезпеку. Якщо компанія таких інвестицій не здійснює вартість полісу кіберстрахування відразу може зростати врази.

Ефективними методами забезпечення захищеності компаній від кібератак є регулярне стрес-тестування: проведення тестів на проникнення (пентестів) та організація баг-баунті програм. Penetration test (пентести) – симуляція кібератаки на комп'ютерні системи, мобільні застосунки та веб-додатки з метою перевірки захищеності системи. Тест на проникнення допомагає виявити, наскільки та чи інша система є вразливою до хакерських атак. Баг-Баунті програми передбачають залучення незалежних IT-фахівців (етичних хакерів) для виявлення вразливостей веб-ресурсів компаній-замовників [13].

Стрес-тестування проводиться на основі міжнародних стандартів, які повинні дотримування компанії, забезпечуючи свою кібербезпеку. Це може бути модель NAIC, яка визначає конкретні вимоги та рекомендації щодо захисту даних страхувальника. Вона включає технічні, адміністративні та фізичні засоби захисту, а також підтримує відповідні заходи кібербезпеки, плани реагування, репортажі та програми навчання співробітників. Окрім моделі NAIC, страхові фірми також повинні дотримуватися інших стандартів, таких як NIST, ISO 27000, OFSI та SOC2. Конкретне законодавство, яке стосується конкретних фірм, може значно відрізнятися залежно від місця розташування та характеру бізнесу [26].

Андерайтери можуть запропонувати нижчу премію для клієнта, якщо той застосує ряд дій, які необхідні для зменшення вартості страхового полісу, тобто відповідність поставленим критеріям. Серед таких рекомендацій можна звернутися до Financial Services Authority (FSA), який є центральним органом нагляду за ринком фінансових послуг Великобританії та рядом інших страхових компанії, узагальнюючі практики яких зображені на рис. 3.5.

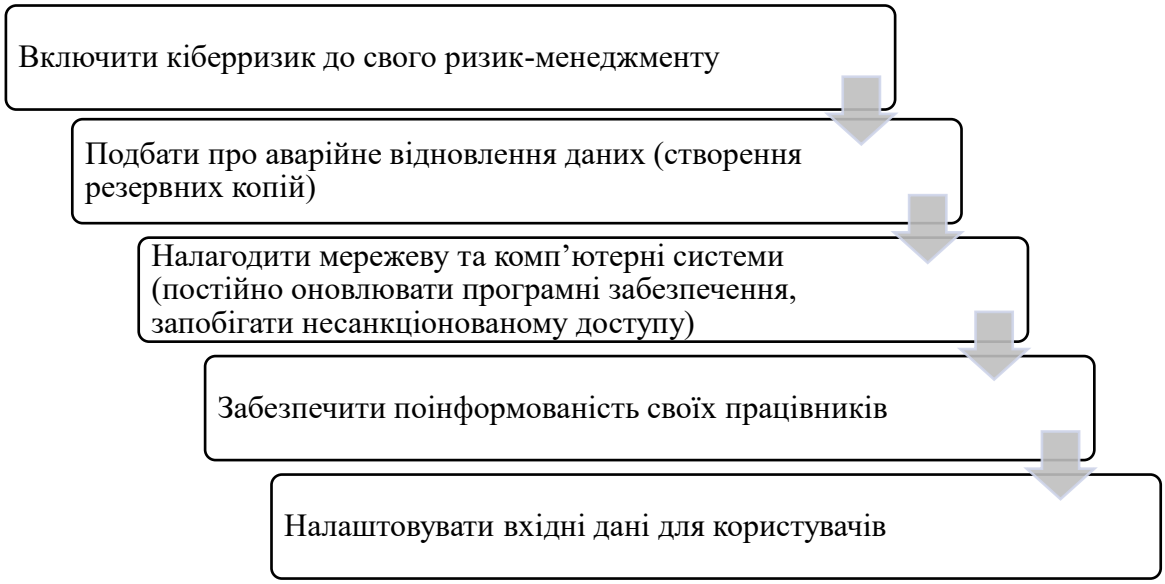

Рис. 3.5 Рекомендації щодо зменшення вартості полісу кіберстрахування

Джерело: складено автором на основі [30]

Поряд з нижчою вартістю полісів кіберстрахування, деякі страховики взагалі переглядають необхідність покриття певних кіберінцидентів, таких як програми-вимагачі. AXA, французька страхова компанія, оголосила, що припиняє покривати виплати програм-викупів у Франції, починаючи з травня 2022 року. Рішення AXA є відповіддю на зростаючі збитки, завдані в результаті атак програм-вимагачів з боку страховиків, а також тиск з боку урядовців, які стверджують, що виплати кіберстрахування сприяють зростання кількості атак програм-вимагачів. Хоча наразі рішення AXA стосується лише Франції, воно може відкрити двері для інших страховиків, щоб наслідувати їх приклад у майбутньому [46]. Багато дослідників стверджують, і це також видно з аналізу у попередніх розділах, що деякі типи покриттів приносять тільки збитковість

страховим компаніям. Тому в найближчі роки нас чекає стандартизація кіберстрахових продуктів.

Отже, незважаючи на постійні загрози кіберстрахового бізнесу, страховики намагаються шукати нові способи оцінки як своїх ризиків, так і своїх клієнтів. Для цього вони починають запроваджувати нові обмеження на ринку, піднімати вартість кіберстрахування, утверджувати нові моделі оцінки та, головне, звертати велику увагу на кібербезпеку кожного страхувальника. Реалізують вони це за допомогою основного інструменту – стрес-тестування, який може стати цінним інструментом для оцінки рівня безпеки та стандартів захисту даних у порівнянні з загальноприйнятими стандартами. Менша кількість на ринку все-таки не готова на такі затрати у своїй діяльності, тому готова задовольнятися малими підприємствами та найменш ризиковими галузями. Українському страховому бізнесу треба активно звернути увагу на такі два сценарії розвитку, адже в певний момент вони можуть втратити шанс на реалізацію кіберстрахового покриття для українських юридичних та фізичних осіб.

3.2 Перспективи впровадження кіберстрахування для фізичних та юридичних осіб в умовах сучасник викликів

Страховим компаніям необхідно активно розвивати ринок кіберстрахування, адже даний сегмент може стати для них «блакитним океаном». Сучасні реалії розвитку страхового ринку України дозволяють зробити висновки стосовно факторів, що перешкоджають впровадженню і розвитку страхування кіберризиків: не існує довіри на стандартні послуги страхування, а такий інноваційний продукт як кіберстрахування взагалі не організує своє коло споживачів; не існує конкретних видів кіберстрахування, лише комплексні продукти, які націлені на страхування різних об'єктів з приводу одного виду небезпеки, наприклад – кібератаки.

Визначення драйверів такого сприйняття та підвищення страхової обізнаності можуть допомогти збільшити попит на страхування кіберризиків. Проте ефективність комунікаційних стратегій для покращення обізнаності та сприйняття кіберризиків також ставиться під сумнів на сучасному етапі.

Компаніям потрібно вкладати гроші в людей, процеси та системи. Зокрема, існує потреба у працівниках, які можуть допомогти усунути розрив між бізнес-менеджерами та IT-спеціалістами. Враховуючи нинішні обмеження безпеки, дизайн кіберстрахових продуктів та інноваційні способи передачі кіберризиків можуть бути цікавими сферами для бізнес-досліджень. Надалі можуть виникнути нові та інноваційні бізнес-моделі, які знижують та передають кіберризики, наприклад, через блокчейн.

Особливою рисою страхування кіберризиків є те, що потреба на нього формується в процесі виникнення кібератак або потенційних кіберзагроз. Відповідна пропозиція на ринку залежить від персональних особливостей настання кіберіцедентів у страхувальників, ціни страхового полісу, величини прибутку страховиків та повернення збитків від виникання страхових випадків, спроможністю останніх узгоджувати страхові договори через Інтернет (оформлення онлайн-полісів).

Для ринку кіберстрахування характерна консервативна модель побудови, і страховикам необхідно: будувати репутацію серед страхувальників шляхом удосконалення страхових пропозицій у сфері інформаційної безпеки; аналізувати тенденції на кіберринку для можливості надання актуальних пропозицій.

Наприклад, з 2020 року розпочали впроваджувати технологію 5G, що може призвести до більш швидкої та розширеної мережі пристроїв IoT. Така новація відразу призведе до більших DDoS-атак і нових викликів щодо кібербезпеки. Страхові компанії повинні звернути особливу увагу на цю загрозу ще до її масштабного впливу.

Характерною тенденцією в сфері сучасних кіберзагроз є оновлення програмних забезпечень. Головна загроза полягає в тому, що незахищені

вразливості є головною причиною системних компромісів. Підтримка Windows 7 закінчилася 14 січня 2020 року, що призвело до появи більше непідтримуваних та незахищених застарілих систем і, як наслідок, може проявитися тенденція до атак, як це було із атакою викупного програмного забезпечення WannaCry, через яку багато організацій зазнали нападу за нерегулярного оновлення операційних систем та використання застарілих та непідтримуваних операційних систем, таких як Windows XP (і вже Windows 7).

Більшість полісів кіберстрахування містять виключення для непідтримуваних систем, і страховики націлені на інформування своїх клієнтів про необхідність оновлення системних забезпечень, як тільки вони стають доступні. Отже, страховики мають забезпечити не тільки функцію страхового захисту, а й інформування для свої потенційних та майбутніх [22].

Основною проблемою формування страхового захисту за рахунок кіберстрахування на сучасному етапі є відсутність достатніх статистичних даних про кіберзагрози та фінансові наслідки їх впливу, так як компанії не розкривають цю інформацію із власних суджень для збереження своєї репутації. Для того, щоб компанії зберегли свій бренд, а актуарії змогли проводити свої розрахунки та моделювати наслідки, необхідно регулятору страхового ринку (НБУ) започаткувати збір такої інформації. На основі таких даних актуарії зможуть побудувати актуарні таблиці на прикладі майнового або страхування життя.

Зобов’язанням регулятора для збору такої інформації може послужити Загальний європейський регламент щодо захисту даних (GDPR 2018). Його запровадження є обов’язковим для країн Євросоюзу, в тому числі і України, як претендента на повноцінне членство в ЄС, а також в рамках оновленого внутрішнього законодавства щодо кібербезпеки. За його обмеженнями бізнес може бути оштрафований за нерозголошення обставин порушення кібербезпеки - до 20 мільйонів євро або 4% його обороту [28].

Існує кілька ознак розвитку кіберстрахування, які свідчать про відносну незрілість ринку. По-перше, бракує стандартизації страхових пропозицій. Окремі страховики пропонують підходи, які передбачають чіткий поділ між

традиційними полісами страхування кіберризиків. Інші страховики вирішили вбудувати кіберзахист в наявне у них покриття, керуючись аргументом, що цей варіант простіше продати клієнтів, ніж цілком новий вид страхування. Однак, вкладення кіберстрахування в інше покриття може призвести до недостатньої ясності і якості щодо того, що охоплює такий вид покриття. За таких умов, страховики можуть опинитися в ситуації, коли їм доведеться покривати ті ризики, які можуть принести їм кумулятивний збиток, або не покривати їх і цим самим спровокувати невдоволення своїх клієнтів до страхової компанії та повного комплексу її послуг.

Подальший розвиток кіберстрахування в Україні суттєво залежить і від коректності формування страхових премій. З цією метою страховим компаніям необхідно розуміти конкретні потреби компаній, переконатися, що вся мережа компанії покрита, а не лише окремі машини чи пристрої, врахувати, чи потрібне страхування третьої сторони (це стосується не тільки компанії та її співробітників, а й усіх клієнтів, дані яких можуть зберігатися на серверах). Це дозволить також уникнути витрат на непотрібні додаткові послуги.

Європейський досвід свідчить, що більше ніж 40% світової страхової премії за страхування кіберризиків припадає на перестраховиків. Для порівняння, у більш розвинених сферах страхової діяльності, таких як страхування майна або відповідальності, частки премій, що передаються перестраховикам, зазвичай залишаються між 10 та 15%. Переважно, страховики перестрахують свій бізнес за допомогою самостійних кібердоговорів, підкреслюючи еволюцію страхування кіберризиків як окремої сфери бізнесу [23]. Характерною тенденцією є укладання договорів пропорційного покриття застрахованих ризиків. Таким чином компанії перестраховують себе від ризиків введення нового виду страхування.

З урахуванням особливих загроз страхування кіберризиків страховики та перестраховики неохоче додають до своїх вже великих і важко оцінених ризиків ризики іншої компанії. Тому, як перспективний варіант вирішення перестрахування діяльності страхових компаній в сфері кіберстрахування, є

використання катастрофічних облігацій, або так званих «cat bonds». Це є прикладом страхової сек'юритизації, коли створюються цінні папери, пов'язані з ризиком, які передають певний набір ризиків (як правило, ризики катастрофи, стихійного лиха чи кібератаки) від емітента чи спонсора (компанії, що передає кошти) інвесторам на ринку капіталу [45].

Типова структура cat bonds (рис. 3.6) передбачає, що страхова компанія укладає договір про страхування із страхувальником (або контрагентом), отримуючи від нього премії в обмін на забезпечення покриття. Страхова компанія випускає цінні папери інвесторам і отримує взамін основні суми (заставу). Потім кошти перекладаються на заставний рахунок, з якого вони, як правило, вкладаються у високорейтингові фонди грошового ринку. Для інвесторів дохід виплати відсотків складається з відсотків, які сплачує страхова компанія з суми застави та премій, які сплачує страхувальник [42]. Якщо відбувається страховий випадок, який відповідає умовам активації виплати, страхова компанія ліквідує заставу, необхідну для здійснення платежу, та відшкодовує страхувальнику всю суму відповідно до умов транзакції за cat bonds. Якщо страховий випадок не відбувається, застава ліквідується наприкінці строку котирувальної облігації, і повертається інвесторам із нарахованими відсотками.

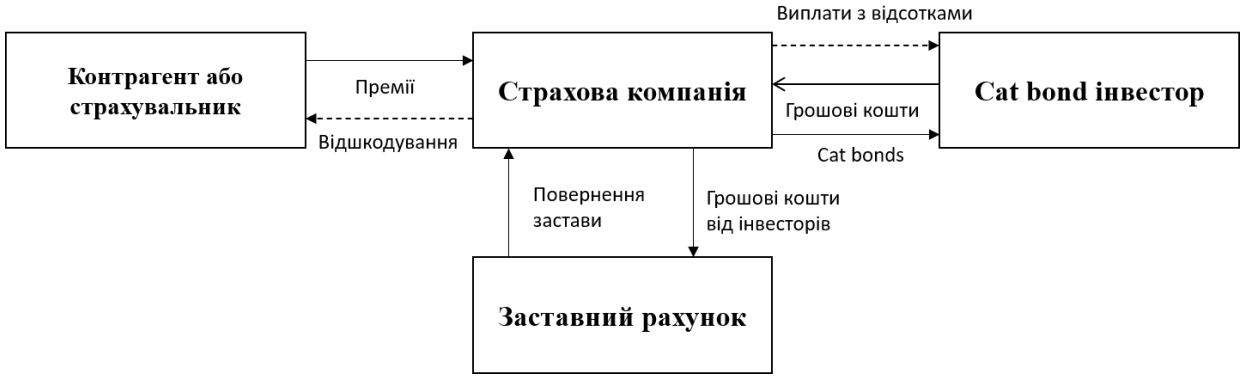

Рис. 3.6 Структура реалізації катастрофічних облігацій [42]

Катастрофічні облігації сприяють диверсифікації портфеля страховика та можуть розглядатися як супутня інвестиція в рамках основної інвестиційної стратегії. Таким чином, інвестори беруть на себе ризик втрати внаслідок

катастрофи або кібератаки, що настає, за привабливі ставки прибутку від інвестицій. Якщо така катастрофа чи названий випадок небезпеки трапиться, інвестори втратять частину або всю основну суму, яку вони інвестували, і емітент (як правило, страхова або перестрахувальна компанія, але іноді корпорація або суверенна особа) отримає ці гроші для покриття своїх втрат. Якщо страховий випадок не відбудеться, інвестори отримують більш високу процентну ставку, ніж якби вони розмістили свої інвестиційні гроші в казначейських облігаціях.

З урахуванням сучасного стану розвитку вітчизняного страхового ринку та в умовах особливих викликів для українських компаній такий досвід є доцільним і особливо перспективним стосовно розвитку кіберстрахування.

Отже, кіберстрахова галузь лише починає розвиватися на ринку України, страхові компанії не мають достатніх ресурсів для розроблення власного підходу до оцінки кіберризиків, а потенційні клієнти не проявляють попиту на відносно новий вид страхування. Проте поточні оцінки і прогнози свідчать про те, що необхідність даної галузі щорічно збільшується в геометричній прогресії. І ті, страхові компанії, які зможуть запропонувати якісні кіберстрахові поліси, які будуть включати в себе високі відсотки на покриття та адекватні страхові премії можуть відразу зайняти лідируючі позиції, так як наплив клієнтів буде збільшуватися в тій же прогресії.

ВИСНОВКИ

В результаті проведеного дослідження отримано наступні висновки:

1. У світі комп'ютерів та комп’ютерних мереж зростаюча кількість кібератак є головною турботою для цілого ряду компаній та урядів. Такі напади призначені для отримання доступу, зміни або видалення несанкціонованої інформації. У міру того, як технології швидко просуваються та диверсифікуються, кіберзлочини також продовжують свій розвиток. Кібератаки незалежно від того, розпочаті вони хакерами, злочинцями, інсайдерами чи навіть національними державами, трапляться і можуть спричинити помірні та серйозні збитки для великих та малих організацій. Хоча існують різні рішення безпеки для запобігання кібератакам, ні одне з них не буде гарантувати 100-відсоткову безпеку інформації. З цієї причини багато компаній приймають рішення про страхування кіберризиків.

2. Визначено, що кіберризик – це ймовірність настання подій, які вражають роботу ІТ-систем та кібербезпеку організації через стороннє втручання цифрових та інших електронних технологій, що призводить до отримання збитків, руйнування цифрових активів та можливої втрати репутації організації.

3. Одним із найбільш дієвих інструментів в системі ризик-менеджменту стосовно кібкрризиків є кіберстрахування. Кіберстрахування можна визначити як страховий продукт, який пов'язаний з передачею фінансового ризику третій стороні, тобто страховій компанії для того, щоб допомогти державі, суспільству, суб’єктам господарювання та фізичній особі зменшити вплив ризику шляхом компенсації витрат, пов’язаних із потенційно руйнівними наслідками кіберзлочинів, забезпечити захист від збитків, що виникають внаслідок порушення безпеки та конфіденційності. Можна виділити два підходи до формування покриття кіберризиків в страхуванні: страхування кібервідповідальності і майнове страхування наслідків можливих кібератак.

4. Нормативно-правове забезпечення інноваційного сегменту страхового ринку – кіберстрахування, знаходиться на стадії формування і в Україні і світі. Європейська Директива щодо мережевої та інформаційної безпеки ЄС є першою частиною законодавства про кібербезпеку в усіх країнах ЄС. Підвищення кібербезпеки в Євросоюзі є основною метою Директиви NIS шляхом встановлення загального рівня безпеки мережевих та інформаційних систем. Європейська Директива має позитивний вплив на розвиток ринку кіберстрахування в Україні особливо для інтернет-ринків, пошукових систем в Інтернеті, служби хмарних обчислень і може стати основою відповідного законодавства в країні.

5. Встановлено, що сприйняття населенням та компаніями страхування кіберризиків, як інструменту кібербезпеки напряму залежить від тенденції розвитку кіберзагроз. Тому було побудовано модель на основі кореляційно-регресійного аналізу для визначення впливу можливих факторів на статистичні тенденції кібератак. Аналіз було здійснено на основі даних країн Європейського Союзу, так як така модель найкраще підходить для ринка України.

6. Кіберстрахування існує менше 30 років, тому це галузь, яка все ще розвивається, як і кіберризики з часом. Тому ринок, на відміну, від інших ринків страхування є доволі динамічним. Ще три роки назад популярність кіберстрахування не була такою високою на міжнародному ринку, проте із збільшенням вартості кібервтрат, юридичні та фізичні особи почали проявляти підвищений попит на новий вид страхування. І на ринку утворилась тенденція: попит збільшується, а пропозиція зменшується, що пов’язано з тим, що в попередні періоди страхові компанії не змогли провести адекватну оцінку кіберризиків і зазнали значних втрат, дехто навіть критичних для продовження бізнесу. Як наслідок, значно виросли страхові тарифи, були встановлені нижчі межі покриття в деяких бізнес-секторах та введено обмеження на групу покриттів, які тепер недоступні для страхувальників.

7. Встановлено, що зменшення пропозиції на ринку кіберстрахування спричинено відсутністю стандартизованих моделей актуарних розрахунків.

Через це кожна страхова компанія пропонує свій підхід на основі проаналізованих джерел, тому на ринку переважає завищена вартість полісів і недоскональні характеристики кіберстрахових покриттів. Для можливості страхових компаній України запроваджувати страхування кіберризиків було представлено порівняння як базових, так і авторських принципів стратегії ціноутворення. Хоча ці дослідницькі моделі дещо полегшить обмеження укладання кіберстрахових угод через відсутність історичних даних претензій, вони не можуть впоратися з швидко розвиваючою природою методів кібератак.

8. Визначено, що незважаючи на постійні загрози кіберстрахового бізнесу, страховики намагаються шукати нові способи оцінки як своїх ризиків, так і своїх клієнтів. Для цього вони починають запроваджувати нові обмеження на ринку, піднімати вартість кіберстрахування, утверджувати нові моделі оцінки та, головне, звертати велику увагу на кібербезпеку кожного страхувальника. Реалізують вони це за допомогою основного інструменту – стрес-тестування, який може стати цінним інструментом для оцінки рівня безпеки та стандартів захисту даних у порівнянні з загальноприйнятими стандартами. Менша кількість на ринку все-таки не готова на такі затрати у своїй діяльності, тому готова задовольнятися малими підприємствами та найменш ризиковими галузями. Українському страховому бізнесу треба активно звернути увагу на такі два сценарії розвитку, адже в певний момент вони можуть втратити шанс на реалізацію кіберстрахового покриття для українських юридичних та фізичних осіб.

9. Встановлено, що розвиток кіберстрахування в Україна має значні перспектики, оскільки ряд вітчизняних компаній вже займаються даним продуктом та продають його на ринку. Доведена необхідність використання перестрахування та катастрофічних облігацій для страхових компаній у новій галузі страхування.

Страхування кіберризиків в Україні є потенційно зростаючою галуззю для страхового ринку, оскільки кожна компанія для успішного введення бізнесу використовує сучасні технології. Щоб зайняти цей сегмент ринку, страховим

компаніям необхідно врахувати досвід зарубіжних колег, забезпечити диверсифікацію спектра можливих послуг, адекватно оцінювати взяті на себе ризики та зобов’язання, та популяризувати не тільки кіберстрахові продукти серед потенційних клієнтів, а й інструменти кібербезпеки, як одного з головних етапів ризик-менеджемнту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Братюк В. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. №9((171)). 2015. С. 421-427. URL: http://dspace.msu.edu.ua:8080/jspui/handle/123456789/1403
2. Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. *Зовнішня торгівля: економіка, фінанси, право.* 2018. № 3. С.101–115. URL: http://nbuv.gov.ua/UJRN/uazt_2018_3_10.
3. Глобальні тарифи на кіберстрахування зросли на 34%, страхові премії на 74%. Огляд Fitch. *Форіншурер*. URL: https://forinsurer.com/news/22/04/18/41141.
4. Гудзь О. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. *Економіка. Менеджмент. Бізнес*. № 3 (29). 2019. ст. 4 – 12. DOI: 10.31673/2415-8089.2019.030412.
5. Кіберзлочинність в світі. Стан кіберзлочинності в різних регіонах світу. *Tadviser*. 2017. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5#.
6. Нагайчук. Н.Г., Третяк Н.М., Ткаленко О. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки. *Фінансовий простір*. 2019. No 1 (33). ст. 97 - 111. DOI: 10.32702/2307-2105-2020.4.6.
7. Приказюк Н.В., Гуменюк Л.С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Електронне наукове фахове видання «Ефективна економіка»*. 2020. № 4. DOI: 10.32702/2307-2105-2020.4.6.

8. Правова база української кібербезпеки: загальний огляд і аналіз. *Міжнародна фундація виборчих систем в Україні*. 2019. URL: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf.
9. Про захист інформації в інформаційно-комунікаційних системах: Закон України № 1089-IX від 16.12.2020. *Відомості Верховної Ради України (ВВР)*. 1994. № 31. ст.286. Поточна редакція від 01.01.2022. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
10. Про основні засади забезпечення кібербезпеки України: Закон України № 2469-VIII від 21.06.2018. *Відомості Верховної Ради України.* 2017. № 45. ст.403. Поточна редакція від 15.12.2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
11. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України із змінами № 447/2021 від 26.08.2021. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.
12. 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#n12.
13. Секрети кібербезпеки: раціональність інвестицій у кібербезпеку? Європейська Бізнес Асоціація. URL: https://eba.com.ua/sekrety-kiberbezpeky-ratsionalnist-investytsij-u-kiberbezpeku/.
14. Стратегія кібербезпеки України: цілі та пріоритети. URL: https://armyinform.com.ua/2021/08/27/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/.
15. Adrian Mak. Cyber Insurance Cost. *Advertiser Disclosure*. April 7, 2021. URL: https://advisorsmith.com/cyber-liability-insurance/cost/.

16. Allianz risk barometer identifying the major business risks for 2021. URL: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.
17. Bohme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework. Conference. 2010. URL: ttp://www.icsi.berkeley.edu/pubs/networking/modelingcyber10.pdf.
18. Burke D. Cyber Insurance 101: What Cyber Insurance Covers. *Woodruff Sawyer*. 2021. URL: https://woodruffsawyer.com/cyber-liability/cyber-101-liability-insurance/.
19. Cost of a Data Breach Report 2021. *IBM websites*. URL: https://www.ibm.com/security/data-breach.
20. CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk. *CRO Forum*. June 2016. URL: https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf.
21. Cyber Insurance Market Report 2020-2030. *Visiongain*. 2020. – URL: https://cdn.visiongain.com/wp-content/uploads/Sample-Pages-from-CYB0053.pdf.
22. Cyber Insurance Top 11 Threat Trends for 2020. URL: https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-top-11-threat-trends-for-2020/.
23. Cyber Market Conditions. *Gallagher*. JANUARY 2022. URL: https://www.ajg.com/us/-/media/files/gallagher/us/cyber-insurance-market-conditions-january2022.pdf.
24. Cyber Insurance Market Overview: Fourth Quarter 2021. *Marsh*. URL: https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html.
25. Cyber risk insurance. URL: https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/.

26. Cybersecurity Regulations for Insurance Companies. URL: https://www.packetlabs.net/posts/cybersecurity-regulations-for-insurance-companies/.
27. Directive (eu) 2016/1148 of the European parliament and of the council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union.* L 194/1. 19.7.2016. URL:https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.
28. General Data Protection Regulation: Regulation (EU) 2016/679 in the current version of the OJ L 127, 23.5.2018. URL: https://gdpr-info.eu/.
29. Global cybersecurity market - growth, trends, covid-19 impact, and forecasts (2022 - 2027). *Mordor Intelligence.* URL: https://www.mordorintelligence.com/industry-reports/cyber-security-market.
30. Good cyber security – the foundations [El. resource]. – Financial Conduct Authority - 2017. – URL: https://www.fca.org.uk/publication/documents/cyber-security-infographic.pdf.
31. G. Zeller, M. Scherer. A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal*. August 2021. DOI:10.1007/s13385-021-00290-1.
32. Kaffenberger L. Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment. *Carnegie endowment for internation peace*. September 30, 2019. URL: https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911.
33. NAIC Report Show 2020 Premiums Grew 29.1% as Cyberthreats Rise. *National Association of Insurance Commissioners.* Nov. 8, 2021. URL: https://content.naic.org/article/naic-report-show-2020-premiums-grew-291-cyberthreats-rise.
34. How often do Cyber Attacks occur? URL: https://aag-it.com/how-often-do-cyber-attacks-occur/.

35. H1 2021 cyber insurance claims. Cyber Risk, Solved. URL: https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2021-07-Coalition-Cyber-Insurance-Claims-Report-2021-h1.pdf .
36. O. Mirsanova. ANALYSIS AND SYSTEMATISATION OF BASIC PRICING MODELS AND APPROACHES IN CYBER RISK INSURANCE. *On the Way to a Stable World: Security and Sustainable Development. San Diego, CA*. 2015. DOI:1017809/02(2015)-04.
37. Saket Modi. The success of cyber insurance lies in risk standardization. Security Magazine. April 8, 2022. URL:https://www.securitymagazine.com/articles/97391-the-success-of-cyber-insurance-lies-in-risk-standardization.
38. Sharply Rising Cyber Insurance Claims Signal Further Risk Challenges. *FITCH WIRE*. 15 Apr, 2021. URL: https://www.fitchratings.com/research/insurance/sharply-rising-cyber-insurance-claims-signal-further-risk-challenges-15-04-2021.
39. S. Romanovsky, L. Ablon, A. Kuehn, T. Jones. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity*. Volume 5. Issue 1. 2019. tyz002. DOI: https://doi.org/10.1093/cybsec/tyz002.
40. What Businesses are Most & Least Vulnerable to a Cyber Attack? URL: https://businessworld.net/blog/post/38/what-businesses-are-most-least-vulnerable-to-a-cyber-attack.
41. What Does a Cyber Liability Policy Cover? URL: https://www.thebalancesmb.com/what-s-covered-under-a-cyber-liability-policy-462459.
42. What is a catastrophe bond (or cat bond)? URL: https://www.artemis.bm/library/what-is-a-catastrophe-bond/.
43. What Isn’t Vulnerable to Cyber Attack? URL: https://partnerre.com/opinions_research/what-isnt-vulnerable-to-cyber-attack/.

44. Y. Antonio, S. Indratno, R. Simanjuntak. Cyber Insurance Ratemaking: A Graph Mining Approach. *Risks*. 2021. 9(12). 224. DOI: https://doi.org/10.3390/risks9120224.
45. Y. Babenko., R. Pikus. Cyber insurance: new opportunities for the insurance market of Ukraine. *Economy and state*. 2022. № 2. С. 134–140. DOI: 10.32702/2306-6806.2022.2.134.
46. Сайт страхової компанії AXA. URL: https://www.axa.com/en/press.
47. Сайт страхової компанії Helvetia Insurance. URL: https://www.helvetia.com/ch/web/en/corporate-customer/contact/services/premium-calculator/cyber-insurance.html/cyber/risk.

ДОДАТКИ

ДОДАТОК А

Таблиця А.1

Зведені дані для кореляційно-регресійного аналізу впливу факторних величин на кількість кібератка

Country	Attack	Victim	CSI	XNODE	Malware
Malta	42	17	40	18	27
Greece	41	11	48	22	23
Romania	41	18	59	28	26
Slovakia	40	9	36	18	31
Spain	40	12	52	22	24
Lithuania	39	13	50	23	29
Cyprus	39	14	49	22	31
Portugal	39	15	51	24	33
Hungary	39	14	53	22	28
Bulgaria	38	8	58	27	24
Slovenia	38	13	34	18	45
Croatia	37	14	59	24	30
Denmark	36	24	62	11	28
Latvia	35	16	69	21	28
Czech Rep	35	17	61	17	34
Poland	34	16	62	23	40
Ireland	33	17	68	13	30
Luxembourg	32	20	60	14	44
Austria	32	18	64	13	37
Belgium	32	20	67	15	39
Sweden	32	21	73	11	32
Italy	31	17	63	21	51
France	31	19	82	18	33
UK	31	21	78	13	33
Netherlands	30	27	76	14	44
Germany	30	17	68	13	42
Estonia	30	17	85	19	32
Finland	29	15	74	8	34

Джерело: складено автором на основі даних [19, 20, 22, 26, 29, 33].

ДОДАТОК Б

Таблиця Б.1

Базові премії за доходами

Дохід (у мільйонах)	**Щорічні валові базові премії**
0 - 10 дол	1913,91 дол
10 - 20 дол	2602,92 дол
20 - 50 дол	3502,46 дол
50 - 100 дол	5224,98 дол

Джерело: [39]

Таблиця Б.2

Граничні коефіцієнти

Обмеження	**Фактор**
500 000 доларів США	0.809
1 000 000 доларів США	1.000
2 000 000 доларів США	1.132
3 000 000 доларів США	1.245
4 000 000 доларів США	1.371
5 000 000 доларів США	1.405

Джерело: [39]

Таблиця Б.3

Історія претензій

Категорія	**Хв**	**Макс**
Дуже сприятливий	0,75	0,85
Сприятливий	0,9	0,99
Середній	1,0	1,0
Трохи несприятливий	1.01	1.15
Матеріально несприятливі	1.16	1,25
Дуже несприятливо	1,26	1.4
Надзвичайно несприятливий	1,41	1.7

Джерело: [39]

Таблиця Б.4

Перерва виробничого процесу

Промисловість	Період очікування (година)	Плата за переривання бізнесу (%)
Автосалон	10	10,0
Автомобільні послуги	10	10,0
Побутові послуги (наприклад, сантехніки, електрики, садівники)	8	5,0
Електронна комерція	24	50,0
Освіта - коледжі/університети (вища освіта)	8	5,0
Професійні послуги (крім юридичних послуг)	12	25,0
Ріелтор - комерційний / житловий	10	10,0
Ресторан	10	10,0
Роздрібна торгівля	24	50,0
Спортивні клуби / спортзали	8	5,0
Телекомунікації	24	50,0

Джерело: [39]

Таблиця Б.5

Чотири класи небезпеки

Клас	Опис	Фактор
1	Компанії, основна особиста інформація яких стосується працівників	0,804
2	Компанії, які зберігають інформацію про фінансові рахунки або номери рахунків для окремих клієнтів, але не зберігають номери соціального страхування клієнтів	1.000
3	Компанії з номерами соціального страхування клієнтів	1.497
4	Суб'єкти, які збирають і зберігають великий обсяг особливо чутливої особистої інформації, мають високий ризик втрати або викрадення цієї інформації та підлягають структурним обмеженням у витратах на безпеку.	1.905

Джерело: [39]

Таблиця Б.6

Галузевий ризик

Коефіцієнт класифікації галузі	**Зважування**
Некомерційний, немедичний	1,0
Для отримання прибутку, виробник	1.5
Для отримання прибутку, оптом	1.5
Для отримання прибутку, нетехнічний постачальник послуг	1.5
Комп'ютерні консультанти	2.0
Системна інтеграція	2.0
Виробник програмного забезпечення	2.0
Роздрібна торгівля	3.0
Охорона здоров'я	3.0
Бухгалтери	3.0
Фінансові	4.0
Великий ризик (понад $ 250 млн доходу)	5,0
Всі інші	3.0

Джерело: [39]

Таблиця Б.7

Основні модифікатори безпеки

Категорія	**Модифікація**		
	Нижче середнього	**Середній**	**Вище середнього**
Контроль конфіденційності	1.20	1.00	0,80
Контроль безпеки мережі	1.20	1.00	0,80
Контроль відповідальності за вміст	1.20	1.00	0,80
Політика безпеки ноутбуків та мобільних пристроїв	1.10	1.00	0,90
План реагування на випадки	1.10	1.00	0,90

Джерело: [39]

Таблиця Б.8

Ваговий коефіцієнт безпеки

Рейтинг	**Зважування**
Відмінно	0,75–0,85
Добре	0,85–1,00
Задовільно	1.00–1.25
Погано	1,25–1,50

Джерело: [39]