Хмельницький національний університет

Факультет економіки і управління

Кафедра фінансів, банківської справи, страхування та фондового ринку

КВАЛІФІКАЦІЙНА РОБОТА

Страхування кібер-ризиків: сутність та особливості реалізації за матеріалами ПрАТ «Українська пожежно-страхова компанія»

Рівень вищої освіти бакалавр

Галузь знань 07 «Управління та адміністрування»
Шифр і назва галузі знань

Спеціальність 072 «Фінанси, банківська справа та страхування»
Шифр і назва спеціальності

Освітня програма Фінанси, банківська справа та страхування

КВРФБС 022194.01.06.00

Виконав студент III курсу, група ФБСс-22-1 _____ Олена СЛОБОДЯНЮК
Шифр Підпис Ім'я, ПРІЗВИЩЕ

Керівник канд. екон. наук, доцент _____ Леся МАТВІЙЧУК
Науковий ступінь, учене звання Підпис Ім'я, ПРІЗВИЩЕ

Нормоконтролер _____ Олександр ФРАДИНСЬКИЙ
Підпис Ім'я, ПРІЗВИЩЕ

До захисту допускаю:
Завідувач кафедри фінансів, банківської справи, страхування та фондового ринку _____ Ніла ХРУЩ
Назва Підпис Ім'я, ПРІЗВИЩЕ

17.06 2025
Дата

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет економіки і управління
Кафедра фінансів, банківської справи, страхування та фондового ринку
Рівень вищої освіти бакалавр
Галузь знань 07 «Управління та адміністрування»
Шифр і найменування
Спеціальність 072 «Фінанси, банківська справа та страхування»
Шифр і найменування
Освітня програма «Фінанси, банківська справа та страхування»

ЗАТВЕРДЖУЮ
Завідувач кафедри ФБСС
Ніла ХРУЩ
10 02 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Слободянюк Олени Валентинівни
Прізвище, ім'я, по батькові студента

1 Тема роботи: Страхування кібер-ризиків: сутність та особливості реалізації за матеріалами ПрАТ «Українська пожежно-страхова компанія»
Керівник роботи Матвійчук Леся Олексіївна, канд. екон. наук, доцент
Прізвище, ім'я, по батькові, науковий ступінь, учене звання
Затверджено наказом ректора університету від 07.02.2025 № 23 (додаток № 5)

2 Строк подання студентом роботи на кафедру до 07.06.2025

3 Вихідні дані до роботи: законодавчі та нормативні акти; спеціальна методична та наукова література (вітчизняні та зарубіжні видання); періодичні видання за темою дослідження; фінансова звітність ПрАТ «Українська пожежно-страхова компанія»

4 Зміст роботи (перелік питань, що їх належить розробити)
1 Теоретичні засади страхування кібер-ризиків
2 Аналітико-практичні аспекти страхування кібер-ризиків

5 Перелік графічного матеріалу:
1. Підходи до побудови страхового покриття кібер-ризиків
2. Механізм організації страхування кібер-ризиків
3. Функції страхування кібер-ризиків
4. Динаміка валових страхових премій вітчизняних страховиків у 2022-2024 роках
5. Динаміка валових страхових виплат здійснених вітчизняними страховими компаніями у 2022-2024 роках
6. Динаміка зобов'язань за страховими контрактами ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках
7. Динаміка зобов'язань за страховими контрактами з кібер-страхування ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках

6.Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийня

7 Дата видачі завдання: 10 лютого 2025 року

КАЛЕНДАРНИЙ ПЛАН

Назва розділів (етапів) кваліфікаційної роботи	Строк виконання	Примітк
1 Затвердження плану кваліфікаційної роботи	до 10.04.2025	Виконано
2 Аналіз, систематизація економічної літератури, збір та обробка статистичних матеріалів, фінансової звітності за темою кваліфікаційної роботи	до 25.04.2025	Виконано
3 Написання текстової частини кваліфікаційної роботи	до 25.05.2025	Виконано
4 Підготовка ілюстративних матеріалів та оформлення кваліфікаційної роботи	до 01.06.2025	Виконано
5 Попередній захист кваліфікаційної роботи	до 14.06.2025	Виконано
6 Захист кваліфікаційної роботи	з 18.06.2025	Виконано

Студентка _____ Підпис Олена СЛОБОДЯНЮК Ім'я, ПРІЗВИЩЕ

Керівник роботи _____ Підпис Леся МАТВІЙЧУК Ім'я, ПРІЗВИЩЕ

АНОТАЦІЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Студент: Олена СЛОБОЛЯНЮК

Керівник: Леся МАТВІЙЧУК, к.е.н, доцент

Тема роботи: Страхування кібер-ризиків: сутність та особливості реалізації за матеріалами ПрАТ «Українська пожежно-страхова компанія»

Ключові слова: страхова компанія, кібер-ризики, страхування кібер-ризиків, механізм організації страхування кібер-ризиків, асистанс.

Мета роботи: поглиблення теоретико-методичних положень і практичних підходів до страхування кібер-ризиків.

Об'єктом кваліфікаційної роботи є страхування кібер-ризиків.

Предмет дослідження є теоретико-методичні аспекти та практичні рекомендації щодо організації страхування кібер-ризиків.

За результатами дослідження сформульовані такі висновки: проаналізовано погляди науковців на сутність поняття «страхування кібер-ризиків», визначено особливості страхування кібер-ризиків, систематизовано функції кіберстрахування, виокремлено види кібер-ризиків та напрями кіберстрахування. Розглянуто особливості організації страхування кібер-ризиків.

Визначені такі перспективи (шляхи) розвитку: розроблено напрями удосконалення страхування кібер-ризиків.

Структура та обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, двох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг кваліфікаційної роботи – 54 сторінки друкованого тексту. Робота містить 8 таблиць, 7 рисунків та 3 додатки. Список використаних джерел налічує 40 найменування.

Дата виконання кваліфікаційної роботи 06.06.2025

Дата захисту кваліфікаційної роботи 18.06.2025

Студент _____ Олена СЛОБОЛЯНЮК _____

(ім'я, ПРІЗВИЩЕ) (підпис)

Зміст

Вступ 5
1 Теоретичні засади страхування кібер-ризиків 7
1.1 Економічна сутність та особливості страхування кібер-ризиків 7
1.2 Механізм організації страхування кібер-ризиків 15
2 Аналітико-практичні аспекти страхування кібер-ризиків 25
2.1 Аналіз сучасного стану страхового ринку України та фінансово-господарської діяльності ПрАТ «Українська пожежно-страхова компанія» за 2022-2024 роки 25
2.2 Напрями удосконалення страхування кібер-ризиків ПрАТ «Українська пожежно-страхова компанія» 38
Висновки 46
Список використаних джерел 49
Додатки 54

Вступ

У сучасну цифрову епоху кіберпростір стає не лише ключовим чинником розвитку бізнесу, державних інституцій і суспільства загалом, але й джерелом нових загроз і викликів. З кожним роком кількість кіберінцидентів невпинно зростає, охоплюючи все більше сфер суспільного життя. Хакерські атаки, витоки персональних даних, порушення безперервності бізнес-процесів – усе це спричиняє суттєві фінансові збитки та підриває довіру до цифрових технологій. У таких умовах актуалізується потреба в ефективних механізмах управління кібер-ризиками, одним із яких є страхування. Незважаючи на активний розвиток цього сегмента на світовому ринку, в Україні він знаходиться на етапі становлення, що зумовлює необхідність дослідження його сутності, структури страхових продуктів та практичних аспектів реалізації.

Тематика кіберстрахування є об’єктом наукових досліджень низки вітчизняних та зарубіжних науковців, серед яких Н.В. Приказюк, В.Д. Базилевич, Н.Г. Нагайчук, Н.М. Внукова, О.Є, Гудзь, О.О. Гаманкова, Р.В. Пікус. Водночас питання формування та просування страхування кібер-ризиків досі залишаються недостатньо опрацьованими та потребують подальших наукових досліджень.

Метою кваліфікаційної роботи є поглиблення теоретико-методичних положень і практичних підходів до страхування кібер-ризиків.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

– визначити сутність та особливості страхування кібер-ризиків;

– систематизувати види та напрями страхування кібер-ризиків;

– дослідити організаційні аспекти створення та просування продуктів із страхування кібер-ризиків;

– проаналізувати сучасний стан розвитку страхового ринку та ринку кіберстрахування;

– визначити напрями удосконалення страхування кібер-ризиків.

Об’єктом кваліфікаційної роботи є страхування кібер-ризиків.

Предмет дослідження є теоретико-методичні аспекти та практичні рекомендації щодо організації страхування кібер-ризиків.

Методи дослідження. У ході дослідження було застосовано як загальнотеоретичні, так і спеціальні методи наукового пізнання. Зокрема, для уточнення наукових підходів до трактування поняття кібер-ризиків використовувалися методи критичного аналізу наукових джерел і наукової абстракції; для розкриття сутності та основних функцій страхування кібер-ризиків – методи абстрагування та конкретизації; для оцінки фінансово-господарської діяльності ПрАТ «Українська пожежно-страхова компанія» та для визначення сучасних тенденцій розвитку ринку страхових послуг України – методи аналізу й синтезу, а також порівняльний аналіз; для наочного представлення результатів дослідження – табличні та графічні методи.

Практична значимість одержаних результатів полягає у визначені особливостей страхування кібер-ризиків, систематизації видів кіберстрахування та розробці напрямів удосконалення страхування кібер-ризиків.

Інформаційну основу дослідження становлять: законодавчі акти та нормативні документи, що регулюють сферу страхування, кібербезпеки та захисту інформації; наукові публікації, монографії, аналітичні звіти міжнародних організацій, які аналізують тенденції ринку кіберстрахування; фінансова звітність ПрАТ «Українська пожежно-страхова компанія», матеріали страхової компанії, що містять описи страхових продуктів у сфері страхування кібер-ризиків.

Структура та обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, двох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг кваліфікаційної роботи – 54 сторінки друкованого тексту. Робота містить 8 таблиць, 7 рисунків та 3 додатки. Список використаних джерел налічує 40 найменування.

1 Теоретичні засади страхування кібер-ризиків

1.1 Економічна сутність та особливості страхування кібер-ризиків

В умовах глобалізації та трансформації економічного середовища спостерігається інтенсивна цифровізація всіх сфер суспільного життя, що зумовлює суттєві зміни у функціонуванні економічних систем, інституцій та бізнес-середовища. Цифрові технології дедалі активніше інтегруються у виробничі процеси, управлінські моделі та комунікаційні платформи, сприяючи підвищенню ефективності, продуктивності та інноваційності. Водночас із перевагами цифрової трансформації посилюються і загрози, пов’язані з вразливістю цифрового простору до техногенних, соціальних та криміногенних чинників. Становлення цифрової економіки супроводжується появою нових ризиків – кібер-ризиків, які можуть завдати значних збитків суб’єктам господарювання та інституціям. «Економічні наслідки реалізації кібер-ризиків можуть проявлятися як у формі прямих, так і непрямих втрат. До прямих належать безпосередні фінансові витрати, пов’язані з необхідністю проведення внутрішнього розслідування інциденту, залучення юридичної підтримки, інформування клієнтів про порушення в роботі інформаційної системи, а також впровадження додаткових заходів із підвищення рівня кібербезпеки. Непрямі втрати, у свою чергу, включають втрату ділової репутації, недоотримання доходів, зниження вартості інтелектуальних активів тощо» [1, с.87].

Одним із найбільш дієвих механізмів мінімізації негативних наслідків кібер-ризиків виступає страхування, яке забезпечує фінансову компенсацію у випадку настання страхового випадку, пов’язаного з кіберінцидентами. Страхування кібер-ризиків, як специфічний різновид страхових послуг, покликане підвищити рівень кіберстійкості суб’єктів економічної діяльності та сприяти зміцненню загальнонаціональної системи кібербезпеки. У зв’язку з

цим розвиток страхування кібер-ризиків набуває пріоритетного значення в умовах цифровізації економіки.

З метою визначення сутності поняття «страхування кібер-ризиків» розглянемо погляди науковців на його зміст (таблиця 1.1).

Таблиця 1.1 – Систематизація поглядів науковців на зміст поняття «страхування кібер-ризиків»

Автор	Визначення поняття «страхування кібер-ризиків»
Р. Пікус, Ю. Бабенко	«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» [22, с. 136].
Н. Нагайчук, Н. Третяк, О. Ткаленко	«Складова ризик-менеджменту підприємства, що представляє собою – фінансовий механізм відновлення після значних збитків, метою якого є допомога страхувальникам повернутися до нормального функціонування, зберегти стабільність, платоспроможність та знизити витрати, пов’язані з перервами у виробництві, викликаними дією кібер-ризиків. З позиції страхувальників кібер-страхування – метод управління ризиками й захист від різноманітних загроз, що виникають при здійсненні електронної комерції» [16, с.104]
Д. Попович, Н. Бундз, В. Іванків	«Вид страхування, який надає захист від ризиків, пов’язаних з кібербезпекою» [23, с.169].
В. Апацький, І. Тарасенко	«Страховий продукт, який призначений для захисту компанії від ризиків, пов’язаних із використанням мережі Інтернет та із ризиками, що виникають під час використання інформаційних технологій, ІТ-інфраструктури та діяльності підприємства в кіберпросторі» [1, с.86].
Н. Приказюк, Л. Гуменюк	«Правовідносини, що виникають між страхувальником та страховиком у процесі передачі кібер-ризику останньому для захисту його безпеки, включаючи фінансову та кібербезпеку, через асекурацію майнових інтересів страхувальників від наслідків настання страхових подій у кіберпросторі шляхом виплати страхового відшкодування та / або пост-інцидентного супроводу до повного відновлення постраждалих об’єктів» [25].
А. Шолойко	«Інструмент передачі страховику на договірній основі несприятливих фінансових наслідків ризиків, що виникають у кіберпросторі з фізичними та юридичними особами (страхувальниками), задля зміцнення їх фінансової безпеки шляхом виплати страхового відшкодування» [39, с. 103].
О. Гудзь	«Страховий продукт, який захищає економічні суб’єкти від ризиків, що відносяться до інформаційно-комунікаційних технологій, використання Інтернет - мережі, ІКТ-інфраструктури та діяльності у кібер-просторі» [8, с. 5].

Джерело: систематизовано автором на основі [1,8,16,22,23,25,39]

У результаті аналізу підходів до визначення сутності кіберстрахування, можна виокремити три основні напрями його трактування: по-перше, як окремий вид страхового продукту; по-друге, як форму страхового полісу або контракту; по-третє, як інструмент чи метод управління кібер-ризиками.

Кіберстрахування забезпечує покриття фінансових втрат, спричинених пошкодженням або втратою інформації, що зберігається в інформаційно-технологічних системах та мережах. Окрім компенсації збитків, такі страхові продукти, як правило, передбачають надання комплексної підтримки у реагуванні на кіберінциденти, зокрема в частині управління кризовими ситуаціями, що є особливо важливим у випадках репутаційних втрат або дотримання вимог примусового регулювання.

У сучасному цифровому середовищі кібер-ризики стали одними з найнебезпечніших загроз для бізнесу, державних установ і приватних осіб. Тому страхування кіберризиків набуває дедалі більшого значення як інструмент управління ризиками та забезпечення фінансової стійкості. Його основні завдання охоплюють декілька ключових напрямів: забезпечення фінансового захисту від наслідків кіберінцидентів; мінімізація операційних і бізнес-ризиків; компенсація репутаційних втрат; планування та прогнозування кіберризиків.

Одним із головних завдань страхування кібер-ризиків є надання фінансової підтримки страхувальникам у разі настання кіберінциденту. Страховий поліс покриває витрати на відновлення роботи, спеціалістів з кібербезпеки, сповіщення потерпілих осіб, аудит, а також інші витрати, пов’язані з подоланням наслідків атаки; юридичний захист та відповідальність перед третіми особами. Кіберстрахування сприяє зменшенню потенційного впливу кіберзагроз на повсякденну діяльність фізичних та юридичних осіб. В умовах, коли багато процесів залежить від цифрових технологій, збої в роботі IT-систем можуть призводити до серйозних зупинок у роботі.

Репутаційні ризики є надзвичайно важливими в епоху цифрової відкритості. У разі витоку даних клієнтів компанія може втратити довіру з боку клієнтів, партнерів та інвесторів. Страховий поліс може покривати витрати на

кризові PR-заходи, інформаційну підтримку, відновлення іміджу компанії та юридичні консультації щодо публічних комунікацій.

Часто наслідки кіберінцидентів виходять за межі самої компанії – можуть бути скомпрометовані клієнти, партнери або інших сторін. Це призводить до судових позовів, вимог про компенсацію та втручання регуляторів. Кіберстрахування передбачає покриття витрат на юридичний захист, сплату штрафів, витрати на врегулювання претензій тощо.

Ще одне важливе завдання – сприяння довгостроковому управлінню ризиками. Наявність кіберстрахування допомагає компаніям усвідомлювати потенційні загрози, оцінювати вразливості та враховувати ці фактори при стратегічному плануванні, впровадженні нових технологій або розширенні бізнесу.

Підходи до побудови страхового покриття кібер-ризиків наведені на рисунку 1.1

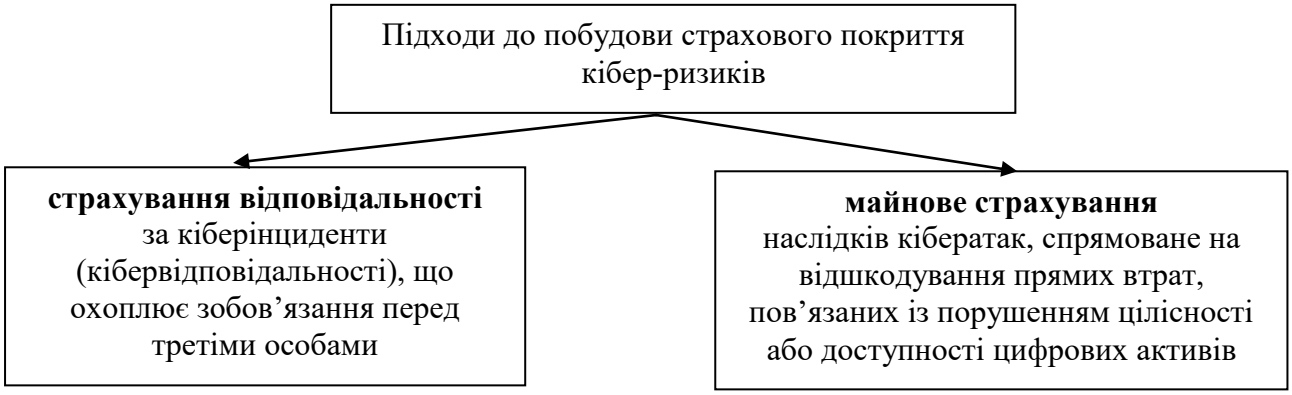

Рисунок 1.1 – Підходи до побудови страхового покриття кібер-ризиків

Джерело: побудовано автором на основі [1,8,16,22,23,25,39]

Страхування відповідальності за кіберінциденти може виникати у випадках порушення конфіденційності, цілісності або доступності даних третіх осіб, що обробляються, зберігаються або передаються за допомогою інформаційних систем страхувальника. Крім того, об'єктом страхового захисту може бути відповідальність за нанесення шкоди стабільній роботі інших суб'єктів унаслідок кіберінциденту, спричиненого недоліками в системах безпеки або діяльністю самого страхувальника.

«Другий підхід до формування страхового покриття у сфері кіберстрахування ґрунтується на типах можливих кібератак і кіберінцидентів, з якими може зіткнутися компанія, а також на характері об’єктів, що зазнають негативного впливу в результаті таких подій» [22, с.136]. У межах цього підходу страхові продукти розробляються з урахуванням конкретних загроз – таких як різного роду атаки, шкідливе програмне забезпечення (включаючи програми-вимагачі), несанкціонований доступ до інформаційних систем, витоки конфіденційних даних, а також інші форми кіберзлочинності, що можуть призвести до фінансових втрат або порушення безперервності бізнес-процесів. Окрему увагу в межах цього підходу приділяють ідентифікації об'єктів, які можуть постраждати внаслідок кібератак (сервери, бази даних, мережі, програмне забезпечення). Також важливо враховувати і зовнішні зобов’язання підприємства, до прикладу, відповідальність перед клієнтами або партнерами за неналежне збереження чи обробку даних. Страхове покриття формулюється відповідно до специфіки загроз і сфери їх впливу, що дозволяє адаптувати поліс до індивідуальних ризиків конкретної організації. Цей підхід передбачає гнучкість у розробці страхових програм і дозволяє забезпечити більш точне покриття тих аспектів діяльності компанії, які є найбільш вразливими до кіберзагроз.

«Однією з форм додаткового покриття в межах кіберстрахування може бути компенсація вартості технічної заміни, яка передбачає відшкодування витрат на оновлення або заміну пошкодженого обладнання. Такий тип страхового покриття відноситься до категорії майнового страхування» [22,с.136].

Таким чином, страхування кібер-ризиків охоплює широкий спектр майнових інтересів, враховуючи як внутрішні ресурси підприємства, так і зобов’язання перед зовнішніми контрагентами, що зумовлює складність і багатовимірність побудови відповідних страхових продуктів.

Розглянемо детальніше види кібер-ризиків та напрями кіберстрахування (таблиця 1.2.).

Таблиця 1.2 – Види кібер-ризиків та напрями кіберстрахування

Види кібер-ризиків	Напрям кіберстрахування
Ризик несанкціонованого доступу через злам паролів, втрати інформації або порушення функціонування систем внаслідок DDoS-атак.	Страхування кібер-ризик, пов'язаних із втратою даних і порушенням роботи комп'ютерної системи. Кіберстрахування передбачає компенсацію витрат, необхідних для відновлення інформаційно-технологічної інфраструктури, зокрема таких ресурсів, як веб-сайти.
Ризик фінансових втрат через збій комп'ютерної системи	Відповідний напрям кіберстрахування спрямований на захист суб'єктів господарювання від фінансових втрат, спричинених кіберзлочинною діяльністю у разі збоїв у функціонуванні комп'ютерних систем. Такий формат страхового захисту є особливо актуальним для онлайн-бізнесів, зокрема інтернет-магазинів, цифрових медіа-сервісів (наприклад, онлайн-кінотеатрів), а також платформ на зразок торрент-трекерів.
Ризик збитків внаслідок крадіжки, розкриття або використання особистої інформації	Такий вид страхування спрямований на компенсацію втрат, заподіяних власникам персональних даних при їх втраті або несанкціонованого використання.
Ризик фінансових збитків унаслідок вимагання, що виникає в результаті блокування комп'ютерних систем шкідливим програмним забезпеченням (вірусами).	Кібервимагання проявляється у формі примусового стягнення оплати за відновлення доступу до інформаційних систем або даних, які були попередньо заблоковані шляхом втручання в роботу програмного забезпечення чи баз даних. Кіберстрахування передбачає відшкодування витрат, пов'язаних із розблокуванням заблокованих ресурсів, за умови належного підтвердження фактичних витрат страхувальника та документального засвідчення факту кіберзлочину.
Ризик витрати коштів на відновлення програмного забезпечення або інформації внаслідок дії кіберзлочинців	Кіберстрахування в цьому випадку передбачає компенсацію витрат на відновлення пошкодженого програмного забезпечення та/або втрачених даних.

Джерело [23, с.169]

Одна з головних особливостей страхування кібер-ризиків полягає в невизначеності та динамічності ризиків, що підлягають страхуванню. Кібератаки постійно змінюються, стають складнішими й менш передбачуваними, що ускладнює актуарну оцінку й тарифікацію страхових продуктів. Часто безпека окремої системи залежить не лише від її власних механізмів захисту, а й від рівня кібербезпеки пов'язаних з нею зовнішніх систем. У сучасному цифровому середовищі компанії активно взаємодіють із партнерами, постачальниками та клієнтами, створюючи численні канали обміну даними. Якщо одна з цих сторон виявиться вразливою до кіберзагроз, це може створити ризик і для всієї мережі. Зокрема, шкідливе програмне забезпечення

може проникнути в систему саме через такий канал зв’язку з недостатньо захищеною партнерською організацією. У зв’язку з цим страхові компанії змушені застосовувати індивідуальний підхід до кожного страхувальника з урахуванням рівня їхньої кібербезпеки, особливостей ІТ-інфраструктури, галузевої належності та масштабів операцій.

Другою важливою рисою є інтегрований характер страхового покриття, який охоплює як прямі, так і непрямі збитки.

Ще одна характерна особливість полягає в комплексному характері страхової послуги, що поєднує страхових і сервісні елементи. Так, у межах страхування кібер-ризиків страхувальник, у разі настання страхового випадку, отримує не лише компенсацію збитків, тобто виплату страхового відшкодування, а й має змогу отримати професійну допомогу з управління загрозами, включаючи послуги спеціалістів із кібербезпеки, консалтинг, реагування на інциденти, проведення криміналістичних досліджень тощо.

Особливістю страхування кібер-ризиків є конфіденційності та регуляторна відповідальності. У контексті жорстких вимог до захисту персональних даних кіберстрахування може включати відповідальність за витоки інформації або порушення режиму її обробки.

Крім того, страхування кібер-ризиків вирізняється необхідністю залучення висококваліфікованих спеціалістів як під час розробки страхових продуктів так і під час оцінки збитків. Поліси розробляються під конкретні бізнес-моделі та типи діяльності: інтернет-магазини, фінансові установи, телекомунікаційні компанії, освітні заклади, медичні установи тощо. Такий підхід забезпечує релевантність страхового покриття до реальних загроз, притаманних кожному виду діяльності.

«Кіберризики становлять суттєвий виклик для страхової сфери, оскільки бракує достовірних і тривалих даних про масштаб можливих збитків, що ускладнює застосування традиційних моделей оцінки ризиків. До того ж, характер кіберзагроз постійно змінюється в умовах цифрової трансформації бізнесу, що потребує гнучкого підходу та комплексних рішень, які виходять за межі звичайного страхового покриття» [16, с.105].

Систематизація особливостей страхування кібер-ризиків за різними аспектами прояву, які пов’язані із специфікою надання страхових послуг наведена у таблиці 1.3

Таблиця 1.3 – Особливості страхування кібер-ризиків за різними аспектами прояву, які пов’язані із специфікою надання страхових послуг

Специфіка надання страхових послуг	Характеристика страхування кібер-ризиків
Аквізиційний процес	Страховик не завжди володіє тим самим обсягом інформації, що й страхувальник, адже частина даних нерідко має обмежений або засекречений характер і не підлягають розголошенню
	Чітке встановлення меж страхового покриття ускладнюється тим, що страхувальнику важко заздалегідь ідентифікувати всі можливі ризики
	Поліси страхування кібер-ризиків, як правило, включають численні виключення та обмеження, що звужують обсяг покриття та впливають на рівень реальних виплат
Андерайтинговий процес	Складність оцінити збитки, що пов’язано з природою інформаційних активів (вартість ноу-хау чи вартість репутації)
	Відсутність відкритих статистичних даних про кіберзагрози, зумовлена конфіденційністю таких випадків, позбавляє страховиків можливості об’єктивно аналізувати надійність страхових продуктів
	Постійна еволюція кіберзагроз, з огляду на змінність і непередбачуваність методів, що використовуються кіберзлочинцями, значно ускладнює процес оцінювання вартості страхових полісів
Комплікація прийняття ризику	Індивідуальність страхових продуктів для кожного страхувальника з врахуванням специфіки його діяльності
	Взаємозалежність безпеки означає, що рівень захисту однієї системи або мережі може залежить від захисту інших мереж через які і потрапляє вірус
Ліквідаційні процеси	Складність оцінити збитки, оскільки вартість інформаційних активів важко вирахувати, що пов’язано з природою інформаційних активів (ноу-хау чи вартість репутації)
	Складність визначення відповідальність, оскільки за умови здійснення кібератаки, страхова компанія має встановити рівень відповідальності за збитки і визначити, хто несе відповідальність за нанесену шкоду (до прикладу відповідальність може бути покладена на власника систем або розробника програмного забезпечення тощо)
	Період, протягом якого можна заявити страховий випадок, ускладнюється в умовах кіберзагроз. Часто атаки залишаються непоміченими одразу, а їхні наслідки виявляються лише через певний час після вторгнення. Деякі кібератаки можуть тривати місяцями, непомітно впливаючи на систему. Це створює додаткові труднощі для страховиків, оскільки постає питання: яким чином і за яких умов слід компенсувати понесені збитки

Джерело: систематизовано та доповнено автором на основі [16,25,26]

Страхові компанії, перед укладанням договору страхування, як правило, висувають умови щодо рівня інформаційної безпеки суб’єкта господарювання. Вимоги страховиків стимулюють страхувальників до активних дій у сфері кіберзахисту. Це пояснюється тим, що страхові компанії, оцінюючи ризики, пов'язані з кіберінцидентами, намагаються мінімізувати свої потенційні збитки. Тому вони часто висувають чіткі умови щодо рівня захищеності інформаційних систем страхувальника, які необхідно виконати для отримання страхового покриття. Це включає розробку та впровадження відповідних політик, що визначають правила та процедури забезпечення інформаційної безпеки, модернізацію інфраструктури, тобто оновлення апаратного та програмного забезпечення, систем захисту, навчання персоналу для підвищення обізнаності про кіберзагрози та методи їх запобігання, а також системне управління ризиками, що передбачає ідентифікацію, оцінку та моніторинг потенційних кіберзагроз. У такий спосіб, страхування виконує подвійне завдання: забезпечує фінансовий захист у разі настання кіберінциденту, покриваючи витрати на відновлення, юридичні витрати та інші збитки, і сприяє підвищенню рівня кіберстійкості компанії, спонукаючи її до вжиття проактивних заходів для захисту від кіберзагроз. Це, в свою чергу, зменшує ймовірність настання страхового випадку та позитивно впливає на загальну безпеку цифрового середовища.

1.2 Механізм організації страхування кібер-ризиків

Розвиток цифрової економіки, що прискорюється завдяки стрімкому технологічному прогресу, робить питання кібербезпеки як ніколи актуальним. Сьогодні, коли бізнес, державні установи та індивідуальні користувачі все більше залежать від цифрових технологій, ризики кіберзагроз набувають безпрецедентного масштабу. Від витоків конфіденційних даних до складних хакерських атак – наслідки кіберінцидентів можуть призводити до значних

фінансових втрат, репутаційної шкоди та порушення бізнес-процесів. У відповідь на зростаючу загрозу кібератак бізнес все частіше вдається до страхування як інструменту захисту, що стимулює попит на такі страхові послуги. Страхування кібер-ризиків стає не лише способом компенсації збитків, а й важливим елементом комплексної стратегії управління ризиками.

Механізм організації страхування кібер-ризиків наведено на рисунку 1.2

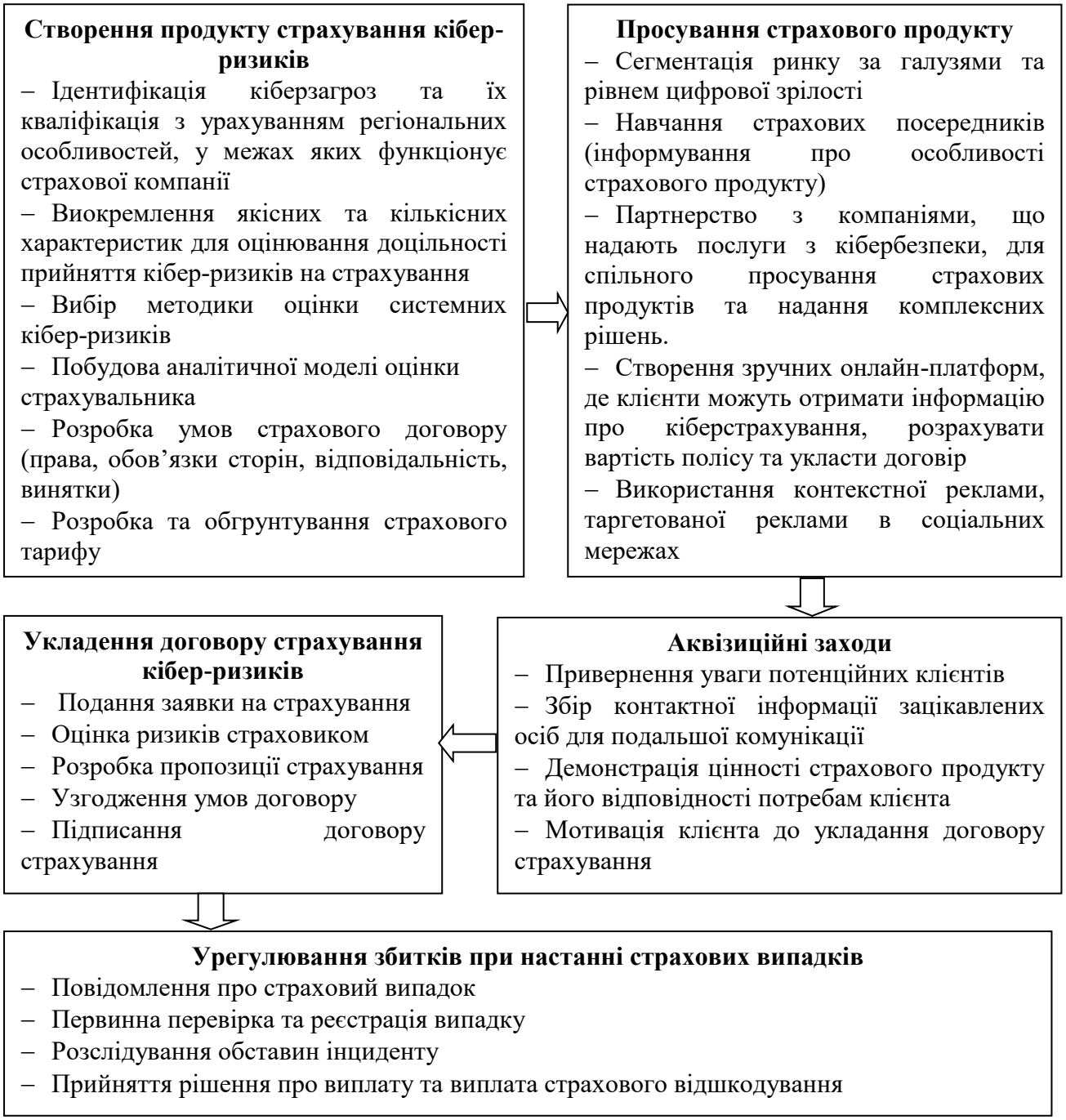

Рисунок 1.2 – Механізм організації страхування кібер-ризиків

Джерело: систематизовано та доповнено автором

Механізм організації страхування кібер-ризиків є динамічною, багатоетапною системою, що поєднує страхові, технічні, юридичні та освітні компоненти, які забезпечують ефективне управління фінансовими наслідками кіберінцидентів шляхом їх страхового покриття. Він охоплює сукупність дій, процедур, суб'єктів і нормативно-правових інструментів, які формують процес укладання, реалізації та виконання договору страхування кібер-ризиків. Його ефективність значною мірою залежить від якості андеррайтингу, рівня цифрової зрілості страхувальника та готовності сторін до спільного управління ризиками в умовах стрімко змінного кіберсередовища.

На етапі розробки страхового продукту відбувається комплексна і всебічна ідентифікація кібер-ризиків, які можуть становити потенційну загрозу для страхувальників. Страховик проводить аналіз цифрового середовища, у якому функціонують потенційні страхувальники, з метою визначення релевантних об’єктів страхового захисту. На основі проведеного аналізу формується базовий перелік кібер-ризиків, що потенційно можуть бути включені до покриття майбутнього договору страхування. До таких ризиків можуть належати: несанкціонований доступ до інформаційних систем, витік або втрата конфіденційної інформації, атаки типу «відмова в обслуговуванні» (DDoS), шкідливе програмне забезпечення (включно з програмами-здирниками), кібер-шантаж, втрати внаслідок збоїв у цифровій інфраструктурі, відповідальність перед третіми особами за порушення захисту даних тощо. Зазначений перелік має універсальний характер і охоплює увесь спектр потенційних кібер-ризиків. Водночас остаточний обсяг страхового покриття визначається індивідуально, з урахуванням особливостей діяльності конкретного страхувальника, рівня цифровізації його бізнес-процесів, архітектури кібербезпеки, а також ступеня вразливості до певних типів загроз. Таким чином, пріоритетність включення окремих ризиків до договору страхування варіюється і потребує глибокої аналітичної оцінки з боку страховика.

«У сфері страхування кіберризиків особливе значення має методологія оцінки кіберзагроз, оскільки вона є основою для формування ефективного

страхового захисту. Основна мета такої оцінки полягає у комплексному аналізі ризиків, пов’язаних з інформаційною безпекою організації. Завдання оцінки є: виявити загрози, які спрямовані на активи; визначити та спрогнозувати якомога більш точно наслідки реалізації кіберризиків; виявити вразливі місця для кібер-загроз в інформаційній безпеці організації; проаналізувати наявні методи контролю ризиків та визначити той, який дозволить мінімізувати виявлені загрози; оцінити ймовірність виникнення та реалізації кіберризиків» [1, с. 87].

Ще однією важливою складовою етапу розробки страхового продукту є розробка страхового тарифу. Формування страхових тарифів у сфері кібер-страхування є досить складним процесом, який потребує ґрунтовного аналізу технічних, економічних та правових аспектів кіберризиків. На відміну від традиційних видів страхування, де тарифи базуються на накопичених статистичних даних за тривалий період, за програмами страхуванн кібер-ризиків відсутня достатня історична база, що значно ускладнює актуарні розрахунки.

Серед ключових особливостей розробки тарифу з кібер-страхування можна виділити такі: високий рівень динамічності ризиків, індивідуалізація тарифу, обмеженість та неоднорідність статистичних даних, варіювання в залежності від набору покриттів, що включені до договору, висока ступінь кореляції ризиків. На відміну від більшості традиційних ризиків, кібер-ризики мають глобальний характер. Одна масштабна атака (наприклад, вірус або уразливість у популярному програмному забезпеченні) може вплинути на велику кількість страхувальників одночасно. Це потребує запровадження механізмів перестрахування та лімітів відповідальності. У процесі формування тарифу страховик часто залучає ІТ-фахівців, аудиторів з кібербезпеки або сторонні компанії для проведення попереднього аудиту систем захисту страхувальника. Результати такого аудиту мають суттєвий вплив на рівень тарифу.

Наступним етапом є етап просування страхових продуктів з кібер-страхування. «Страховим компаніям сьогодні важливо стимулювати попит на пропоновані продукти через їх активне просування на ринку, збільшення їх

доступності онлайн, враховуючи тенденції та проблеми розвитку страхового ринку України» [14, с.176]. Кібер-страхування є порівняно новим і специфічним видом страхового захисту, що потребує нестандартного підходу до просування на ринку. На відміну від традиційних страхових продуктів, просування кібер-страхування стикається з низкою викликів, пов'язаних із низьким рівнем обізнаності клієнтів, технічною складністю продукту та відсутністю регуляторного зобов'язання на його придбання. У зв'язку з цим, маркетингові стратегії потребують адаптації до цільової аудиторії, освітнього компонента та тісної співпраці з фахівцями з ІТ-сфери.

На наступному етапі є залучення страхувальника та розробка індивідуальної страхової пропозиції та обрання уніфікованого страхового пакету.

На наступному етапі відбувається подача заявки до страхової компанії. Страхова компанія в свою чергу здійснює оцінку кібер-ризиків страхувальника, здійснюється визначення рівня захищеності інформаційних ресурсів та каналів передачі даних, а також інших критичних елементів кіберзахисту.

Процес аналізу може включати на два етапи:

– перший етап – поверхневий скринінг, який здійснюється без залучення профільних фахівців з кібербезпеки і має на меті загальну оцінку відповідності страхувальника базовим критеріям прийнятності;

– другого етапу – поглиблений аудиту із залученням спеціалісти у сфері кібербезпеки.

Фахівці з кібербезпеки надають експертний висновок щодо поточного стану кіберзахисту страхувальника. На підставі результатів цієї перевірки страховик проводить оцінку рівня ризику та класифікує його як прийнятний або неприйнятний для укладення договору страхування. У випадку виявлення критичних вразливостей або недоліків у системі безпеки, на цьому ж етапі страховик, самостійно або спільно з експертами, розробляє дорожню карту з усунення виявлених проблем, яка містить конкретні заходи для підвищення рівня кіберзахисту страхувальника та приведення його у відповідність до вимог страхового покриття.

«Критерії, що дозволяють ідентифікувати кібер-ризик як страховий:

– ймовірність настання страхового випадку (складна для точного прогнозування, що ускладнює оцінку та прийняття на страхування кібер-ризиків);

– максимально можлива втрата (піддається достатньо точному визначенню, не створює суттєвих труднощів в оцінці);

– середня втрата на подію (не є проблематичною для оцінки);

– експозиція втрат (обсяг активів, підданих ризику піддається кількісному аналізу);

– страхова премія (визначення розміру премії можливе, хоча може вимагати складних розрахунків, але загалом не є надмірно проблематичним)» [16, с.103].

Такий підхід дозволяє оптимізувати ресурси страховика, зосереджуючи експертну увагу лише на тих суб'єктах, які вже продемонстрували базовий рівень кіберстійкості та потенційно придатні до страхування за результатами попередньої оцінки.

Якщо прийнято позитивне рішення про укладення договору страхування кібер-ризиків, то відбувається формування проєкту договору страхування, який детально регламентує умови надання страхового захисту від кібер-ризиків. Цей документ є результатом попередніх аналітичних, актуарних та консультаційних дій і відображає ключові параметри майбутніх договірних відносин. У процесі підготовки договору систематизується та інтегрується інформація, отримана на попередніх етапах, що охоплює: перелік доступного страхового покриття, класифікацію страхових і нестрахових випадків, винятки з покриття, розмір страхової суми, тарифна ставка, умови визнання страхового випадку, обмеження щодо виплат за різними групами ризиків, а також строк дії договору. Також на даному етапі узгоджуються права, обов’язки і відповідальність сторін договору, що є особливо важливим для забезпечення юридичної визначеності та балансу інтересів. У контексті страхування кібер-ризиків до ключових сторін договору, крім страховика та потенційного страхувальника, можуть також долучатися експерти з кібербезпеки, які

виконують роль незалежних оцінювачів технічного стану систем, здійснюють аудит або супровід реагування на інциденти.

Участь експертів з кібербезпеки може бути закріплена як обов’язкова умова договору, особливо у випадках страхування середніх і великих підприємств із критично важливою ІТ-інфраструктурою або значним обсягом персональних/конфіденційних даних. У деяких випадках страхові компанії самостійно залучають партнерські кібербезпекові фірми, які діють на підставі субпідрядних або акредитованих угод і гарантують належний рівень незалежності оцінок. Експерти з кібербезпеки стають інтегрованим елементом механізму кіберстрахування, сприяючи більш точному оцінюванню ризиків, зниженню ймовірності помилкових рішень щодо виплат і підвищенню довіри до страхового продукту з боку клієнтів.

Останнім етапом механізму організації страхування кібер-ризиків є виплата страхового відшкодування у разі настання страхового випадку. Цей етап передбачає реалізацію зобов’язань страховика перед страхувальником відповідно до умов укладеного договору. Процедура починається з повідомлення страхувальником про факт кіберінциденту в установлені строки. Після цього страховик проводить розслідування та перевірку обставин події, за необхідності залучаючи фахівців з кібербезпеки для технічного та юридичного аналізу ситуації. Далі здійснюється оцінка масштабів завданих збитків, включаючи фінансові втрати, репутаційні ризики, витрати на відновлення інфраструктури та інші супутні витрати, передбачені договором. На підставі отриманих даних ухвалюється рішення про доцільність виплати, її обсяг і порядок реалізації. У разі позитивного рішення страховик перераховує узгоджену суму страхової виплати страхувальнику або, за окремими умовами, третім сторонам, які беруть участь у подоланні наслідків кібератак.

Після завершення виплати страхова компанія може провести підсумковий аналіз врегулювання випадку, який враховується під час подальшого оцінювання ризиків. Цей етап є не лише завершальним, а й ключовим з точки зору формування довіри до страхового продукту, адже саме він демонструє ефективність і практичну цінність кіберстрахування для бізнесу.

Економічна сутність страхування кібер-ризиків розкривається шляхом аналізу його специфічних функціональних проявів. Кібер-страхування, як особливий страховий продукт виконує як загальні так і спеціальні функції (рисунок 1.3).

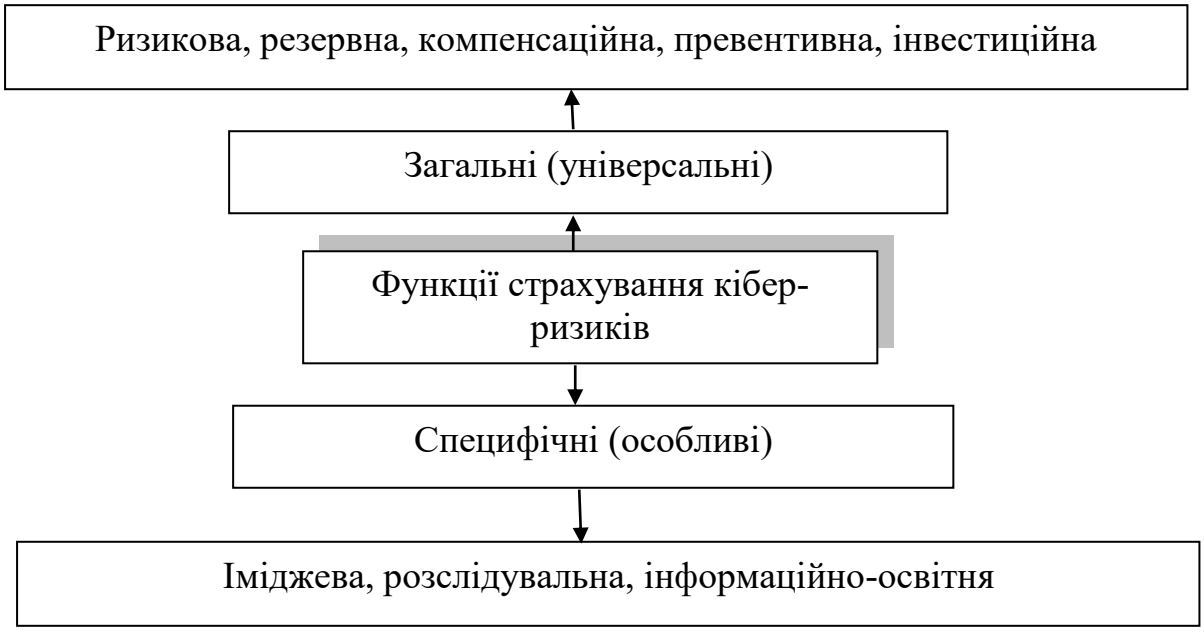

Рисунок 1.3 – Функції страхування кібер-ризиків

Джерело: систематизовано автором на основі [16,25,26,40]

До універсальних функцій страхування, які набувають актуальності й у контексті страхування кібер-ризиків, належать:

– ризикова функція, що полягає у прийнятті страховиком на себе кібер-ризиків страхувальника на визначених умовах та за визначену плату, яка передбачена договором страхування;

– резервна функція передбачає формування страхових резервів за договорами кібер-страхування з метою забезпечення платоспроможності страховика та здійснення виплат страхувальникам у разі настання страхових випадків;

– компенсаційна функція, сутність якої полягає у відшкодуванні збитків понесених страхувальником, у разі настання страхового випадку;

– превентивна функція, що реалізується через здійснення комплексу заходів, спрямованих на зниження ймовірності виникнення або мінімізацію наслідків кібер-ризиків;

– інвестиційна функція, що полягає у розміщенні страхових резервів з метою отримання інвестиційного прибутку страховиком.

Водночас специфіка страхування кібер-ризиків зумовлює розширення традиційного переліку базових функцій, доповнюючи його новими, зокрема:

– іміджевою функцією, яка полягає у розробці та реалізації заходів для відновлення репутації страхувальника до рівня, що існував до настання страхового випадку, за умови наявності відповідного положення у страховому договорі. Реалізація цієї функції може передбачати як самостійне розроблення страховиком комплексу заходів із репутаційного відновлення, так і покриття витрат на їх розробку і реалізацію;

– розслідувальна функція, яка передбачає здійснення самою страховою компанією розслідування страхового випадку або відшкодування відповідних витрат, якщо така опція передбачена умовами страхового договору. У випадках, коли страхувальник, а особливо це стосується юридичних осіб, не має у своєму складі спеціалізованих підрозділів або кваліфікованих фахівців у сфері кібербезпеки, ідентифікація джерела кібер-ризику є досить складною. Під час виникнення таких ситуацій страховик, використовуючи надану страхувальником інформацію, здійснює аналітичну оцінку з метою оперативного виявлення потенційних вразливих зон або, за необхідності, залучає зовнішніх фахівців з кібербезпеки для проведення поглибленого розслідування. Витрати, пов’язані з реалізацією таких заходів, можуть компенсуватися страховиком у разі внесення такого пункту до умов страхового договору;

–- інформаційно-освітня функція передбачає впровадження превентивних заходів, спрямованих на підвищення рівня обізнаності страхувальників щодо основ інформаційної безпеки та сучасних загроз у кіберпросторі. Реалізація цієї функції відбувається, зокрема, через залучення страховиком кваліфікованих експертів у сфері кібербезпеки, які здійснюють діагностику рівня цифрової

грамотності страхувальника. Якщо страхувальником є фізична особо, то така оцінка зосереджена на індивідуальному рівні знань, навичок і практик безпечного використання цифрових ресурсів. Якщо страхувальником є юридична особа, то аналіз охоплює більш широкий спектр – компетентність персоналу, наявність внутрішніх політик інформаційної безпеки, а також загальну культуру кібергігієни в організації. У разі виявлення недостатнього рівня підготовки розробляється стратегія покращення цифрової обізнаності, яка може включати проведення спеціалізованих тренінгів, навчальних програм, консультацій або впровадження корпоративних стандартів з питань кібербезпеки. Інформаційно-освітня функція виступає не лише як інструмент зниження ймовірності настання страхового випадку, але й як чинник формування сталого підходу до управління кіберризиками в довгостроковій перспективі.

2 Аналітико-практичні аспекти страхування кібер-ризиків

2.1 Аналіз сучасного стану страхового ринку України та фінансово-господарської діяльності ПрАТ «Українська пожежно-страхова компанія» за 2022-2024 роки

Динамічний розвиток цифрової економіки, зумовлений безперервним удосконаленням технологій, висуває на перший план питання кібербезпеки. Зростання обсягів обробки, зберігання та передавання даних у цифровому середовищі супроводжується збільшенням потенційних загроз і вразливостей, які можуть бути використані зловмисниками. Розвиток хмарних обчислень, штучного інтелекту та інших інноваційних рішень, з одного боку, забезпечує нові можливості для бізнесу, державного управління та суспільства загалом, а з іншого – створює додаткові виклики у сфері інформаційної безпеки. У цих умовах питання забезпечення кіберзахисту стає критично важливим для сталого функціонування цифрової інфраструктури, збереження довіри користувачів та запобігання фінансовим і репутаційним втратам.

За даними Державної служби спеціального зв’язку та захисту інформації у 2024 році в Україні зафіксовано 4315 кібератак, що на 69,8 % більше порівняно з 2023 роком, коли було зареєстровано 2541 випадок [19].

«У 2023 році в Україні було зафіксовано 2541 кіберінциденти, що на 15,9 % більше порівняно з 2022 роком. Упродовж 2022 року країна зазнала близько 7000 кібератак, спрямованих на об’єкти національної інформаційної інфраструктури. Україна посідає друге місце у світі за кількістю кібератак, поступаючись лише Сполученим Штатам Америки. Порівняно з 2021 роком, кількість атак у 2022 році зросла у 3,5 рази» [17, с. 281].

Протягом останніх трьох років об’єктами кібератак в Україні ставали державні та військові структури, підприємства комунального сектору,

банківські установи, логістичні компанії, оператори телекомунікацій, страхові організації, а також медіа і сфера інформаційного простору.

Такий стрімкий ріст загроз підкреслює актуальність впровадження ефективних засобів кіберзахисту як на державному, так і на приватному рівнях, одним з яких є страхування.

У 2020 році глобальний ринок кіберстрахування оцінювався в 7,8 мільярда доларів США [37, с.81]. За прогнозами аналітиків, обсяг щорічних страхових премій у сегменті кіберстрахування зросте з 16 мільярдів доларів США у 2024 році до 23 мільярдів у 2026 році, що свідчить про стабільний щорічний приріст на рівні 15–20 %. Втім, український ринок страхування кібер-ризиків перебуває на етапі зародження, лише деякі учасники страхового ринку пропонують страхові продукти, які покривають кібер-ризики, серед них СК «УПСК».

Попри зростання актуальності та необхідності кіберстрахування, цей продукт досі залишається досить дорогим, що може стримувати широке поширення на ринку. Висока вартість часто є перешкодою для малих і середніх підприємств, які не можуть собі дозволити витрати на таке страхування. Крім того, рівень обізнаності потенційних клієнтів щодо можливостей та переваг кіберстрахування залишається на досить низькому рівні. Часто підприємства не повністю усвідомлюють масштаби фінансових ризиків, пов’язаних з кібератаками, а також не розглядають кіберстрахування як невід’ємну частину системи управління ризиками. Це створює бар’єри для впровадження даного страхового продукту на ринку, попри його потенційну користь для захисту бізнесу від великих фінансових втрат.

Також розвиток кіберстрахування в Україні стримується складною ситуацією на ринку страхових послуг, зумовленою як економічними труднощами, так і впливом повномасштабної війни. Значний відтік страховиків з ринку, скорочення обсягів страхування та концентрація ресурсів на базових напрямах діяльності призводять до зменшення інвестицій у нові страхові продукти, зокрема й ті, що стосуються кібер-ризиків.

Запровадження нових ризикових страхових продуктів, таких як кіберстрахування, вимагає не лише фінансових ресурсів, а й залучення висококваліфікованих спеціалістів у сфері кібербезпеки, ІТ-аудиту, актуарних розрахунків та юридичного супроводу. У воєнний час це стає особливо складним завданням, адже більшість компаній зосереджені на підтримці основних процесів, забезпеченні платоспроможності та мінімізації витрат. Крім того, високий рівень невизначеності, зміни у законодавстві, обмеження на проведення міжнародних переказів та загальні ризики воєнного стану знижують готовність ринку до впровадження інновацій. У таких умовах пріоритет надається класичним видам страхування (життя, майна, транспорту), тоді як спеціалізовані продукти, що потребують глибокої технічної експертизи, відсуваються на другий план.

Проаналізуємо основні показники розвитку страхового ринку України у 2022-2024 роках (таблиця 2.1).

На основі проведеного аналізу відмітимо, що протягом аналізованого періоду кількість страхових компаній суттєво скоротилася. Так, у 2023 році, у порівнянні з 2022 роком їх кількість зменшилася на 21,09 % (- 27 страховиків) і склала 101 страховика. У 2024 році скорочення операторів страхового ринку продовжилося і на кінець року в Україні функціонувало лише 65 страхових компаній, що на 35,64 % менше, ніж у 2023 році. В цілому, протягом року з ринку пішло 36 страховиків.

Що стосується галузевої структури страхового ринку, то менший відтік спостерігався на ринку страхування життя, оскільки протягом аналізованого періоду лише 2 страхові компанії покинули ринок і станом на кінець 2024 року на ринку залишилося 10 лайфових страховиків.

Що стосується ринку страхування іншого, ніж страхування життя, то протягом аналізованого періоду ринок втратив 61 страхову компанію. Так, у 2023 році, у порівнянні з 2022 роком кількість страховиків зменшилася на 16,38 % (- 19 страховиків) і склала 97 компаній. У 2024 році, у порівнянні з 2023 роком кількість страховиків з ризикового страхування зменшилася на 43,3 % (- 42 страховика) і склала 55 компаній.

Таблиця 2.1 – Основні показники розвитку вітчизняного страхового ринку у 2022-2024 роках

Показники	Рік			Абсолютне відхилення (+,-), млн. грн		Відносне відхилення (приріст / зменшення), %	
	2022	2023	2024	2023/2022	2024/2023	2023/2022	2024/2023
Кількість зареєстрованих страхових компаній, на кінець року, од., із них:	128	101	65	-27	-36	-21,09	-35,64
страхові компанії, що здійснюють страхування життя, од.	12	12	10	0	-2	0	-16,67
страхові компанії, які здійснюють інші види страхування, ніж страхування життя, од.	116	97	55	-19	-42	-16,38	-43,30
Кількість укладених договорів страхування, за період, тис. одиниць	88003,0	94821,5	89962,1	6818,5	-4859,4	7,75	-5,12
Активи за балансом	70298,3	74412,2	72818,8	4113,9	-1593,4	5,85	-2,14
Обсяг сплачених статутних капіталів	6716,8	5955,6	5550,6	-761,2	-405	-11,33	-6,80
Сформовані страхові резерви	41000,6	46781,2	36653,6	5780,6	-10127,6	14,1	-21,65
Валові страхові премії, з них:	39661,8	47014,7	53078,9	7352,9	6064,2	18,54	12,90
від страхувальників – фізичних осіб	24551,6	28755,0	32965,7	4203,4	4210,7	17,12	14,64
від перестрахувальників	1131,6	1057,1	302,1	-74,5	-755	-6,58	-71,42
Валові страхові виплати, з них:	13001,4	16867,3	20861,4	3865,9	3994,1	29,73	23,68
страхувальникам – фізичним особам	7028,5	9150,7	13712,0	2122,2	4561,3	30,19	49,85
перестрахувальникам	176,8	133,6	104,4	-43,2	-29,2	-24,43	-21,86
Чисті страхові премії	38515,0	46011,0	48560,3	7496	2549,3	19,46	5,54
Чисті страхові виплати	12810,9	16736,1	18935,8	3925,2	2199,7	30,64	13,14
Обсяг страхових платежів, належних перестраховикам, із них:	4250,7	4650,3	4518,6	399,6	-131,7	9,4	-2,83
перестраховикам-нерезидентам	3103,9	3646,6	3983,7	542,7	337,1	17,48	9,24

Джерело: побудовано автором на основі [21]

Кількість укладених договорів страхування у 2023 році зросла на 7,75 % (на 6818,5 тис. одиниць) порівняно з 2022 роком і досягла 94821,5 тис. договорів. У 2024 році страхові компанії уклали 89962,1 тис. договорів, що на 5,12 % менше, ніж у 2023 році, що свідчить про помірне уповільнення динаміки розвитку страхового ринку.

У 2022 році загальний обсяг активів страхових компаній становив 70298,3 млн грн. У 2023 році він зріс на 5,85 % і досяг 74412,2 млн грн, що свідчить про стабільне зростання фінансової бази страхового сектора. Проте у 2024 році

активи скоротилися на 2,14 % – до 72818,8 млн грн, що було зумовлено як економічними викликами, так і зниженням ділової активності на страховому ринку. Така динаміка вказує на необхідність підвищення ефективності управління активами та посилити адаптацію до змін зовнішнього середовища.

У 2023 році обсяг резервів страхових компаній, у порівнянні з 2022 роком зріс на 14,1 % і склав 46781,2 млн грн. У 2024 році обсяг сформованих резервів, у порівнянні з 2023 роком скоротився на 21,65 % і склав 36653,6 тис. грн. Таке скорочення з одного боку викликане зменшенням обсягу укладених договорів страхування, а з іншого зміною динаміки та структури страхових продуктів (зростання частки короткострокових чи менш ризикованих договорів, які не потребують значних резервів).

Обсяг валових страхових премій у 2023 році, у порівнянні з 2022 роком зріс на 18,54 % або на 7352,9 млн грн і склав 47014,7 тис. грн. У 2024 році їх обсяг, у порівнянні з 2023 роком зріс на 12,9 % і склав 53078,9 тис. грн (рисунок 2.1).

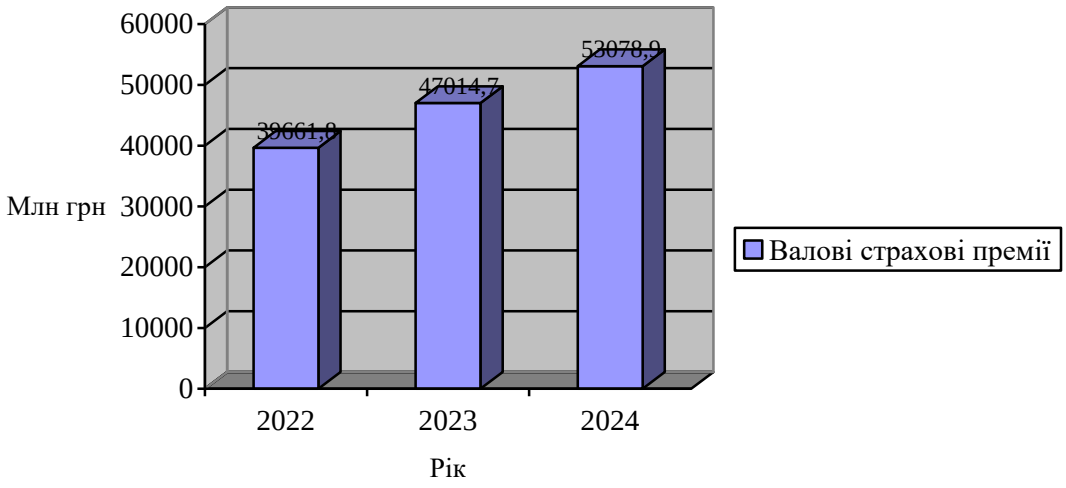

Рисунок 2.1 – Динаміка валових страхових премій вітчизняних страховиків у 2022-2024 роках

Джерело: складено на основі таблиці 2.1

У структурі валових страхових премій переважають страхові премії від страхувальників-фізичних осіб, частка яких у 2022 році складала 61,9 %, у 2023 році – 61,16 %, у 2024 році – 62,11 %.

Обсяг валових страхових премій, які надійшли від страхувальників-фізичних осіб, у 2023 році, у порівнянні з 2022 роком зріс на 17,12 % або на 4203,4 млн грн і склав 28755 млн грн. У 2024 році, у порівнянні з 2023 роком їх обсяг зріс на 14,64 % або на 4210,7 тис. грн і склав 32965,7 тис. грн.

У 2023 році валові страхові премії, отримані від перестрахувальників, становили 1057,1 млн грн, що було на 6,58 % менше порівняно з попереднім роком, що зумовлене коригуванням обсягів перестрахування, зміною умов співпраці з перестрахувальними компаніями або зменшенням загального рівня ризиків, переданих на перестрахування. Однак у 2024 році відбулося суттєве скорочення цього показника – на 71,42 % у порівнянні з 2023 роком. Така різка динаміка може свідчити про глибші структурні зміни у страховому секторі. Зокрема, зниження попиту на перестрахування з боку українських страховиків у зв’язку з переглядом внутрішніх ризиків або через намагання зменшити витрати на перестрахування в умовах економічної нестабільності; ускладнення співпраці з міжнародними перестраховиками, через воєнні ризики, зростання тарифів на перестрахування або посилення вимог до контрагентів.

Таке скорочення валових премій від перестрахувальників може негативно вплинути на диверсифікацію ризиків у страховому секторі та свідчить про необхідність адаптації ринку до нових умов. Страховим компаніям варто зважено підходити до балансування між прямим покриттям ризиків і передачею їх на перестрахування, особливо в умовах зростаючої економічної та політичної невизначеності.

У структурі валових страхових премій транспортне та особисте страхування залишаються домінуючими сегментами, забезпечуючи понад 80 % надходжень у сфері ризикового страхування.

Обсяг валових страхових виплат у 2023 році, у порівнянні з 2022 роком зріс на 29,73 % або на 3865,9 млн грн і склав 16867,3 тис. грн. У 2024 році їх

обсяг, у порівнянні з 2023 роком зріс на 23,68 % і склав 20861,4 тис. грн (рисунок 2.2).

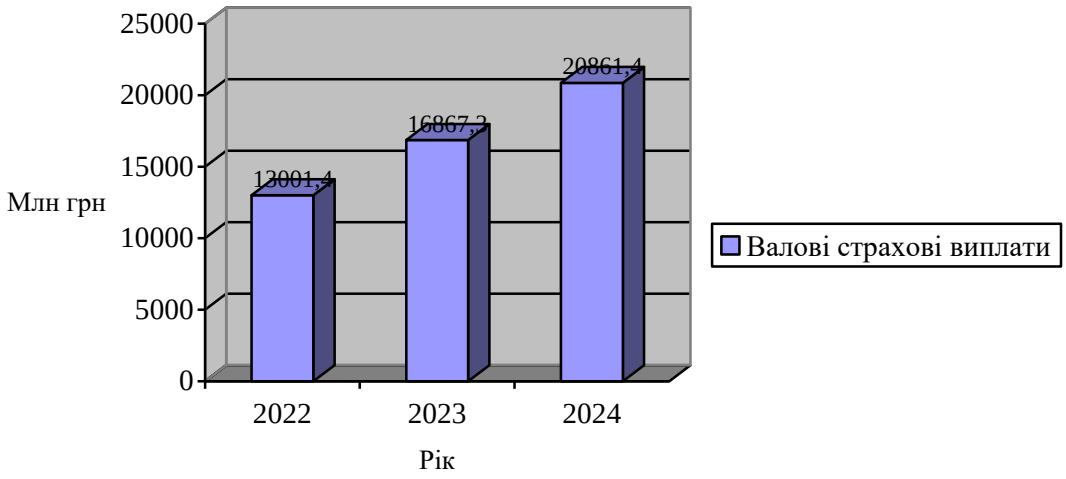

Рисунок 2.2 – Динаміка валових страхових виплат здійснених вітчизняними страховими компаніями у 2022-2024 роках

Джерело: складено на основі таблиці 2.1

У структурі валових страхових виплат переважають страхові виплати страхувальникам-фізичним особам, частка яких у 2022 році складала 54,06 %, у 2023 році – 54,25 %, у 2024 році – 65,73 %.

Обсяг валових страхових виплат, які здійснені страхувальникам-фізичним особам, у 2023 році, у порівнянні з 2022 роком зріс на 30,19 % або на 2122,2 млн грн і склав 9150,7 млн грн. У 2024 році, у порівнянні з 2023 роком їх обсяг зріс на 49,85 % або на 4561,3 тис. грн і склав 13712 тис. грн.

Валові страхові виплати перестрахувальникам у 2023 році склали 133,6 тис грн, що на 24,43 % менше, ніж у 2022 році. У 2024 році обсяг валових страхових випали перестрахувальникам зменшився на 21,6 % у порівнянні з 2023 роком і склав 104,4 тис. грн.

Аналіз динаміки чистих страхових премій за 2022–2024 роки свідчить про стабільне зростання цього ключового показника діяльності страхових компаній. Так, у 2023 році їх обсяг, у порівнянні з 2022 роком, зріс на 19,46 % і склав

46011,0 млн грн. У 2024 році обсяг чистих страхових премій склав 48560,3 млн грн, що на 5,54 % більше, ніж у 2023 році.

Зростання чистих премій означає, що страховики утримують більшу частину премій після вирахування тих, що передані на перестрахування. Це свідчить про підвищення ролі власного ризик-менеджменту і, ймовірно, посилення фінансової стійкості компаній, які готові покривати більші обсяги зобов'язань самостійно. Водночас темп уповільнення в 2024 році може сигналізувати про необхідність адаптації до нових економічних умов, змін у споживчій поведінці або перегляду регуляторної політики. Загалом, тенденція є позитивною, але з ознаками стабілізації, що вимагає від ринку гнучкості та інноваційного підходу до формування продуктів і тарифної політики.

Чисті страхові виплати у 2023 році склали 16736,1 млн грн, що на 30,64 % більше, ніж у 2022 році. У 2024 році їх обсяг зріс на 13,14 %, у порівнянні з 2023 роком, і склав 18932,8 млн грн. Зростання чистих страхових виплат у 2022-2024 роках свідчать про посилення навантаження на страхові компанії у зв'язку з підвищенням кількості страхових випадків та їхньої вартості.

Станом на кінець 2024 року всі страхові компанії виконували нормативні вимоги щодо капіталу платоспроможності та мінімального необхідного капіталу.

Проаналізувавши основні показники розвитку вітчизняного страхового ринку у 2022-2024 роках здійснимо аналіз діяльності ПрАТ «Українська пожежно-страхова компанія» на страховому ринку України.

ПрАТ «Українська пожежно-страхова компанія» є одним із лідерів вітчизняного страхового ринку. Страхова компанія розпочала роботу на ринку у 1992 року і за понад 32-річну історію діяльності сформувала розгалужену мережу відокремлених підрозділів і представництва в усіх регіонах країни. Компанія реалізує власні страхові продукти через понад 5000 пунктів продажу. Страхова компанія здійснює діяльність у сфері прямого страхування та вхідного перестрахування, охоплюючи повний спектр ризиків у межах 18 класів страхування, що включають 25 видів ризиків у рамках цих класів.

Проаналізуємо динаміка активів балансу ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках (таблиця 2.2).

Таблиця 2.2 − Динаміка активів балансу ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках

Показник	Роки, тис. грн			Абсолютне відхилення(+,-), тис. грн		Відносне відхилення, %	
	2022	2023	2024	2022/ 2023	2024 / 2023	2022/ 2023	2024 / 2023
Гроші та їх еквіваленти	306516	389891	454134	83375	64243	27,20	16,48
Активи за контрактами з перестрахування	5125	17786	25638	12661	7852	247,04	44,15
Необоротні активи, призначені на продаж	4205	2285	862	-1920	-1423	-45,66	-62,28
Інші активи	7558	8014	4844	456	-3170	6,03	-39,56
Кошти в централізованих джерелах	90826	79773	82355	-11053	2582	-12,17	3,24
Нематеріальні активи	952	538	42	-414	-496	-43,49	-92,19
Інвестиційна нерухомість	74369	156492	148190	82123	-8302	110,43	-5,31
Активи з права використання	16467	14984	13938	-1483	-1046	-9,01	-6,98
Власна нерухомість та обладнання	121639	36058	37949	-85581	1891	-70,36	5,24
Загальна сума активів	627657	705821	767952	78164	62131	12,45	8,80

Джерело : побудовано та пораховано за даними фінансової звітності страхової компанії

У 2022–2024 роках структура активів ПрАТ «Українська пожежно-страхова компанія» зазнала низки важливих змін, які свідчать про активну фінансову політику, спрямовану на оптимізацію ресурсів, посилення ліквідності та інвестиційний розвиток.

Позитивною динамікою відзначаються гроші та їх еквіваленти, обсяг яких постійно зростав: на 27,2 % у 2023 році та ще на 16,48 % у 2024-му. Це свідчить про покращення грошових потоків, що забезпечує компанії високу платоспроможність і фінансову гнучкість.

Суттєве зростання показали активи за контрактами з перестрахування – у 2023 році вони збільшилися майже в чотири рази (+247,04 %), а у 2024 – ще на 44,15 %. Це говорить про активне використання механізмів перестрахування для диверсифікації ризиків і зменшення потенційних зобов’язань.

Водночас компанія продовжила зменшення необоротних активів, призначених на продаж (- 45,66 % у 2023, - 62,28 % у 2024), що свідчить про

реалізацію або списання балансово неактивних ресурсів. Подібну динаміку мають і нематеріальні активи, які у 2024 році зменшилися на 92,19 % порівняно з попереднім роком, що вказує на завершення терміну дії прав або знецінення таких активів, що потребує оновлення інтелектуального потенціалу або IT-інфраструктури.

Інвестиційна нерухомість різко зросла в 2023 році більш ніж удвічі (+110,43 %), що свідчить про вкладення в прибуткову нерухомість. У 2024 році спостерігалося незначне її зниження (-5,31 %), що було результатом переоцінки та часткового відчуження.

Активи з права користування, пов’язані з орендованим майном, поступово скорочувалися протягом двох років, що свідчить про оптимізацію орендної політики компанії або завершення договорів оренди.

Значним є також зменшення власної нерухомості та обладнання – у 2023 році майже на 70 %, що пов’язано з продажем основних засобів або їх перекласифікацією до інвестиційної нерухомості. У 2024 році цей показник дещо виріс (+5,24 %), що свідчить про стабілізацію структури основних засобів.

Інші активи у 2024 році скоротилися на 39,56 %, що свідчить про списання або переоцінку низьколіквідних активів. Кошти в централізованих джерелах залишалися відносно стабільними, не демонструючи суттєвих змін.

Загалом, загальна сума активів зросла з 627657 тис. грн у 2022 році до 767952 тис. грн у 2024-му, що становить приріст на 22,37 % за два роки. Це свідчить про позитивну тенденцію у розвитку компанії, зокрема завдяки зростанню грошових коштів, активній роботі з перестрахуванням та інвестиційній діяльності.

ПрАТ «Українська пожежно-страхова компанія» демонструє збалансовану фінансову стратегію, що поєднує підвищення ліквідності, диверсифікацію ризиків, інвестиційне розширення та оптимізацію структури активів. Це забезпечує стійкість до зовнішніх впливів і створює передумови для подальшого зростання.

Проаналізувавши активи ПрАТ «Українська пожежно-страхова компанія» здійснимо аналіз пасиву балансу (таблиця 2.3).

Таблиця 2.3 − Динаміка пасиву балансу ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках

Показник	Роки, тис. грн			Абсолютне відхилення(+,-), тис. грн		Відносне відхилення, %	
	2022	2023	2024	2022/ 2023	2024 / 2023	2022/ 2023	2024 / 2023
Статутний капітал	100000	100000	100000	0	0	0	0
Капітал у дооцінках	70221	75345	69790	5124	-5555	7,30	-7,37
Резервний капітал	12859	15720	16005	2861	285	22,25	1,81
Нерозподілений прибуток	117248	111787	108054	-5461	-3733	-4,66	-3,34
Загальна сума власного капіталу	300328	302852	293849	2524	-9003	0,84	-2,97
Поточні зобов’язання з податку на прибуток	3174	5937	6019	2763	82	87,05	1,38
Інші поточні зобов’язання	28230	22212	21046	-6018	-1166	-21,32	-5,25
Зобов’язання за страховими контрактами	260365	335745	408786	75380	73041	28,95	21,75
Зобов’язання з оренди	19556	18476	17914	-1080	-562	-5,52	-3,04
Зобов’язання з виплати працівникам	3722	6637	7732	2915	1095	78,32	16,50
Зобов’язання за відстроченим податком на прибуток	12282	13962	12606	1680	-1356	13,68	-9,71
Загальна сума зобов’язань	327329	402969	474103	75640	71134	23,11	17,65
Загальна сума власного капіталу та зобов’язань	627626	705821	767952	78195	62131	12,46	8,80

Джерело : побудовано та пораховано за даними фінансової звітності страхової компанії

У 2022–2024 роках компанія демонструвала загалом стабільну, але неоднорідну фінансову динаміку. Статутний капітал залишався незмінним на рівні 100000 тис. грн протягом усього періоду. Страхова компанія не проводила додаткових емісій або змін у статутному капіталі, що свідчить про свідчить про стабільність базового капіталу, але також про відсутність інвестицій у розширення через цей інструмент.

Капітал у дооцінках у 2023 році збільшився на 7,3 %, внаслідок позитивної переоцінки активів, однак уже в 2024 році знизився на 7,37 %, що було результатом зниження ринкової вартості активів та консервативного підходу до їх оцінки. Резервний капітал зростав упродовж усього періоду (на 22,25 % у 2023 році та на 1,81 % у 2024 році), що свідчить про поступове зміцнення фінансової стабільності компанії.

Водночас нерозподілений прибуток демонстрував спадну динаміку: у 2023 році зменшився на 4,66 %, а в 2024 – ще на 3,34 %, що свідчить про активне використання прибутку на інші цілі (виплати, інвестиції, покриття збитків тощо). Загальна сума власного капіталу зросла лише на 0,84 % у 2023 році, а у 2024 році знизилася на 2,97 %, що є сигналом про обмеженість внутрішніх ресурсів компанії.

Поточні зобов'язання з податку на прибуток різко зросли у 2023 році (на 87,05 %), а в 2024 році майже не змінилися (+1,38 %), що може свідчити про різкі коливання податкового навантаження або прибутку. При цьому інші поточні зобов'язання суттєво скоротилися: на 21,32 % у 2023 році та ще на 5,25 % у 2024 році, що є позитивним результатом, свідчить про зменшення короткострокових боргових зобов'язань.

Найпомітнішим позитивним трендом є зростання зобов'язань за страховими контрактами – на 28,95 % у 2023 році та на 21,75 % у 2024 році. Це свідчить про активне укладання договорів та зростання довіри клієнтів до ПрАТ «Українська пожежно-страхова компанія», хоча й підвищує навантаження на резерви(рисунок 2.2).

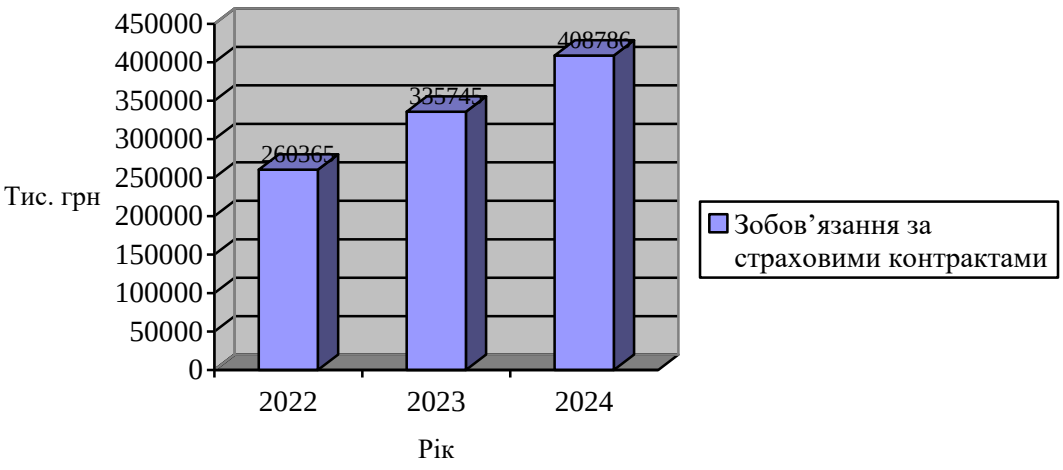

Рисунок 2.3 – Динаміка зобов'язань за страховими контрактами ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках

Джерело: складено на основі таблиці 2.3

Зобов’язання з оренди зменшувалися протягом обох років, що вказує на оптимізацію витрат на нерухомість та перегляд договорів оренди.

Зобов’язання з виплати працівникам зросли значно – на 78,32 % у 2023 році та ще на 16,5 % у 2024 році, що свідчить про підвищення заробітних плат або впровадження бонусних програм, однак потребує контролю для уникнення надмірного навантаження на фонд оплати праці.

Відстрочені податкові зобов’язання зросли у 2023 році (+13,68 %), проте знизилися у 2024 році на 9,71 %, що дозволяє зробити висновок про зміну в податкових розрахунках або прогнозах майбутніх податкових платежів ПрАТ «Українська пожежно-страхова компанія».

Загальна сума зобов’язань продовжує зростати: на 23,11 % у 2023 році та на 17,65 % у 2024 році, що свідчить про активне використання зовнішніх джерел фінансування. Водночас загальна сума власного капіталу та зобов’язань у 2023 році зросла на 12,46 %, а у 2024 – на 8,80 %, демонструючи поступове нарощування обсягів ресурсів, хоч і з переважанням зростання зобов’язань над власним капіталом.

На основі аналізу Звіту про прибутки та збитки, визначено, що за результати діяльності у 2022 році ПрАТ «Українська пожежно-страхова компанія» отримала прибуток в обсязі 122838 тис. грн. У 2023 році розмір прибутку склав 4954 тис. грн, що на 96,17 % менше, ніж у 2022 році. У 2024 році прибуток страхової компанії зріс, у порівнянні з 2023 роком на 218,69 % і склав 15788 тис. грн.

ПрАТ «Українська пожежно-страхова компанія» демонструє помірне зростання фінансових показників, активне залучення нових страхових контрактів та покращення структури поточних зобов’язань. Однак зниження нерозподіленого прибутку та домінування зобов’язань над зростанням власного капіталу вказують на необхідність зміцнення фінансової стійкості. Для забезпечення стабільного розвитку у довгостроковій перспективі доцільно зосередитися на підвищенні прибутковості, ефективному управлінні витратами (особливо на персонал) та підтримці балансу між власними та залученими ресурсами.

2.2 Напрями удосконалення страхування кібер-ризиків ПрАТ «Українська пожежно-страхова компанія»

На глобальному рівні ринок страхування кібер-ризиків демонструє впевнене зростання протягом останніх десяти років. Це зумовлено стрімкою цифровізацією бізнесу, активним розвитком інформаційних технологій та зростанням кількості і складності кіберзагроз. У відповідь на ці виклики страховики постійно вдосконалюють свої продукти: розширюються як види страхового покриття (включаючи захист від атак з використанням шкідливого програмного забезпечення, витоку конфіденційної інформації, фінансових шахрайств тощо), так і комплекс заходів щодо усунення або мінімізації наслідків кіберінцидентів, включаючи технічну, правову та PR-підтримку постраждалих компаній.

Водночас український страховий ринок лише починає формувати відповідну пропозицію. Продукти кіберстрахування представлені обмежено, а рівень обізнаності потенційних клієнтів про переваги такого захисту залишається низьким.

ПрАТ «Українська пожежно-страхова компанія» була однією з перших на ринку страхових послуг України, що забезпечувала своїм клієнтам захист від кіберзагроз. Продукт «Страхування кібер-ризиків» виступав ефективним інструментом для безпечного та зручного управління бізнесом в умовах цифровізації. Кібер-ризики охоплюють загрози, пов’язані з використанням комп’ютерної техніки та програмного забезпечення у таких сферах, як локальні мережі, глобальна мережа Інтернет, платіжні та облікові системи, онлайн-торгівля, спеціалізовані бізнес-системи, а також процеси збору, зберігання і використання персональних даних клієнтів і партнерів підприємства [21].

Протягом аналізованого періоду страхова компанія пропонувала кіберстрахування насамперед для юридичних осіб, діяльність яких в першу чергу пов’язана з обробкою, зберіганням або передачею конфіденційної інформації. До таких належать підприємства, що працюють з електронними

базами даних, співпрацюють із закордонними партнерами на умовах аутсорсингу або виконують контракти на надання ІТ-послуг.

Враховуючи специфіку діяльності потенційних страхувальників, ПрАТ «Українська пожежно-страхова компанія» виокремлювала основні групи ризиків, які можуть підлягати «страхуванню: втрата (повна або часткова) електронної бази даних; неможливість доступу до електронних даних; розповсюдження електронних даних; втрата прибутку від перерви у господарській діяльності через вплив таких кібер-небезпек: збій у роботі мережі; відмова роботи ІТ-інфраструктури; хакерська атака, атака комп'ютерного вірусу; помилка програмування; крадіжка електронних даних, несанкціоноване використання або змінення електронної системи третьою особою» [21].

Проаналізуємо основні показники розвитку страхування кібер-ризиків ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках (таблиця 2.4).

Таблиця 2.4 – Основні показники страхування кібер-ризиків ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках

Показник	Роки, тис. грн			Абсолютне відхилення(+,-), тис. грн		Відносне відхилення, %	
	2022	2023	2024	2022/ 2023	2024 / 2023	2022/ 2023	2024 / 2023
Зобов'язання за страховими контрактами	128	251	152	123	-99	96,09	-39,44
Доходи за договорами страхування кібер-ризиків	74	196	98	122	-98	164,86	-50,00
Витрати від страхової діяльності за страхуванням кібер-ризиків	132	275	140	143	-135	108,33	-49,09
Страхові премії	101	246	104	145	-142	143,56	-57,72
Страхові виплати	54	105	83	51	-22	94,44	-20,95

Джерело: побудовано та пораховано за даними фінансової звітності страхової компанії

У період з 2022 по 2024 рік простежується нестабільна динаміка основних фінансових показників страхування кібер-ризиків. У 2023 році показники за

даним видом страхування демонстрували зростання, однак у 2024 році спостерігається помітне зниження майже за всіма позиціями.

Зокрема, зобов'язання за страховими контрактами зросли з 128 тис. грн у 2022 році до 251 тис. грн у 2023 році, що становить приріст на 96,09 %. Проте вже у 2024 році цей показник знизився до 152 тис. грн (падіння на 39,44 % порівняно з попереднім роком). Така динаміка свідчити про зменшення обсягу нових укладених договорів та завершення раніше укладених контрактів (рисунок 2.4).

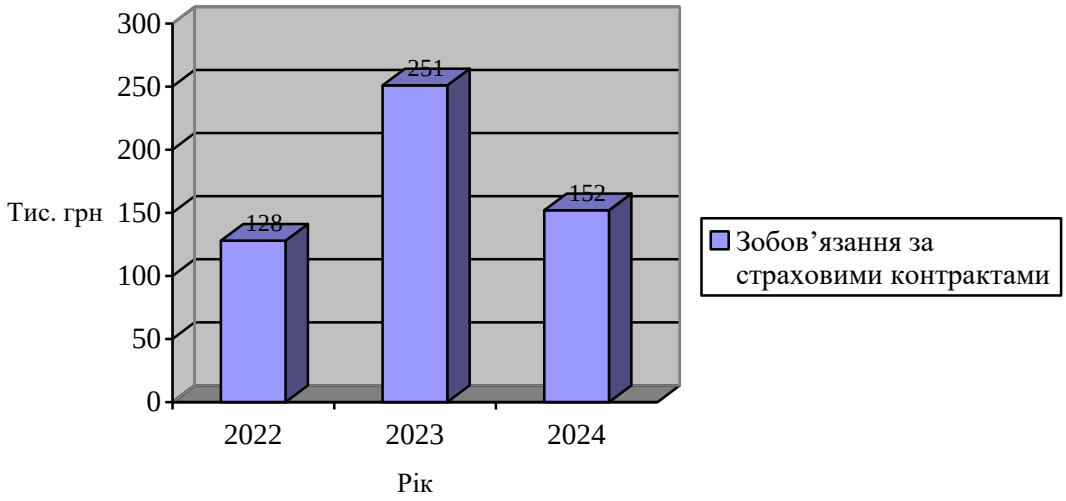

Рисунок 2.3 – Динаміка зобов'язань за страховими контрактами з кібер-страхування ПрАТ «Українська пожежно-страхова компанія» у 2022-2024 роках

Джерело: складено на основі таблиці 2.4

Доходи за договорами страхування кібер-ризиків також зросли у 2023 році більш ніж удвічі – з 74 тис. грн до 196 тис. грн (+164,86 %). Проте вже у 2024 році цей показник зменшився на 50 %, склавши лише 98 тис. грн, що вказує на зменшення попиту на страхування кібер-ризиків.

У сфері страхування кібер-ризиків витрати також зросли у 2023 році – з 132 тис. грн до 275 тис. грн (+108,33%). Проте у 2024 році вони зменшилися до 140 тис. грн (падіння на 49,09 %), що свідчить про зменшення виплат

страхувальникам за даним видом страхування та суттєве скорочення укладених договорів протягом року.

Подібна тенденція спостерігається і у страхових преміях: у 2022 році вони становили 101 тис. грн, у 2023 – 246 тис. грн (+ 143,56 %), але в 2024 – лише 104 тис. грн (зниження на 57,72 %), ще свідчить про нестабільність у притоку клієнтів та зміну стратегічного фокусу компанії.

Щодо страхових виплат, то вони також зросли у 2023 році з 54 тис. грн до 105 тис. грн (+ 94,44 %), а в 2024 зменшилися до 83 тис. грн (- 20,95 %).

У 2022–2024 роках страхування кібер-ризиків характеризується нестабільною динамікою фінансових показників. Після помітного зростання у 2023 році, яке було пов’язане із розширенням страхової програми по кіберзахисту, у 2024 році зафіксовано суттєве зниження практично за всіма ключовими показниками. Зниження зобов’язань за страховими контрактами, доходів, страхових премій та витрат свідчить про зменшення обсягу нових договорів, скорочення попиту на даний вид страхування, завершення короткострокових контрактів та зміну клієнтських пріоритетів. Зменшення страхових виплат також свідчить про зниження кількості страхових випадків та більш жорсткий андеррайтинг.

Загалом, така динаміка вказує на циклічність розвитку ринку кіберстрахування та потребу в адаптації стратегії страховиків до змін середовища. Для забезпечення сталого розвитку цього сегмента доцільно посилити аналітику ризиків, удосконалити страхові продукти, а також проводити інформаційно-освітню роботу серед потенційних клієнтів.

Незважаючи на високу актуальність страхування кібер-ризиків в умовах цифровізації економіки, зростання кількості кіберінцидентів та обмежену конкуренцію в цьому сегменті українського страхового ринку, ПрАТ «Українська пожежно-страхова компанія» ухвалило рішення про припинення надання даного страхового продукту. Таке рішення може бути зумовлене низкою внутрішніх факторів, зокрема переглядом стратегічних пріоритетів компанії, недостатнім рівнем попиту з боку клієнтів, а також необхідністю оптимізації витрат на адміністрування специфічних страхових послуг.

Водночас це створює потенційні можливості для інших страховиків, які готові інвестувати в розвиток кіберстрахування, враховуючи зростаючі ризики та потребу бізнесу у цифровому захисті.

Основні напрями удосконалення кіберстрахування, які можуть сприяти його розвитку та підвищенню ефективності як у ПрАТ «Українська пожежно-страхова компанія» так і в інших страхових компаніях наведені у таблиці 2.5.

Таблиця 2.5 – Основні напрями удосконалення страхування кібер-ризиків

Напрям	Заходи
Розширення страхового покриття	– включення нових ризиків: DDoS-атаки, інциденти з програмами-вимагачами, соціальна інженерія, внутрішні порушення тощо – відшкодування витрат на розслідування кібер-злочинів – страхування репутаційних втрат, фінансових збитків від простоїв, витрат на юридичну допомогу та PR-підтримку – врахування особливостей різних секторів (IT-компанії, охорона здоров'я, фінансовий сектор тощо) – витрати на захист у суді і відновлення роботи IT-системи
Персоналізація страхових продуктів	– розробка гнучких програм залежно від розміру бізнесу, рівня цифрової інфраструктури, типу оброблюваних даних. – створення пакетів для малого та середнього бізнесу з доступними умовами й преміями
Вдосконалення андеррайтингу та оцінки ризиків	– використання автоматизованих систем для аналізу кібер-ризиків та кіберзагроз – співпраця з IT-компаніями для попереднього аудиту IT-інфраструктури страхувальника – введення обов'язкових заходів з кібербезпеки як умови для укладання договору
Освітні ініціативи та підвищення обізнаності клієнтів	– проведення тренінгів, семінарів і вебінарів для бізнесу щодо важливості кіберстрахування – пояснення механізмів дії полісу, прикладів страхових випадків та переваг захисту
Впровадження цифрових технологій	– створення онлайн-платформ для оформлення полісів, подачі заявок та управління ризиками – застосування штучного інтелекту для моніторингу загроз і швидкої обробки страхових подій
Співпраця з IT компаніями та кібербезпековими компаніями	– формування партнерств для комплексного захисту клієнтів: страхування + технічний аудит + реагування на інциденти – можливість надання клієнтам доступу до антивірусних рішень, систем моніторингу чи швидкої технічної допомоги

Джерело: систематизовано та доповнено

На сьогодні українські страхові компанії здійснюють оцінку кібер-ризиків суб'єктів господарювання переважно на основі непрямих ознак, індикаторів і характеристик. «До таких відносяться: наявність впровадженої системи ризик-менеджменту, функціонування підрозділів економічної та інформаційної безпеки, використовувані методи і технології захисту конфіденційних даних, регулярність проведення аудиту та тестування систем інформаційної безпеки, а також чисельність і кваліфікація IT-персоналу» [8, с.7]. Такий підхід не дозволяє в повній мірі оцінити рівень кібер-ризику та сформувати адекватний страховий тариф, який з одного боку дозволить здійснити виплату страхового відшкодування, у разі настання страхового випадку, а з іншої сторони – буде посильним для страхувальника.

«Для забезпечення ефективного страхового захисту та обґрунтованих актуарних розрахунків необхідно, щоб регулятор страхового ринку – Національний банк України – ініціював систематичний збір і узагальнення даних про кіберінциденти. Наявність такої інформаційної бази дозволить актуаріям розробити відповідні статистичні моделі й актуарні таблиці за аналогією з майновим або страхуванням життя, що сприятиме точнішому розрахунку страхових тарифів та підвищенню надійності кіберстрахових продуктів» [22, с.138].

Одним із ключових напрямів удосконалення системи страхування кібер-ризиків в Україні є розвиток ефективної інституційно-правової бази, яка б забезпечувала прозорість, передбачуваність і стабільність цього сегмента ринку. Наразі законодавче регулювання у сфері кіберстрахування є фрагментарним і не охоплює всіх аспектів цифрових ризиків, що стримує як розвиток страхових продуктів, так і попит з боку бізнесу.

З метою зміцнення правових основ доцільно:

– розробити нормативні акти або внести зміни до чинного страхового законодавства з метою визначення поняття, класифікації та мінімальних вимог до страхування кібер-ризиків;

– передбачити обов’язкову або рекомендовану форму розкриття інформації про кіберінциденти для підприємств, щоб забезпечити зростання прозорості та створити статистичну базу для актуарних розрахунків;

– установити стандарти оцінки кібер-ризиків, які б орієнтували як страховиків, так і страхувальників на об’єктивні критерії;

– підвищити роль регулятора (НБУ) у координації дій між страховими компаніями, державними структурами та представниками кібербезпекового сектору;

– запровадити стимули для бізнесу, зокрема податкові пільги або преференції, для компаній, які укладають договори кіберстрахування та дотримуються заходів кіберзахисту.

Розбудова інституційно-правової системи кіберстрахування дозволить створити сприятливі умови для формування дієвого ринку страхування кібер-ризиків, підвищить рівень довіри до страхових продуктів і сприятиме загальному зростанню кіберстійкості економіки.

Страхування кібер-ризиків залишається складною і специфічною сферою, у якій потенційним страхувальникам часто важко обійтись без кваліфікованої допомоги менеджера. У зв’язку з цим страхові онлайн-платформи мають бути оснащені розширеними функціями підтримки користувачів. Служба підтримки повинна охоплювати всі наявні канали комунікації: телефон, електронну пошту, соціальні мережі, месенджери тощо, забезпечуючи зручність і швидкість взаємодії з потенційними клієнтами.

Забезпечення оперативного реагування на будь-який запит клієнта є одним із ключових чинників підвищення конкурентоспроможності страхової компанії, особливо в умовах цифрової трансформації ринку. Клієнти очікують швидких, точних і зручних відповідей незалежно від складності запиту чи часу доби. На першій лінії взаємодії з потенційними страхувальниками ефективним інструментом стають чат-боти, що працюють на основі генеративного штучного інтелекту (ШІ). Такі системи здатні автоматично обробляти й надавати вичерпні відповіді на стандартні запитання, пов’язані з умовами страхування, оформленням полісів, оплатами, процедурою врегулювання

страхових випадків тощо. Це дозволяє суттєво знизити навантаження на операторів кол-центрів і прискорити час реагування на типові запити.

Однак у ситуаціях, коли страхувальник зіштовхується з нетиповою проблемою, має індивідуальні умови договору або потребує персоналізованого підходу, важливо забезпечити швидкий перехід до спілкування з менеджером або оператором контакт-центру. Затримка в таких випадках може негативно вплинути на рівень довіри клієнта та його лояльність до страхового продукту.

Для реалізації такого рівня обслуговування необхідно інтегрувати сучасні цифрові технології, зокрема:

– CRM-системи, які зберігають історію взаємодії з кожним клієнтом, дозволяють сегментувати аудиторію та оперативно передавати запити відповідним фахівцям;

– IP-телефонію, що забезпечує надійний голосовий зв’язок та можливість гнучкого маршрутування дзвінків;

– системи обробки природної мови (NLP), які дозволяють чат-ботам «розуміти» наміри клієнта, аналізувати запити в реальному часі та адаптувати відповіді.

Висновки

У першому розділі кваліфікаційної роботи проаналізовано погляди науковців на зміст поняття «страхування кібер-ризиків», виокремлено галузі страхування до яких можна віднести кібер-страхування. Досліджено види кібер-ризиків та напрями кіберстрахування, виокремлено особливості страхування кібер-ризиків за різними аспектами прояву, які пов’язані із специфікою надання страхових послуг. У роботі досліджено механізм організації страхування кібер-ризиків, який охоплює сукупність дій та процедур, страхові, технічні, юридичні та освітні компоненти, які забезпечують ефективне управління фінансовими наслідками кіберінцидентів шляхом їх страхового покриття. У ході дослідження систематизовано та проаналізовано загальні та спеціальні функції, що виконує страхування кібер-ризиків.

У другому розділі кваліфікаційної роботи проаналізовано сучасний стан ринку страхування кібер-ризиків. Визначено, що у 2024 році в Україні зафіксовано 4315 кібератак, що на 69,8 % більше порівняно з 2023 роком, коли було зареєстровано 2541 випадок. Протягом останніх трьох років об’єктами кібератак в Україні ставали державні та військові структури, підприємства комунального сектору, банківські установи, логістичні компанії, оператори телекомунікацій, страхові організації, а також медіа і сфера інформаційного простору.

За прогнозами аналітиків, обсяг щорічних страхових премій у сегменті кіберстрахування зросте з 16 мільярдів доларів США у 2024 році до 23 мільярдів у 2026 році, що свідчить про стабільний щорічний приріст на рівні 15–20 %. Втім, український ринок страхування кібер-ризиків перебуває на етапі зародження, лише деякі учасники страхового ринку пропонують страхові продукти, які покривають кібер-ризики.

Попри зростання актуальності та необхідності кіберстрахування, цей продукт досі залишається досить дорогим, що може стримувати широке поширення на ринку. Висока вартість часто є перешкодою для малих і середніх

підприємств, які не можуть собі дозволити витрати на таке страхування. Крім того, рівень обізнаності потенційних клієнтів щодо можливостей та переваг кіберстрахування залишається на досить низькому рівні.

Також розвиток кіберстрахування в Україні стримується складною ситуацією на ринку страхових послуг. У роботі проаналізовано сучасний стан розвитку ринку страхових послуг України. Так, визначено, що протягом аналізованого періоду кількість страхових компаній суттєво скоротилася. Протягом 2024 року з ринку пішло 36 страховиків і на кінець року в Україні функціонувало лише 65 страхових компаній. В цілому ринок страхових послуг у 2024 року показав зростання за показниками валових страхових премій та валових страхових виплат. Як і в попередні роки драйверами ринку було транспортне та особисте страхування. Та, у 2024 році у структурі валових страхових премій транспортне та особисте страхування забезпечило понад 80 % надходжень у сфері ризикового страхування. Що стосується укладених договорів страхування, то протягом аналізованого періоду спостерігалася неоднозначна ситуація. У 2023 році кількість укладених договорів, у порівнянні з 2022 роком зросла, а от у 2024 році, у порівнянні з 2023 роком знову зменшилася.

Що стосується розвитку страхового ринку, то запровадження нових ризикових страхових продуктів, таких як кіберстрахування, вимагає не лише фінансових ресурсів, а й залучення висококваліфікованих спеціалістів у сфері кібербезпеки, ІТ-аудиту, актуарних розрахунків та юридичного супроводу. У воєнний час це стає особливо складним завданням, адже більшість компаній зосереджені на підтримці основних процесів, забезпеченні платоспроможності та мінімізації витрат.

У роботі здійснено аналіз діяльності ПрАТ «Українська пожежно-страхова компанія» на страховому ринку України та визначено, що страхова компанія демонструє помірне зростання фінансових показників, активне залучення нових страхових контрактів та покращення структури поточних зобов’язань. Однак зниження нерозподіленого прибутку та домінування зобов’язань над зростанням власного капіталу вказують на необхідність

зміцнення фінансової стійкості. Для забезпечення стабільного розвитку у довгостроковій перспективі доцільно зосередитися на підвищенні прибутковості, ефективному управлінні витратами (особливо на персонал) та підтримці балансу між власними та залученими ресурсами.

У роботі проаналізовано показники кібер-страхування та визначено, що ПрАТ «Українська пожежно-страхова компанія» була однією з перших на ринку страхових послуг України, що забезпечувала своїм клієнтам захист від кіберзагроз. Продукт «Страхування кібер-ризиків» виступав ефективним інструментом для безпечного та зручного управління бізнесом в умовах цифровізації.

У 2022–2024 роках страхування кібер-ризиків характеризується нестабільною динамікою фінансових показників. Динаміка вказує на циклічність розвитку ринку кіберстрахування та потребу в адаптації стратегії страховиків до змін середовища. Для забезпечення сталого розвитку цього сегмента доцільно посилити аналітику ризиків, удосконалити страхові продукти, а також проводити інформаційно-освітню роботу серед потенційних клієнтів.

У роботі запропоновані напрями удосконалення кіберстрахування, які можуть сприяти його розвитку та підвищенню ефективності як у ПрАТ «Українська пожежно-страхова компанія» так і в інших страхових компаніях. Також визначено, що досить важливим напрямом удосконалення системи страхування кібер-ризиків в Україні є розвиток ефективної інституційно-правової бази, яка б забезпечувала прозорість, передбачуваність і стабільність цього сегмента ринку. Наразі законодавче регулювання у сфері кіберстрахування є фрагментарним і не охоплює всіх аспектів цифрових ризиків, що стримує як розвиток страхових продуктів, так і попит з боку бізнесу.

Список використаних джерел

1. Апацький В. Проблеми та перспективи страхування кіберризиків в Україні / В. Апацький, І. Тарасенко // Проблеми інтеграції освіти, науки та бізнесу в умовах глобалізації: матеріали V Міжнар. наук.-пр. конф. (м. Київ, 6 жовтня 2023 р.). Київ: КНУТД, 2023. С. 86-87.

2. Богріновцева Л. Розвиток та впровадження інноваційних підходів до фінансового управління страховими компаніями в умовах воєнного стану [Електронний ресурс]/ Л. Богріновцева, О.Ключка, І. Заїчко // Економіка та суспільство. – 2024. – Вип.60. – Режим доступу: https://economyandsociety.in.ua/index.php/journal/article/view/3608/3539

3. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні / О.М. Бодунова // Науковий вісник Ужгородського національного університету. – 2023. – Т. 2, № 75. – С. 83–87.

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

5. Волинець В.В. Роль кіберстрахування у забезпеченні безпеки даних в онлайн торгівлі/ В.В, Волинець // Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. – 2024. – №4. –Том 35 (74). – С. 12-17

6. Волосович С. Детермінанти виникнення та реалізації кіберризиків / С.Волосович, Л.Клапків // Зовнішня торгівля: економіка, фінанси, право. – 2018. – № 3. – С. 101-115.

7. Гончаренко А. С. Стратегічні аспекти забезпечення фінансово-економічної безпеки страхових компаній у контексті розвитку конкурентоспроможного ринку страхових послуг / А.С. Гончаренко, Н.В. Зачосова, О.В. Коваль // Вісник Черкаського національного університету імені Богдана Хмельницького. Серія Економічні науки. – 2020. – № 2. – С. 160-168.

8. Гудзь О. Є. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці / О. Є. Гудзь // Економіка. Менеджмент. Бізнес. – 2019. – № 3. – С. 4-12.

9. Гуменюк Л. С. Трансформація продуктів кібер-страхування в умовах глобальної пандемії COVID-19 / Л.С. Гуменюк // Економіка. Фінанси. Бізнес. Управління. Зміни. Адаптація. Нова економіка : Діджиталізація ринку фінансових послуг: нові можливості та подолання бар'єрів : матеріали II Міжнар. форуму, 28 верес.-1 жовт. 2021 р. Київ : Київський нац. ун-т ім. Тараса Шевченка, 2021. – С. 22-24.

10. Дубина М. В. Роль кіберстрахування в системі ризик-менеджменту банківських установ / М.В. Дубина, І.О. Середюк, Н.В. Білоус // Проблеми і перспективи економіки та управління. – 2020. – № 1(21). – С. 183–196.

11. Заволока Л.О. Інновації на ринку страхових послуг/ Л.О.Заволока, Є.О. Колєснік, І.С. Сіліна // Інфраструктура ринку. – 2018. – №19. – С. 195-200.

12. Ільчук В. П. Інноваційні підходи до розвитку ринку кіберстрахування в Україні [Електронний ресурс]/ В.П. Ільчук, О.М. Парубець, Д.О. Сугоняко // Ефективна економіка. – 2018. – № 5. – Режим доступу: http://www.economy.nayka.com.ua/pdf/5_2018/5.pdf

13. Ковбатюк М. В. Цифрова економіка в Україні: стан, проблеми та можливості розвитку / М.В. Ковбатюк, В.О. Шевчук // Збірник наукових праць ДУІТ. Економіка і управління. – 2021. – № 49. – С. 69–77.

14. Косар Н.С. Цифрові технології у просуванні страхових продуктів на ринку / Н.С. Косар, Н.Є. Кузьо, В.Є. Крикавський // Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку. – 2024. – №2 (12). – С. 176-185

15. Мельник В. Функціонування страхового ринку України: нові виклики та загрози / В. Мельник, В. Волкова // Галицький економічний вісник. – 2023. – № 5 (84). – С. 71-80.

16. Нагайчук Н.Г. Страхування в системі управління кібер-ризиками підприємства в умовах цифрової економіки / Н.Г. Нагайчук, Н.М. Третяк, О.О. Ткаленко // Фінансовий простір. – 2019. – № 1 (33). – С. 97-111.

17. Нямещук Г. Страхування кіберризиків як складовий елемент системи ефективного менеджменту: кейс України / Г. Нямещук, В. Біла // Challenges and Issues of Modern Science. – 2024. – № 2. – С. 280-284

18. Обушний С. М. Фінансові технології в Україні: шлях до інновацій та стабільності / С.М. Обушний, К.В. Арабаджи, К.О. Костікова // European scientific journal of Economic and Financial innovation. – 2023. – № 1 (11). – С. 59–72.

19. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації [Електронний ресурс]. – Режим доступу : https://www.cip.gov.ua/ua

20. Офіційний сайт Національного банку України [Електронний ресурс]. – Режим доступу : https://bank.gov.ua

21. Офіційний сайт ПрАТ «Українська пожежно-страхова компанія» [Електронний ресурс]. – Режим доступу: https://upsk.com.ua/

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

23. Попович Д.В. Проблеми та перспективи розвитку страхування кіберризиків на національному ринку / Д.В. Попович, Н.Б. Бундз, В.О. Іванків // Молодий вченний. – 2023. – №4 (116). – С. 168-172

24. Приказюк Н. В. Дорожня карта впровадження кібер-страхування в Україні / Н.В. Приказюк, Л.С. Гуменюк // Innovation and sustainability. – 2021. – № 1. – С. 64–72.

25. Приказюк Н. В. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки [Електронний ресурс]/ Н.В. Приказюк, Л.С. Гуменюк / Ефективна економіка. – 2020. – № 4. – Режим доступу: http://www.economy.nayka.com.ua/?

26. Приказюк Н. В. Передумови розвитку кібер-страхування / Н.В. Приказюк, Л.С. Гуменюк // Інвестиції: практика та досвід. – 2020.– № 15-16. – С. 28–34.

27. Приказюк Н. В. Прогресивний досвід зарубіжних країн у вирішенні проблем розвитку кіберстрахування/ Н. В. Приказюк, М. В. Кукурузняк//

Вісник Одеського національного університету. Серія: Економіка. – 2016. – Т. 21. – № 2. – С. 164-168

28. Про основні засади забезпечення кібербезпеки України: Закон України від 21.06.2018 за № 2469-VIII [Електронний ресурс]/ Верховна Рада України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

29. Пшенична М. Технології штучного інтелекту в страховій індустрії України: аналіз тенденцій та перспективи розвитку / М. Пшенична // Цифрова економіка та економічна безпека – 2023. – №6 (06). – С. 92-96.

30. Ролінський О.В. Візуалізація даних та фінансова безпека на страховому ринку України / О.В. Ролінський, Ю.В. Уланич // Агросвіт. – 2021. № 16. – С. 45–51.

31. Ротова Т. Страхування як фінансовий інструмент захисту від кіберризиків / Т. Ротова, Ю. Шевченко // Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукр. наук. практ. конф. Київ: КНТЕУ, 2019. – С. 177–178.

32. Селіверстова Л. С. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку / Л. С. Селіверстова, Д. А. Трухан // Економіка та держава. – 2020. – № 1. – С. 23-26.

33. Скрипник Г. Діяльність страхових компаній України в умовах воєнного стану / Г. Скрипник, В. Якименко // Цифрова економіка та економічна безпека. – 2024. – № 2 (11). – С. 151-156.

34. Федорович І.М. Основні тренди та напрями розвитку страхового ринку України / І.М. Федорович // Інвестиції: практика та досвід. – 2023. – № 3. – С. 45-49.

35. Фонталін Д. В. Значення страхового ринку для фінансової системи України / Д. В. Фонталін // Економіка. Фінанси. Право. – 2024. – № 8. – С. 25-28.

36. Чвертко Л. А. Цифровізація страхового бізнесу як дієвий важіль управління ризиками / Л. А. Чвертко, Т. О. Корнієнко, О. А. Вінницька // Sciences of Europe. – 2022. – Вип. 89. – С. 7-11.

37. Череп А. В. Перспективи розвитку страхового ринку України в умовах євроінтеграційних процесів / А. В. Череп, Ю. П. Кішко // Держава та регіони. – 2024. – № 2. – С. 78-83.

38. Черняк Я. Детермінанти розвитку інновацій у страховому бізнесі / Я. Черняк, Л. Клапків // Інноваційна економіка – 2018. – № 1-2. – С. 182-188.

39. Шолойко А. С. Актуалізація кіберстрахування в умовах цифровізації економіки / А.С. Шолойко// Науковий вісник Одеського національного економічного університету. – 2023. – № 9 (310). – С. 98–106.

40. Шолойко А. С. Компаративізм продуктів зі страхування кіберризиків / А.С. Шолойко // Науковий вісник Одеського національного економічного університету. – 2023. – № 11-12 (312-313). – С.149-158.

Додатки