КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЕКОНОМІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА СТРАХУВАННЯ, БАНКІВСЬКОЇ СПРАВИ ТА РИЗИК-МЕНЕДЖМЕНТУ

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

РОЗВИТОК СТРАХУВАННЯ КІБЕРРИЗИКІВ В УКРАЇНІ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

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

Науковий керівник:
к.е.н., доцент
Прокоф'єва Олена Володимирівна

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

Робота допущена до захисту в Екзаменаційній комісії рішенням кафедри страхування, банківської справи та ризик-менеджменту від «14» травня 2024 р., протокол № 14

В.о. завідувача кафедри страхування,
банківської справи та ризик-менеджменту,
доктор економічних наук, доцент
Шолойко Антоніна Сергіївна _____
(підпис)

Київ - 2024

АНОТАЦІЯ

Беспалова Ю.Ю. Розвиток страхування кіберризиків в Україні в умовах сучасних викликів.

Кваліфікаційна магістерська робота за спеціальністю 072 «Фінанси, банківська справа та страхування». Кафедра страхування, банківської справи та ризик-менеджменту, економічний факультет. Київський національний університет імені Тараса Шевченка, Київ, 2024.

Кваліфікаційна магістерська робота складається з трьох розділів.

Об'єктом дослідження є економічні відносини, що виникають між суб'єктами страхування кіберризиків.

Предметом дослідження є теоретичні основи, сучасні тенденції та перспективи розвитку страхування кіберризиків в Україні.

Мета магістерської роботи полягає в узагальненні теоретичних основ та формулюванні пропозицій щодо перспектив розвитку страхування кіберризиків в Україні задля підвищення стійкості бізнесу до кіберзагроз.

У роботі розглянуто теоретичні засади здійснення страхування кіберризиків: розкрито та доповнено економічну сутність поняття «кіберризик» та узагальнено класифікацію його видів, визначено об'єктивну необхідність та переваги страхування кіберризиків, охарактеризовано етапи його розвитку. Охарактеризовано сучасний стан страхування кіберризиків, зокрема: визначено особливості інституційно-правового забезпечення страхування кіберризиків, з'ясовано, що кіберризики здійснюють значний вплив на діяльність суб'єктів господарювання та окреслено основні тенденції страхування кіберризиків в Україні та світі, зокрема побудовано прогноз обсягу глобальних премій зі страхування кіберризиків на наступні вісім років. Запропоновано практичні рекомендації щодо удосконалення інституційно-правового забезпечення страхування кіберризиків та розроблено систему заходів спрямованих на підвищення рівня охоплення страхуванням кіберризиків суб'єктів господарювання.

Ключові слова: кіберризик, кібербезпека, кіберінцидент, страхування кіберризиків, кіберзагроза.

Список публікацій магістра:

1. Беспалова Ю.Ю. Кібер-страхування як інструмент управління ризиками в умовах цифрової трансформації. Шевченківська весна 2024. Стратегії економічного зростання: погляд у майбутнє для України, матеріали Міжнародної науковопрактичної конференції студентів, аспірантів та молодих вчених / За заг. ред. Л.А. Анісімової: - К., Інтерсервіс, 2024. – Вип. XXII. С.173-174.
2. Прокоф'єва О.В., Беспалова Ю.Ю. Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації. Інвестиції: практика та досвід. 2024. №10.

ABSTRACT

Bespalova Y.Y. Development of cyber risk insurance in Ukraine in the context of modern challenges.

Qualifying master's thesis in the specialty 072 «Finance, banking and insurance». Department of Insurance, Banking and Risk Management, Faculty of Economics. Taras Shevchenko National University of Kyiv, Kyiv, 2024.

The master's qualification work consists of three sections.

The object of the study is the economic relations that arise between the subjects of cyber risk insurance.

The subject of the study is the theoretical foundations, current trends and prospects for the development of cyber insurance in Ukraine.

The purpose of the master's work is to summarize the theoretical foundations and formulate proposals for the prospects for the development of cyber risk insurance in Ukraine in order to increase business resilience to cyber threats.

The work examines thetheoretical foundations of cyber risk insurance: the economic essence of the concept of “cyber risk” is revealed and supplemented, the classification of its types is generalized, the objective necessity and benefits of cyber risk insurance are determined, and the stages of its development are characterized. The current state of cyber risk insurance is characterized, in particular: the peculiarities of institutional legal support for cyber risk insurance are determined, it is found that cyber risks have a significant impact on the activities of business entities and the main trends in cyber risk insurance in Ukraine and the world are outlined, in particular, a forecast of the volume of global cyber risk insurance premiums for the next eight years is made. Practical recommendations for improving the institutional and legal support for cyber risk insurance are proposed and a system of measures aimed at increasing the level of coverage of cyber risk insurance of business entities is developed.

Key words: cyber risk, cybersecurity, cyber incident, cyber risk insurance, cyber threat.

List of Master's publications:

1. Bespalova Y.Y. Cyber insurance as a risk management tool in the context of digital transformation. Shevchenko's spring 2024. Strategies of economic growth: a look into the future for Ukraine, materials of the International Scientific and Practical Conference of Students, Postgraduates and Young Scientists / Edited by L.A. Anisimova: - K., Interservice, 2024 – № 12. P.173-174.
2. Prokofieva O.V., Bespalova Y.Y. Cyber risks and their management in the context of globalization and digital transformation. Investytsii: praktyka ta dosvid. 2024. №10.

ЗМІСТ

ВСТУП

Актуальність дослідження. В умовах швидких змін у світовій економіці, що зумовлені новітніми цифровими технологіями, розвиток страхування кіберризиків набуває першочергового значення. Цифровізація бізнесу, поява великих даних, штучного інтелекту, технології блокчейн та хмарних обчислень призвели до глибоких змін у принципах конкурентних відносин. Однак цифровізація економіки також призвела до появи нових ризиків, пов'язаних з використанням технологій, які потенційно можуть негативно вплинути на економічні суб'єкти та результати їхньої діяльності.

Останніми роками кіберризики привертають все більше уваги і сьогодні розглядаються як одна з головних глобальних загроз для фінансового сектору та економіки в цілому. Це зумовлює необхідність впровадження та застосування інноваційних інструментів управління ризиками в тому числі інструментів страхування, які б відповідали вимогам цифрової економіки. Тому, питання, пов'язані з інтенсифікацією та розширенням таких сучасних страхових інструментів і методів, а також їх адаптацією до інноваційних змін в економічному ландшафті, набувають сьогодні особливої актуальності.

У контексті триваючої цифрової трансформації кіберризики набули нового рівня значущості для України, особливо з огляду на вразливість країни до кібератак під час війни. Як державні, так і комерційні структури в Україні стикаються з постійними кіберзагрозами, що можуть призвести до значних фінансових втрат, які часто є непомірними для суб’єктів господарювання. Страхування кіберризиків стає єдиним ринковим інструментом, який може забезпечити фінансову стабільність цих суб'єктів та захистити їхню репутацію. Ця форма страхування не лише сприяє

відшкодуванню понесених збитків, але й дозволяє створити надійну превентивну систему цифрової безпеки.

Розвиток надійного ринку страхування кіберризиків може відігравати ключову роль у підтримці переходу України до цифрової економіки шляхом підвищення обізнаності про кіберризики та заохочення проактивного управління ними. Тому це підвищує стійкість бізнесу та державних установ до кіберзагроз, що в кінцевому підсумку сприяє економічній стабільності та безпеці країни.

Теоретико-методичні основи управління кіберризиками в тому числі особливості розвитку їх страхування знайшли своє відображення в роботах як вітчизняних так і зарубіжних економістів серед яких: Братюк В. П., Віннікова І. І., Волосович С., Гудзь. О., Гуменюк Л. С., Клапків Л., Марчук С. В., Пікус Р. В., Приказюк Н. В., Селіверстова Л. С., Шолойко А. С. Серед зарубіжних учених-економістів розвиток страхування кіберризиків досліджували такі вчені, як Беме Р., Шварц Г., Франке У. (Bohme R., Schwartz G., Franke U.).

Однак комплексний ландшафт розвитку кіберстрахування залишається недостатньо висвітленим. Існує нагальна потреба у визначені сучасних тенденцій розвитку страхування кіберризиків в Україні та світі, вдосконаленні інституційно правового забезпечення та визначенні ефективних шляхів впровадження продуктів страхування кіберризиків на страховому ринку України.

Мета дослідження: Узагальнити теоретичні основи, сформулювати пропозиції щодо напрямів розвитку страхування кіберризиків в Україні з метою підвищення стійкості бізнесу до кіберзагроз.

Досягнення поставленої мети зумовило необхідність розв’язання таких завдань:

– Визначити зміст поняття «кіберризик» та узагальнити класифікацію його видів;

– Охарактеризувати об’єктивну необхідність страхування кіберризиків;

– Визначити етапи розвитку страхування кіберризиків;

– Охарактеризувати інституційно-правове забезпечення страхування кіберризиків;

– Визначити вплив кіберризиків на діяльність суб'єктів господарювання;

– Визначити основні тенденції розвитку страхування кіберризиків в Україні та світі;

– Побудувати прогноз обсягу глобальноих премій зі страхування кіберризиків;

– Визначити напрями удосконалення інституційно-правового забезпечення страхування кіберризиків;

– Запропонувати рекомендації щодо підвищення рівня охоплення страхуванням кіберризиків суб'єктів господарювання.

Об'єкт дослідження. Економічні відносини, що виникають між суб'єктами страхування кіберризиків.

Предмет дослідження. Теоретичні основи, сучасні тенденції та перспективи розвитку страхування кіберризиків в Україні.

Методи дослідження. Розв'язання поставлених завдань зумовило використання наступних методів: в основі роботи лежить діалектичний метод; метод критичного аналізу літературних джерел, метод наукової абстракції та метод систематизації та класифікації – для визначення змісту поняття «кіберризик» та характеристики його видів; метод критичного аналізу літературних джерел та метод узагальнення – для характеристики об'єктивної необхідності страхування кіберризиків; історичний та логічний метод – для визначення етапів розвитку страхування кіберризиків; метод критичного аналізу літературних джерел – для характеристики інституційно-правового забезпечення страхування кіберризиків; статистичний метод, метод аналізу та синтезу – для характеристики впливу кіберризиків на діяльність суб'єктів господарювання; статистичний метод, методи

спостереження та узагальнення – при визначенні основних тенденцій розвитку страхування кіберризиків в Україні та світі; метод абстрагування та конкретизації – для побудови прогнозу обсягу премій зі страхування кіберризиків у світі; метод логічного узагальнення – для визначення напрямів удосконалення інституційно-правового забезпечення страхування кіберризиків в Україні; метод логічного узагальнення – для формування рекомендацій щодо підвищення рівня охоплення страхуванням кіберризиків суб'єктів господарювання; візуальний та графічний методи – для аналізу, узагальнення та представлення даних у найбільш інформативний спосіб (таблиці, рисунки).

Інформаційною базою дослідження стали законодавчі та нормативні документи у сфері регулювання діяльності страхових компаній, захисту даних та кібербезпеки України, наукові праці вітчизняних та іноземний вчених з проблематики страхування кіберризиків та статистична інформація, представлена у звітах профільних організацій.

Практичне значення одержаних результатів. Рекомендації та пропозиції щодо розвитку страхування кіберризиків в Україні можуть бути застосовані окремими страховими компаніями та регуляторними органами з метою поліпшення нормативно-правового забезпечення та підвищення рівня охоплення страхуванням кіберризиків суб'єктів господарювання.

Апробація результатів дослідження. Основні аспекти дослідження було апробовано на XXII Міжнародній науково-практична конференції «Шевченківська весна 2024. Стратегії економічного зростання: погляд у майбутнє для України» (19-21 березня 2024 року, Київ). Опубліковано наукову статтю на тему «Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації» у журналі «Інвестиції: практика та досвід» у Випуску №10 (2024).

Обсяг та структура роботи. Кваліфікаційна магістерська робота подана на 74 сторінках, та складається зі вступу, трьох розділів та висновків. Робота включає 10 таблиць та 11 рисунків. Список використаних джерел налічує 72 джерела.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ЗДІЙСНЕННЯ СТРАХУВАННЯ КІБЕРРИЗИКІВ

1.1. Сутність кіберризиків та їх види

Сьогодні кіберризики привертають все більше уваги через широке використання технологій та діджиталізацію різних аспектів сучасного життя. Науковці та експерти з різних галузей зробили свій внесок у розуміння поняття кіберризиків. Однак, незважаючи на зростаючу кількість літератури на цю тему, не існує загальноприйнятого визначення кіберризику. Відсутність консенсусу зумовлена складною та динамічною природою кіберризиків, а також різноманітними поглядами та методологіями, які застосовують дослідники.

Науковці підходять до визначення кіберризику з різних боків, наголошуючи на різних аспектах і вимірах, у табл. 1.1, що наведена нижче, представлено підходи вчених до визначення даної категорії.

Таблиця 1.1

Структура категорії «кіберризик» в підходах різних авторів

№	Автор	Суть явища	Зміст явища	Результат явища
1	2	3	4	5
1	Братюк В.П.	Ризик	пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення як в місцевих (локальних) мережах, так і в глобальній інтернет-мережі; в розрахунково-платіжних системах, у системах інтернет-торгівлі і в промислових системах управління.	–

Продовження табл. 1.1

1	2	3	4	5
2	Пікус Р.В. Бабенко Ю.Л.	Ймовірність настання подій	які вражають роботу ІТ-систем та кібербезпеку організації через стороннє втручання цифрових та інших електронних технологій	що призводить до отримання збитків, руйнування цифрових активів та можливої втрати репутації організації.
3	Беме Р. Шварц Г.	Можливі зломи, перебої та інші порушення у роботі комп'ютерних та інформаційних систем та мереж	–	при настанні яких можуть виникнути негативні наслідки.
4	Волосович С.	Операційний ризик	який полягає в	отриманні прямих чи побічних збитків економічними суб'єктами внаслідок їх функціонування у кіберпросторі.
5	Івашина Н. В.	будь-який ризик	у результаті виходу з ладу ІТ систем, систем інформаційної безпеки.	що призводить до фінансових втрат, знищення або погіршення репутації
6	Chief Risk Officer Forum (групи професійних менеджерів з ризиків страхової галузі)	Будь-які ризики	пов'язані з використанням електронних даних та їх передачею, включаючи технологічні інструменти, такі як Інтернет і телекомунікаційні мережі;	–
		Фізичні збитки	які можуть бути спричинені кібератаками;	–
		Шахрайство	вчинене шляхом неправомірного використання даних;	–
		Будь-яка відповідальність	що випливає з використання, зберігання і передачі даних;	–
		Доступність, цілісність і конфіденційність електронної інформації	незалежно від того, чи стосується вона фізичних осіб, компаній або урядів.	–

Джерело: складено автором на основі [3,6,11,20,47,48]

Зважаючи на відсутність стандартизованого визначення, важливо прийняти комплексний підхід, який би інтегрував ідеї різних вчених. Аналіз вище наведених підходів до визначення поняття «кіберризику» дозволяє нам сформулювати власне тлумачення цього поняття: кіберризик - це ймовірність настання несприятливих подій, пов'язаних з використанням комп'ютерного обладнання та програмного забезпечення, що призводять до збоїв в роботі IT-систем, витоку даних, фінансових втрат та репутаційної шкоди організації. Такий цілісний погляд має вирішальне значення для розробки ефективних стратегій пом'якшення кіберзагроз і розробки відповідних рішень для управління кіберризиками.

У сучасному цифровому ландшафті існує широкий спектр кіберризиків, кожен з яких представляє унікальні виклики та потенційні наслідки для окремих осіб, організацій та суспільства в цілому. У таблиці 1.2 наведено класифікацію найпоширеніших кіберризиків, з якими можуть зіткнутися організації, що охоплюють різні типи загроз і вектори атак.

Таблиця 1.2

Узагальнена класифікація «кіберризиків»

Категорія ризику	Опис
1	2
Шкідливе програмне забезпечення	Несанкціонований доступ, розголошення або крадіжка чутливої або конфіденційної інформації, включаючи персональні дані, фінансову документацію або інтелектуальну власність.
Програми-вимагачі	Шкідливе програмне забезпечення, яке шифрує файли або системи, роблячи їх недоступними доти, доки зловмисник не отримає викуп за розшифрування.
Переривання діяльності	Порушення бізнес-операцій, послуг або критично важливих систем через кіберінциденти, що призводить до фінансових втрат, включаючи простої, недоотриманий дохід і додаткові витрати на відновлення діяльності.
Мережева безпека	Ризик, пов'язаний з безпекою комп'ютерних мереж, зокрема несанкціонований доступ, витік даних, зараження шкідливим програмним забезпеченням та атаки на відмову в обслуговуванні.
Відповідальність за конфіденційність	Юридична відповідальність, що виникає внаслідок порушення законів, правил або договірних зобов'язань, пов'язаних з обробкою, зберіганням або передачею особистої чи конфіденційної інформації.

Продовження табл. 1.2

1	2
Кібервимагання	Погрози або вимоги грошей, послуг чи інших вигод в обмін на нерозголошення конфіденційної або шкідливої інформації чи зупинення кібератаки, наприклад, DDoS-атаки або знищення даних.
Шахрайський переказ	Несанкціонований або шахрайський переказ коштів, активів або цінних паперів внаслідок кібератак, шахрайства з використанням соціальної інженерії або компрометації фінансових систем чи процесів.
Відповідальність перед третіми особами	Відповідальність, що виникає внаслідок кіберінцидентів, які впливають на третіх осіб, зокрема клієнтів, постачальників, партнерів або інших зацікавлених сторін, таких як витік даних, збої в роботі мережі або збої в системі безпеки, що впливають на зовнішні суб'єкти.
Штрафи регуляторних органів	Штрафи або санкції, накладені регуляторними органами за недотримання норм, законів або стандартів щодо захисту даних, конфіденційності або кібербезпеки.
Реагування на інциденти	Витрати, пов'язані з управлінням та реагуванням на кіберінциденти, включаючи судові розслідування, судові витрати, витрати на повідомлення, кредитний моніторинг, зв'язки з громадськістю та кризове управління.

Джерело: складено автором на основі [5,22,35,36,54]

Існує широкий спектр подій, які можуть призвести до виникнення кіберризиків. До них належать:

1. Зловмисні дії:

– Кібератаки – навмисні дії зловмисників, спрямовані на завдання шкоди інформаційним системам, даним або користувачам;

– Внутрішні загрози – можуть виникати з боку співробітників, які ненавмисно або навмисно розголошують конфіденційну інформацію, шкодять комп'ютерним системам або вчиняють шахрайські дії.

2. Збої в роботі:

– Програмні помилки – помилки в програмному забезпеченні, які можуть призвести до збоїв у роботі IT-систем або втрати даних;

– Збої в роботі апаратних компонентів, які можуть призвести до втрати даних або перебоїв у роботі;

– Перебої в електропостачанні, які можуть призвести до вимкнення комп'ютерних систем та пошкодження даних;

– Стихійні лиха, такі як повені, урагани та землетруси, що можуть призвести до механічного пошкодження ІТ-систем, втрати даних або інших проблем.

3. Людська помилка:

– Ненавмисне розголошення конфіденційної інформації співробітниками, наприклад, надіславши її на неправильну адресу електронної пошти або залишивши її без нагляду;

– Використання ненадійних паролів – слабкі або повторно використовувані паролі, що можуть полегшити зловмисникам доступ до інформаційних систем;

– Відкриття шкідливих файлів – співробітники можуть ненавмисно відкрити такі файли, що може призвести до зараження комп'ютерних систем шкідливими програмами;

– неналежне поводження з носіями даних – співробітники можуть ненавмисно загубити або пошкодити носії даних, що може призвести до їх втрати.

Одними з найпоширеніших кіберризиків на сьогодні є кібератаки, які постійно вдосконалюються у сучасному цифровому середовищі. Ці атаки охоплюють широкий спектр шкідливих дій, спрямованих на використання вразливостей у комп’ютерних системах, мережах і цифрових активах. Кібератаки можуть приймати різні форми, кожна з яких має свій набір тактик, методів і цілей. На рисунку 1.1. зображено найпоширеніші види кібератак з якими можуть зіштовхнутись приватні та державні установи.

Рис. 1.1. Найпоширеніші види кібератак

Джерело: складено автором на основі [45,52]

Загалом кібератаки можна розділити на дві категорії: цільові та нецільові.

1. Цільові атаки – це навмисні та цілеспрямовані зусилля, для проникнення в певні організації або системи зі зловмисною метою. Такі атаки передбачають ретельну розвідку та планування для виявлення вразливостей і використання їх для досягнення конкретних цілей. Цілеспрямовані атаки можуть включати фінансове шахрайство, крадіжку даних, промислове шпигунство або саботаж. Зловмисники часто використовують складні тактики, щоб обійти систему захисту та уникнути виявлення. Цілеспрямовані атаки становлять значні ризики для

організацій, оскільки вони можуть призвести до значних фінансових втрат, репутаційних збитків або витоку конфіденційної інформації.

2. Нецільові атаки – це атаки широкого спектру на цифрові системи та мережі, які не спрямовані на конкретну організацію. Ці атаки охоплюють велику кількість користувачів, орієнтуючись на слабкі місця, які є спільними для багатьох організацій або окремих осіб. Нецільові атаки можуть включати широкомасштабні кампанії шкідливого програмного забезпечення, фішингові афери або автоматизовану експлуатацію відомих слабких місць програмного забезпечення організацій. Хоча нецільові атаки не спрямовані на конкретну жертву, вони все одно можуть завдати значної шкоди, такої як: витоки даних, фінансові втрати або порушення роботи сервісів. Через свою невибіркову природу нецільові атаки часто покладаються на використання типових людських помилок або слабких місць у конфігураціях програмного забезпечення.

Отже у сучасному цифровому ландшафті кіберризики становлять серйозну загрозу для організацій, осіб та суспільства в цілому. Залежно від мотивів та цілей зловмисників, кіберризики можна поділити на дві категорії: цільові та нецільові. Існує також безліч типів кіберзагроз, таких як шкідливе програмне забезпечення, програми-вимагачі, переривання діяльності, мережева безпека, відповідальність за конфіденційність, кібервимагання, шахрайські перекази, відповідальність перед третіми особами, штрафи регуляторних органів та реагування на інциденти. Розуміння сутності, видів та наслідків кіберризиків є ключовим фактором для розробки ефективних стратегій захисту та управління ризиками.

1.2. Об’єктивна необхідність страхування кіберризиків

В останні роки людство відзначилось значним зростанням впровадження та інтеграції цифрових технологій у різні аспекти повсякденного життя, включаючи торгівлю, охорону здоров'я, освіту та державне управління. Хоча цей технологічний прогрес приносить численні переваги та можливості, він також створює нові виклики та ризики, особливо у сфері кібербезпеки. Організації та окремі особи все більше покладаються на цифрові технології для ведення бізнесу, спілкування та зберігання конфіденційної інформації, що робить їх більш вразливими до потенційних кіберзагроз.

Злочинні кібератаки, такі як зараження зловмисним програмним забезпеченням, фішингове шахрайство, атаки програм-вимагачів і DDoS-атаки, стають все більш поширеними та складними. Кіберзлочинці використовують передові методи та вразливі місця в програмному забезпеченні, мережах і поведінці людей. Ці атаки можуть мати серйозні наслідки для організацій, зокрема фінансові втрати, репутаційні збитки, регулятивні штрафи та юридичну відповідальність.

Крім того, технічні збої, такі як помилки програмного забезпечення, збої в роботі апаратного забезпечення або системні збої, також можуть становити значні ризики для цифрової безпеки. Вони можуть бути результатом недоліків у програмному забезпеченні, помилок кодування, неадекватного тестування або непередбачених взаємодій між різними компонентами IT-системи. Технічні порушення можуть призвести до перебоїв в обслуговуванні, втрати даних, збоїв у роботі та фінансових збитків для організацій.

Внутрішні загрози в організаціях, зокрема загрози з боку співробітників, їх недбалість або зламані облікові записи ще більше посилюють кіберризики. Працівники організацій можуть зловживати своїми правами доступу, щоб викрасти конфіденційну інформацію, саботувати системи або сприяти кібератакам. Недбалі співробітники можуть ненавмисно розкрити конфіденційні дані через необережні дії, такі як перехід за зловмисними посиланнями, надання паролів або неправильне

поводження з конфіденційною інформацією. Зламані облікові записи, створені в результаті фішингових шахрайств, викрадення облікових даних або слабких методів автентифікації, можуть використовуватися кіберзлочинцями для отримання несанкціонованого доступу до корпоративних мереж і ресурсів.

Зростаюча складність і взаємопов'язаність цифрових технологій підкреслюють необхідність розробки ефективних інструментів і стратегій захисту від кіберризиків. Незважаючи на розвиток протоколів цифрової безпеки, мінливий характер кіберризиків і розвиток кіберзлочинності роблять традиційні заходи безпеки недостатніми і часто неефективними.

Страхування кіберризиків стає ефективним інструментом мінімізації ризиків господарської діяльності під час кіберінциденту, а також відшкодування фінансових витрат на окремі елементи боротьби з ними [38].

На сьогодні існує проблема у відсутності єдиного обґрунтованого поняття страхування кіберризиків (кіберстрахування, cyber insurance), основні підходи до трактування визначення даного поняття наведено в таблиці 1.3.

Таблиця 1.3

Структура категорії «страхування кіберризиків» в підходах різних авторів

№	Автор	Суть явища	Зміст явища	Результат явища
1	2	3	4	5
1	Приказюк Н.В. Гуменюк Л.С.	комплексний продукт	який включає в себе страхування майна, відповідальності та фінансових ризиків.	–
2	Іванова Т.Г.	страховий продукт	для захисту бізнесу та фізичних осіб від ризиків, пов'язаних із користуванням інтернетом, зберіганням та обробкою даних в електронному вигляді, роботою з IT-інфраструктурами.	–

Продовження табл. 1.3

1	2	3	4	5
3	Попович Д.	вид страхування	який надає захист	від ризиків, пов'язаних з кібербезпекою.
4	Беме Р. Шварц Г.	передача фінансового ризику	пов’язаного з мережевими та комп’ютерними інцидентами, третій стороні.	–
5	Гудзь О.	страховий продукт	який захищає економічні суб’єкти від ризиків, що відносяться до інформаційно-комунікаційних ехнологій, використання Інтернет-мережі, ІКТ-інфраструктури та діяльності у кіберпросторі.	
6	Пікус Р.В. Бабенко Ю.Л.	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, забезпечи ти захист від збитків, що виникають внаслідок порушення безпеки та конфіденційності.
7	Шолойко А.С.	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.

Джерело: складено автором на основі [9,10,20,21,22,47]

На основі аналізу вищезазначених підходів до визначення суті поняття «страхування кіберризиків» можемо сконструювати власне визначення даної

категорії: страхування кіберризиків – це інструмент передачі страховику фінансового ризику, що виникає в результаті використання цифрових технологій та проведення операцій через Інтернет, з метою захисту підприємств, фізичних осіб і державних структур від збитків спричинених кіберзагрозами та пом’якшення наслідків настання кіберінцидентів.

Поліс страхування кіберризиків надає страхувальнику важливу фінансову безпеку, гарантуючи компенсацію збитків, понесених в результаті кіберінцидентів. Ці збитки можуть включати широкий спектр фінансових наслідків, спричинених кіберризиками. У таблиці 1.4 представлено збитки, які можуть покриватись полісами страхування кіберризиків.

Таблиця 1.4

Витрати, що покривають поліси страхування кіберризиків

Вид витрат	Опис
1	2
Прямий збиток	– Перерва діяльності: витрати, пов'язані з простоєм бізнесу внаслідок кіберінциденту. Це може включати втрату доходу, витрати на зарплату співробітників, які не можуть працювати, та інші витрати, пов'язані з простоєм. – Витрати на відновлення даних: витрати, пов'язані з відновленням даних, які були втрачені або пошкоджені внаслідок кіберінциденту. Це може включати вартість програмного забезпечення для відновлення даних, роботу фахівців з відновлення даних та інші витрати, пов'язані з відновленням даних. – Втрати доходу в результаті виходу з ладу IT-мереж або веб-сайтів: витрати, пов'язані з втратою доходу внаслідок того, що IT-мережі або веб-сайти недоступні через кіберінцидент. Це може включати втрату продажів, втрату продуктивності та інші витрати, пов'язані з недоступністю IT-систем.
Збиток завданий третім особам	– Відповідальність за збереження даних: витрати, пов'язані з відповідальністю за збереження даних третіх осіб, які були втрачені або пошкоджені внаслідок кіберінциденту. Це може включати вартість повідомлення про порушення, виплати компенсацій третім особам та інші витрати, пов'язані з відповідальністю за збереження даних. – Позовні витрати у зв'язку з відповідальністю щодо злому бази даних конфіденційної інформації: витрати, пов'язані з юридичним захистом у суді у випадку позовів, пов'язаних з кіберінцидентом. Це може включати гонорари адвокатів, судові витрати та інші витрати, пов'язані з судовими розглядами.

Продовження табл. 1.4

1	2
Додаткові витрати	– Витрати на юридичний супровід: витрати на юридичну допомогу у зв'язку з кіберінцидентом. Це може включати гонорари адвокатів, консультації з питань кібербезпеки та інші витрати, пов'язані з юридичною допомогою. – Покриття суми штрафів і стягнень у зв'язку з порушеннями конфіденційної інформації: витрати на сплату штрафів і стягнень, які можуть бути накладені на стразувальника у зв'язку з порушеннями конфіденційної інформації. Це може включати штрафи, накладені урядовими органами, та штрафи, передбачені договорами з вашими клієнтами або партнерами.
Додаткові послуги	– Послуги, пов'язані з врегулюванням наслідків інциденту: витрати на послуги, які можуть допомогти страхувальнику врегулювати наслідки кіберінциденту. Це може включати послуги з повідомлення клієнтів, судову експертизу, експертну підтримку та інші послуги, пов'язані з врегулюванням наслідків інциденту.

Джерело: складено автором на основі [4]

Страхування кіберризиків є ефективним інструментом для часткової компенсації наслідків, спричинених кіберінцидентами. Воно може допомогти знизити фінансовий ризик, пов'язаний з кіберінцидентами. Це може бути особливо важливо для малих та середніх підприємств, які не можуть дозволити собі самостійно нести витрати на відновлення після кіберінциденту.

Багато страхових компаній, які пропонують послуги страхування кіберризиків, також надають доступ до експертної допомоги у випадку настання кіберінциденту, що може включати допомогу у реагуванні на інцидент, відновленні даних та захисті IT-інфраструктури страхувальника від майбутніх атак.

Загалом страхування кіберризиків має ряд переваг, які сприяють загальній стратегії управління ризиками організацій:

1. Фінансовий захист. Страхування кіберризиків забезпечує фінансовий захист від значних витрат, пов'язаних з кіберінцидентами, включаючи витік даних, атаки з вимогою викупу, перебої в роботі, юридичну відповідальність, регуляторні штрафи та витрати на усунення наслідків. Передаючи фінансовий ризик

страховику, організації можуть пом'якшити потенційно руйнівний фінансовий вплив кіберризиків і забезпечити безперервність бізнесу в разі кіберкризи.

2. Передача ризиків. Страхування кіберризиків дозволяє організаціям передати фінансовий ризик кіберінцидентів страховій компанії, зменшуючи вразливість організації до фінансових втрат та зобов'язань. Купуючи поліс страхування кіберризиків, організації фактично переносять тягар фінансової відповідальності за кіберінциденти на страховика, який бере на себе витрати на реагування та відновлення після кіберінцидентів, включаючи, судові розслідування, юридичний захист та виплати.

3. Підтримка в управлінні ризиками. Багато полісів страхування кіберризиків пропонують доступ до ресурсів і послуг з управління ризиками, покликаних допомогти організаціям зменшити кіберризики та зміцнити їхню позицію в сфері кібербезпеки. Ці послуги можуть включати оцінку кібербезпеки, програми навчання співробітників, планування реагування на інциденти та доступ до мережі експертів і постачальників послуг з кібербезпеки. Використовуючи ці ресурси, організації можуть підвищити свою стійкість до кіберзагроз і зменшити ймовірність та вплив майбутніх кіберінцидентів.

4. Захист репутації. Страхування кіберризиків може допомогти захистити репутацію та імідж організації у випадку кіберінциденту. Забезпечуючи покриття заходів зі зв'язків з громадськістю, кризового управління та відновлення репутації, страхування кіберризиків дозволяє організаціям ефективно управляти наслідками кіберкризи та відновлювати довіру з клієнтами, партнерами та зацікавленими сторонами. Це може допомогти мінімізувати довгострокову репутаційну шкоду та зберегти довіру до організації та її ділову репутацію на ринку.

5. Відповідність нормативним вимогам. Страхування кіберризиків може допомогти організаціям відповідати нормативним вимогам, пов'язаним з кібербезпекою та захистом даних. Багато полісів страхування кіберризиків

пропонують покриття регуляторних штрафів і санкцій, накладених органами захисту даних за порушення конфіденційної інформації або недотримання правил захисту даних.

Хоча значна частина наявної літератури з інформаційної безпеки переважно наголошує на організаційних і технічних заходах, таких як апаратні та програмні рішення безпеки, важливо визнати значення економічних методів, зокрема страхування кіберризиків, у забезпеченні комплексного управління ризиками.

Страхування кіберризиків, відіграє значну роль в пом’якшенні фінансового впливу кіберризиків поряд з технічними рішеннями. Страхування служить проактивним інструментом управління кіберризиками, який доповнює технічні заходи, надаючи фінансовий захист від потенційних фінансових втрат і зобов’язань, пов’язаних з кіберінцидентами.

Метою корпоративної системи управління кіберризиками за допомогою страхування, є ефективне пом’якшення різноманітних ризиків, пов’язаних з діяльністю компанії. Передаючи певні ризики страховику через кіберстрахування, організації можуть зменшити свій ризик фінансових втрат і зобов’язань, в кінцевому підсумку приводячи свій профіль ризиків до відповідного рівня, що прийнятний для акціонерів або власників.

Отже страхування кіберризиків виступає важливим інструментом для захисту організацій та окремих осіб від кіберзагроз та пом'якшення їх фінансових наслідків. Воно може допомогти мінімізувати фінансові втрати, захистити репутацію та сприяти відповідності нормативним вимогам.

1.3. Етапи розвитку страхування кіберризиків

Розвиток страхування кіберризиків можна умовно розділити на кілька ключових етапів, кожен з яких відображає еволюцію відповіді страхової галузі на нові виклики та складнощі кібербезпеки. Ці етапи підкреслюють поступовий розвиток страхування кіберризиків від його початку до його нинішнього статусу як життєво важливого компонента комплексних стратегій управління ризиками. На рисунку 1.2 наведено основні етапи становлення страхування кіберризиків.

Рис. 1.2. Етапи становлення страхування кіберризиків

Джерело: Складено автором на основі [23]

Розвиток технологій поступово формував потребу у цифровій безпеці. У «період зародження цифрових технологій» у 1947-1969 роках перед суб'єктами господарювання ще не поставала проблема захисту даних в сучасному розумінні.

Даний період ознаменував зародження і ранній розвиток технологій, які заклали основу для цифрової революції. Такі інновації, як транзистор, мікросхема МОР (мікропроцесор на кристалі) та технологія MOS (метал-оксид-напівпровідник) ознаменували початок третьої промислової революції, що зробило можливим масове виробництво та широке впровадження цифрових обчислювальних та телекомунікаційних технологій.

Цей період характеризується розвитком перших електронних обчислювальних машин і мейнфреймів. Хоча власники організацій не стикалися з проблемою захисту інформації в сучасному розумінні, оскільки більшість конфіденційних даних були засекречені і надавалися лише зі спеціальним доступом, поява цифрових обчислювальних технологій заклала підґрунтя для майбутньої появи кіберризиків.

Організації в цей період були зосереджені насамперед на максимізації ефективності та якості виробництва шляхом впровадження інноваційних технологій. Впровадження цифрових технологій у процеси масового виробництва дозволило організаціям досягти безпрецедентних рівнів продуктивності та конкурентоспроможності, хоча і з новими викликами, пов'язаними з безпекою даних та захистом інформації.

У період з 1969 по 1989 рік було «запущено масове виробництво і широке впровадження цифрових технологій» у різних галузях і секторах. Поява персональних комп'ютерів (ПК), локальних мереж (ЛОМ) та Інтернету докорінно змінила природу бізнес-операцій та комунікацій, що призвело до зростання рівня оцифрування даних і процесів.

У цей період відбулося поширення телекомунікаційних технологій із розширенням телефонних мереж, супутникового зв’язку та волоконно-оптичних кабелів. З масовим виробництвом цифрових технологій організації та окремі особи почали досліджувати різноманітні цифрові додатки в різних галузях і секторах. Від

програмного забезпечення для підвищення продуктивності бізнесу та електронної пошти до систем автоматизованого проектування і відеоігор, цифрові технології проникли в усі аспекти життя, змінивши принципи роботи, спілкування та взаємодії.

Швидкі технологічні інновації та конкуренція серед гравців галузі призвели до постійного прогресу в обчислювальній техніці, телекомунікаціях і цифровій електроніці. Компанії інвестували значні кошти в дослідження та розробки, щоб стимулювати інновації та отримати конкурентну перевагу на зростаючому цифровому ринку.

У міру того, як бізнес став більше залежати від цифрових технологій, почали з'являтися ризики, пов'язані з кіберзагрозами, такі як витік даних. Однак концепція страхування кіберризиків ще не була матеріалізована, і бізнес покладався на традиційні методи для зменшення ризиків.

Період з 1989 по 2005 рік, відомий як «фактичне створення страхування кіберризиків як окремого страхового продукту», характеризувався значними віхами та подіями, які сформували появу та еволюцію страхування кіберризиків як окремого страхового продукту.

У 1995 році створення першого широко використовуваного веб-браузера Mosaic [61] та поява Всесвітньої павутини (WWW) [43], змінили спосіб доступу людей до інформації в Інтернеті та взаємодії з нею. Доступність і популярність Всесвітньої павутини проклали шлях для швидкого зростання електронної комерції та онлайн-бізнесу, створивши нові кіберризики.

Зростання комп’ютерних вірусів в Інтернеті роспочалось зі створенням першого комп’ютерного вірусу Melissa, який широко поширився в Інтернеті через електронну пошту. Мелісса використовувала вразливі місця в програмному забезпеченні Microsoft Word, щоб поширюватися, викликаючи масові збої та пошкодження комп’ютерних систем у всьому світі. Поява комп’ютерних вірусів в

Інтернеті підкреслила потребу в надійних заходах кібербезпеки та стратегіях управління кіберризиками [67].

У відповідь на зростання кіберризиків, з якими стикається бізнес, у 1997 році на з'їзді Міжнародного товариства управління ризиками (International Risk Insurance Management Society) в Гонолулу був запропонований один із перших полісів страхування кіберризиків – Відповідальність за безпеку в Інтернеті (ISL – Internet Security Liability). Цей інноваційний продукт, створений компанією American International Group (AIG), був розроблений для захисту продавців електронної комерції, таких як Amazon, які збирали та зберігали конфіденційні дані клієнтів у своїх внутрішніх мережах. Поліс ISL вважається одним із перших продуктів, доступних для компаній того часу, що покривали кіберризики. Він заклав основу для розвитку страхування кіберризиків як окремої категорії страхових продуктів [72].

У листопаді 2001 року Радою Європи було укладено Будапештську конвенцію про кіберзлочинність, яка стала першою глобальною угодою про кібербезпеку та двадцять два роки потому залишається найактуальнішою міжнародною угодою щодо кіберзлочинності та електронних доказів. Дана конвенція мала на меті боротьбу зі зростаючою загрозою кіберзлочинності шляхом сприяння міжнародному співробітництву та координації у боротьбі з кіберризиками, удосконалення правової бази для розслідування кіберзлочинів і судового переслідування, а також сприяння обміну інформацією та ініціативам щодо розбудови потенціалу між державами-членами. Будапештська конвенція стала значним кроком у напрямку встановлення міжнародних норм і стандартів кібербезпеки, зміцнення довіри та співпраці в кіберпросторі та посилення глобальної відповіді на кіберзагрози [42].

Наступним етапом було створення стандартів кібербезпеки. У 2005 році був створений перший міжнародний стандарт кібербезпеки ISO 27001. Він

забезпечував основу для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) в організації. Прийняття таких стандартів допомогло організаціям підвищити рівень кібербезпеки та зменшити кіберризики, тим самим зменшивши ризик потенційних фінансових втрат [60].

Загалом, період з 1989 по 2005 роки став трансформаційною епохою в розвитку страхування кіберризиків, яка відзначилась значним технологічним прогресом, появою кіберзагроз, впровадженням спеціалізованих страхових продуктів, встановленням стандартів кібербезпеки та прийняттям законодавства про кіберзлочинність.

Період з 2005 по 2015 рік, відомий як «розширення та вдосконалення інструментів кіберстрахування», характеризувався значним прогресом у продуктах і послугах кіберстрахування у відповідь на мінливий ландшафт кіберзагроз.

У даний період у сфері кібербезпеки відбулися значні потрясіння пов’язані з появою серйозних кіберризиків. Хробак Conficker, який з’явився в 2009 році, заразив понад мільярд комп’ютерів у всьому світі, демонструючи масштаб і витонченість сучасних кібератак [56]. Згодом, у 2013 році, розповсюдження програми-вимагача CryptoLocker стало ключовим моментом, продемонструвавши зростання використання криптовалюти в кіберзлочинності та руйнівний вплив атак програм-вимагачів на організації по всьому світу.

У 2014 році Національний інститут стандартів і технологій (NIST) запровадив перший глобальний стандарт кібербезпеки, відомий як NIST Cybersecurity Framework. Його структура надає організаціям повний набір інструкцій, найкращих практик і стандартів для управління кіберризиками та захисту критичної інфраструктури. NIST Cybersecurity Framework став широко поширеним ресурсом для організацій, які прагнуть покращити стан своєї кібербезпеки та узгодити свої зусилля з найкращими галузевими практиками [55].

У період з 2005 по 2015 роки відбулося значне розширення страхування кіберризиків та послуг для боротьби з кіберзагрозами, що розвиваються. Страхові компанії почали пропонувати більш комплексні поліси кіберстрахування, що охоплюють ширший спектр кіберризиків, включаючи порушення даних, атаки програм-вимагачів, перерву в бізнесі та позови про відповідальність. Поліси кіберстрахування також почали включати інноваційні функції, такі як послуги реагування на інциденти, оцінка кіберризиків і покриття кібервідповідальності за претензіями третіх сторін.

Період після 2015 року ознаменувався «значними змінами в ландшафті кіберстрахування», що характеризується впровадженням нормативно-правової бази та інноваційними ініціативами для протидії виникаючим кіберризиків.

Спалах пандемії COVID-19 у 2020 році спричинив значні зміни в ландшафті кібербезпеки, що призвело до сплеску кібератак у всьому світі. Кіберзлочинці скористалися вразливостями систем віддаленого доступу, щоб атакувати приватних осіб, підприємства та державні установи. Пандемія COVID-19 підкреслила критичну важливість кіберстійкості та необхідність надійних заходів безпеки та управління кіберризиками.

У відповідь на збільшення частоти та серйозності кібератак уряди почали досліджувати інноваційні підходи для підвищення кіберстійкості та управління кіберризиками. У 2022 році до Конвенції Ради Європи про кіберзлочинність (Будапештська конвенція), було підписано Другий додатковий протокол. Цей протокол покликаний посилити співпрацю у боротьбі з кіберзлочинністю шляхом покращення взаємодії та розкриття електронних доказів [64].

Ці події підкреслюють зростаюче визнання кібербезпеки як глобального пріоритету та необхідність скоординованих дій для пом’якшення кіберризиків і захисту від кіберзагроз у все більш взаємопов’язаному та цифровому світі.

Отже зростання цифрових технологій та залежності від них спричинили появу кіберризиків, що впливають на діяльність організацій та окремих осіб. Кібератаки, технічні збої та внутрішні загрози можуть призвести до значних фінансових втрат та руйнування репутації суб’єктів господарювання. Страхування кіберризиків стає ефективним інструментом захисту та пом’якшення їх наслідків. Поліси страхування кіберризиків можуть покривати широкий спектр витрат, пов'язаних з кіберінцидентами. Розвиток страхування кіберризиків можна умовно розділити на кілька ключових етапів, що відображають еволюцію страхової галузі у відповідь на зростання нових викликів ризиків. У подальші дослідженнях даної галузі варто зосередити увагу на вивченні та аналізі нових видів кіберризиків та їх впливу.

РОЗДІЛ 2
СУЧАСНИЙ СТАН СТРАХУВАННЯ КІБЕРРИЗИКІВ В УКРАЇНІ

2.1. Інституційно-правове забезпечення страхування кіберризиків

Останнім часом розуміючи важливість та складність забезпечення кібербезпеки, уряди багатьох країн, зокрема ЄС та США ухвалили низку нормативних актів, спрямованих на захист інформації від кіберзагроз.

Основним нормативно-правовим документом, що впливає на європейський ринок страхування кіберризиків є Загальноєвропейський регламент про захист персональних даних (англ. GDPR – General Data Protection Regulation) [15].

Це комплексний закон про захист даних і конфіденційність, який був введений в дію Європейським Союзом (ЄС) у травні 2018 року. Він спрямований на гармонізацію законів про захист даних у всіх країнах-членах ЄС, встановлюючи суворі правила щодо збору, обробки та зберігання персональних даних громадян ЄС і підвищуючи підзвітність організацій, які обробляють такі дані. GDPR має значний вплив на кібербезпеку та страхування кіберризиків, накладаючи на організації певні зобов'язання та створюючи ризики.

Основні положення Загальноєвропейського регламенту про захист персональних даних (GDPR) [13]:

– Одним із центральних положень GDPR є вимога до організацій повідомляти про певні типи порушень персональних даних до відповідного наглядового органу протягом 72 годин після того, як їм стало відомо про порушення. Крім того, організації зобов'язані повідомляти постраждалих осіб без

невиправданої затримки, якщо порушення може призвести до високого ризику для їхніх прав і свобод;

– Збільшення штрафів за недотримання вимог. GDPR запроваджує досить високі штрафи для організацій, які не дотримуються його положень. Штрафи за порушення можуть становити до 20 мільйонів євро або 4% від глобального річного доходу організації, залежно від того, яка сума більша;

– Юридична відповідальність за обробку даних. Відповідно до GDPR, організації зобов'язані впроваджувати відповідні технічні та організаційні заходи для забезпечення безпеки персональних даних, які вони обробляють. У разі витоку даних або іншого інциденту, пов'язаного з безпекою, організації можуть зіткнутися з судовими позовами від осіб, чиї дані були скомпрометовані;

Даний стандарт змусив організації переглянути свої практики кібербезпеки та вжити заходів для кращого захисту персональних даних. Це призвело до зростання попиту на страхування кіберризиків, яке є важливим інструментом їх управління для організацій, які прагнуть пом’якшити фінансові ризики, пов’язані з витоком даних, регулятивними штрафами та судовими претензіями.

GDPR відіграє значну роль у формуванні ландшафту страхування кіберризиків, встановлюючи суворі вимоги щодо захисту даних.

Ще одним важливим міжнародним стандартом, який впливає на забезпечення кібербезпеки організації та страхування кіберризиків є вимоги Ради зі стандартів безпеки в індустрії платіжних карток PCI DSS (Payment Card Industry Data Security Standard) [16]. Це загальноприйнятий стандарт інформаційної безпеки, розроблений для забезпечення безпечної обробки та передачі даних власників кредитних карток. Дотримання PCI DSS є обов'язковим для всіх організацій, які приймають платіжні картки Visa, MasterCard, American Express, Discover та JCB.

Ключові вимоги стандарту PCI DSS [16]:

– Відповідність стандарту PCI DSS є обов'язковою для організацій, які обробляють дані платіжних карток, незалежно від їх розміру або галузі. Невиконання вимог PCI DSS може призвести до серйозних санкцій, включаючи штрафи, обмеження прав на обробку карток і шкоду для репутації;

– PCI DSS забезпечує комплексну систему технічних та операційних вимог безпеки для захисту даних платіжних карток. Ці вимоги охоплюють різні аспекти інформаційної безпеки, такі як мережева безпека, контроль доступу, шифрування, управління вразливостями та реагування на інциденти. Відповідність стандарту PCI DSS допомагає організаціям зміцнити свою систему кібербезпеки та зменшити ризик витоку даних і кіберінцидентів;

– Впровадження засобів контролю PCI DSS може допомогти організаціям зменшити ризик витоку даних і кібератак, тим самим знижуючи ймовірність фінансових втрат і зобов'язань;

– Організації, які обробляють дані платіжних карток, повинні переконатися, що їхні сторонні постачальники послуг і продавці також дотримуються вимог PCI DSS. Це стосується таких організацій, як платіжні системи, хостинг-провайдери, постачальники програмного забезпечення та постачальники хмарних послуг.

Загалом PCI DSS відіграє важливу роль у забезпеченні безпеки даних платіжних карток і зниженні ризику витоку даних та кіберінцидентів для організацій. Відповідність стандарту PCI DSS має важливе значення для організацій, які обробляють дані платіжних карток, адже його дотримання може бути фактором, який враховується при страхуванні кіберризиків. Організації, які дотримуються PCI DSS, можуть сплачувати нижчі премії за страхування кіберризиків, оскільки вони вважаються менш схильними до кіберінцидентів.

Дані міжнародні стандарти PCI DSS та GDPR уможливили оцінку прямих збитків від кіберризиків, включаючи штрафи, накладені за неналежне поводження

або порушення умов зберігання персональних даних клієнтів міжнародними фінансовими установами, постачальниками послуг та транснаціональними торговельними мережами [1].

В Україні питання страхування кіберризиків наразі не врегульовано на системному рівні. Проте, існують певні правові норми, які частково стосуються цієї сфери. Одним із ключових документів є Закон України «Про страхування» від 18 листопада 2021 року № 1909-IX [32], який встановлює загальні принципи страхування в Україні, а також визначає правові засади діяльності страхових компаній та страхувальників.

Закон України «Про страхування» встановлює правові основи для страхування кіберризиків в Україні. Проте, для повноцінного розвитку цієї сфери необхідне прийняття додаткових законодавчих актів, які б чітко визначили кіберризики, встановили стандарти страхування та стимулювали розвиток страхових продуктів.

Основна інфраструктура, необхідна для розвитку страхування кіберризиків в Україні поки лише формується. Так, у травні 2018 року набув чинності Закон «Про основні засади забезпечення кібербезпеки України»[29]. Даний закон відіграє важливу роль у створенні сприятливого середовища для розвитку страхування кіберризиків в Україні. Він встановлює загальні засади забезпечення кібербезпеки в країні, визначає повноваження органів державної влади та суб'єктів здійснення господарської діяльності у цій сфері, а також закладає основи для подальшого розвитку страхування кіберризиків.

Цей закон дає визначення таких понять, як «кібербезпека» та «кіберзагроза». «Кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і

потенційних загроз національній безпеці України у кіберпросторі». «Кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів» [29]. Загалом створення даного закону є важливим кроком у розвитку страхування кіберризиків в Україні.

Даний нормативно-правовий акт передбачає співпрацю між державним і приватним секторами у сфері кібербезпеки, яка здійснюється шляхом організації регулярних національних самітів за участю професійних постачальників послуг від бізнесу, зокрема страховиків, аудиторів та юристів, задля визначення їхньої ролі у вдосконаленні практики управління кіберризиками.

Крім описаних вище законів питання кібербезпеки в Україні регулюється також наступними нормативними документами:

– Стратегія кібербезпеки України [37];

– Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» [25];

– Закон України «Про інформацію» [27];

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [26];

– Закон України «Про національну безпеку України» [28];

Також в Україні діють стратегічні та міжнародні документи, такі як:

– Стратегія національної безпеки України [30];

– Доктрина інформаційної безпеки України [31];

– Конвенція про кіберзлочинність[12].

Хоча в Україні існують численні нормативно-правові акти, що регулюють питання інформаційної безпеки, виникає проблема неузгодженості термінології. Це призводить до нечіткості трактування норм законодавства та ускладнює їх

практичне застосування. Тому для стимулювання розвитку страхування кіберризиків в Україні необхідно внести законодавчі зміни, які б чітко визначили трактування кіберризиків, встановилюва правила страхування цих ризиків та визначили перелік страхових випадків.

Отже, питання страхування кіберризиків в Україні наразі не врегульовано на системному рівні, хоча існують певні кроки у цьому напрямку. Для стимулювання розвитку цієї сфери в Україні необхідно прийняти додаткові законодавчі акти, встановити стандарти для страхування кіберризиків та уніфікувати термінологію, що стосується інформаційної безпеки. Впровадження цих заходів дозволить створити сприятливе середовище для розвитку страхування кіберризиків в Україні, що сприятиме захисту інформаційної безпеки та економічних інтересів українських підприємств та організацій.

2.2. Вплив кіберризиків на діяльність суб'єктів господарювання

Швидкий розвиток технологій призводить до зростання складності та частоти кіберзлочинів, скоєних за допомогою IT-інструментів. Ці кібератаки завдають значної шкоди не лише окремим особам та підприємствам але й цілим галузям економіки та державам. Поширення IT-інструментів і цифрових платформ розширило зону атаки для кіберзлочинців, надавши їм безліч можливостей для використання вразливостей і проникнення в системи. Від складних атак зловмисного програмного забезпечення та програм-вимагачів до складних схем соціальної інженерії, кіберзлочинці використовують широкий набір тактик для зламу мереж, викрадення конфіденційних даних і зриву операцій. Ці кіберризики не лише ставлять під загрозу цілісність і конфіденційність цифрових активів, але й

створюють значні фінансові та репутаційні ризики для компаній будь-якого розміру з різних галузей.

За даними Центру скарг на злочинів в Інтернеті (Internet Crime Complaint Center) за період з 2015 по 2023 рік було задокументовано значний приріст кіберзлочинів, спрямованих проти бізнесу в усьому світі. Протягом даного періоду було зареєстровано понад 5 мільйонів скарг, що свідчить про зростання масштабів та впливу кібератак на підприємства. Зокрема у 2023 році, їхня кількість збільшилась у 3 рази порівняно з 2015 роком (рис. 2.1), що обумовлено широким впровадження хмарних сервісів і криптовалют, а також трансформаційним впливом пандемії COVID-19.

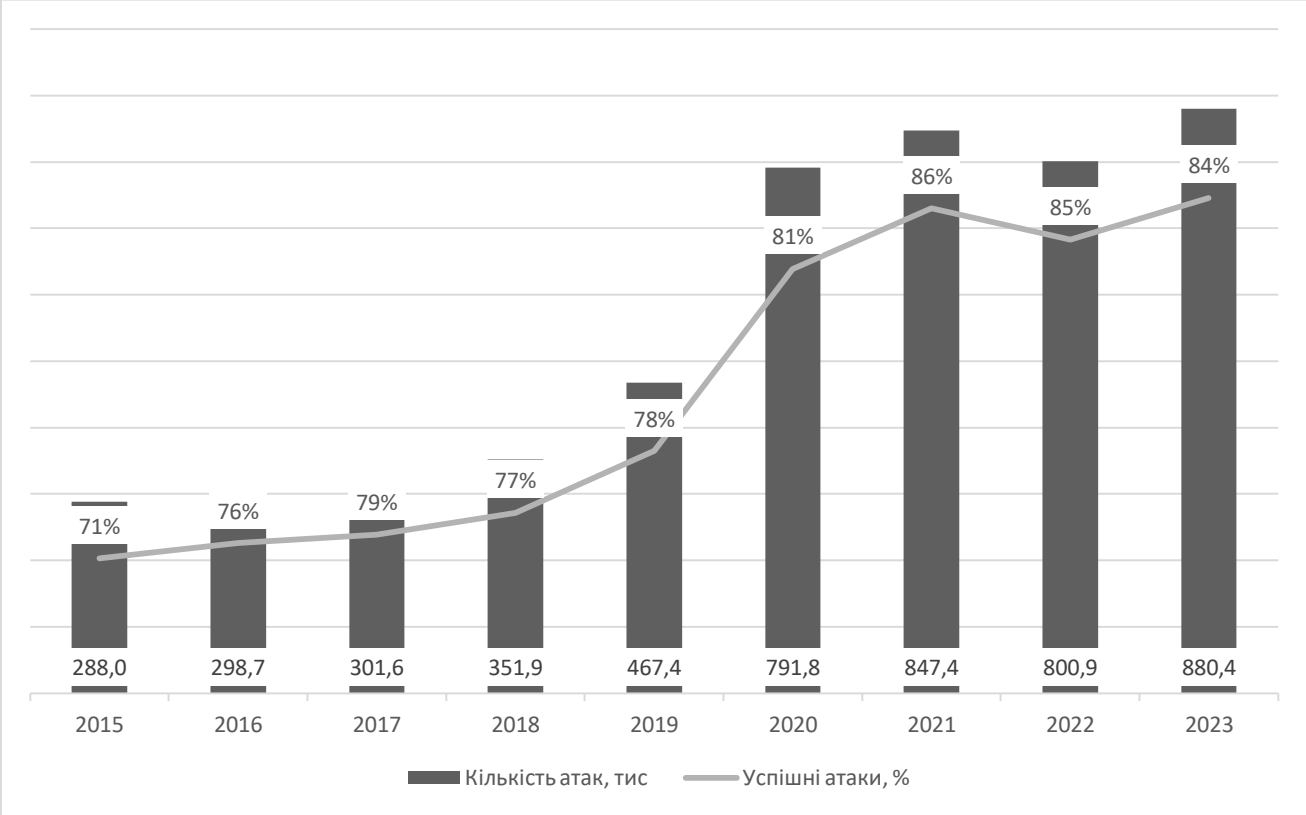

Рис. 2.1. Зареєстровані кібератаки у світі 2015-2023рр.

Джерело: складено автором на основі [41,59]

Глобальна пандемія стала каталізатором цифрової трансформації, прискоривши впровадження віддаленої роботи та цифрових платформ у різних галузях. Хоча ці зміни сприяли збільшенню гнучкості та ефективності, вони також наразили організації на підвищені ризики кібербезпеки. Швидкий перехід до віддаленої роботи в поєднанні зі зростаючою залежністю від цифрових інфраструктур створив для кіберзлочинців сприятливий ґрунт для використання слабких місць у програмному забезпеченні і здійснення цілеспрямованих атак на бізнес по всьому світу.

Ще одним важливим показником стану кібербезпеки та впливу кіберризиків на діяльність підприємств є рівень успішності кібератак, що здійснюються проти них. Протягом аналізованого періоду цей показник стабільно перевищував 70%, досягнувши піку в 86% у 2021 році, що можна пояснити поширенням віддаленої роботи, яка підвищує складність захисту даних на розподілених пристроях працівників. Нездатність багатьох компаній належним чином захистити дані на пристроях своїх віддалених працівників підкреслює недостатній рівень кібербезпеки підприємств в різних галузях по всьому світу.

Ще одним важливим показником для оцінки серйозності та масштабу впливу кіберризиків на діяльність суб’єктів господарювання є динаміка грошових збитків заподіяних кібератаками протягом останніх років. За даними Центру скарг на злочинів в Інтернеті (Internet Crime Complaint Center) у 2023 році грошова шкода заподіяна кіберзлочинністю в США, зросла майже в 12 разів порівняно з 2015 роком, досягнувши історичного піку в 12,5 млрд доларів США (рис. 2.2). Таке стрімке зростання фінансових втрат підкреслює глибокий вплив кіберризиків на бізнес-структури та економіку в цілому.

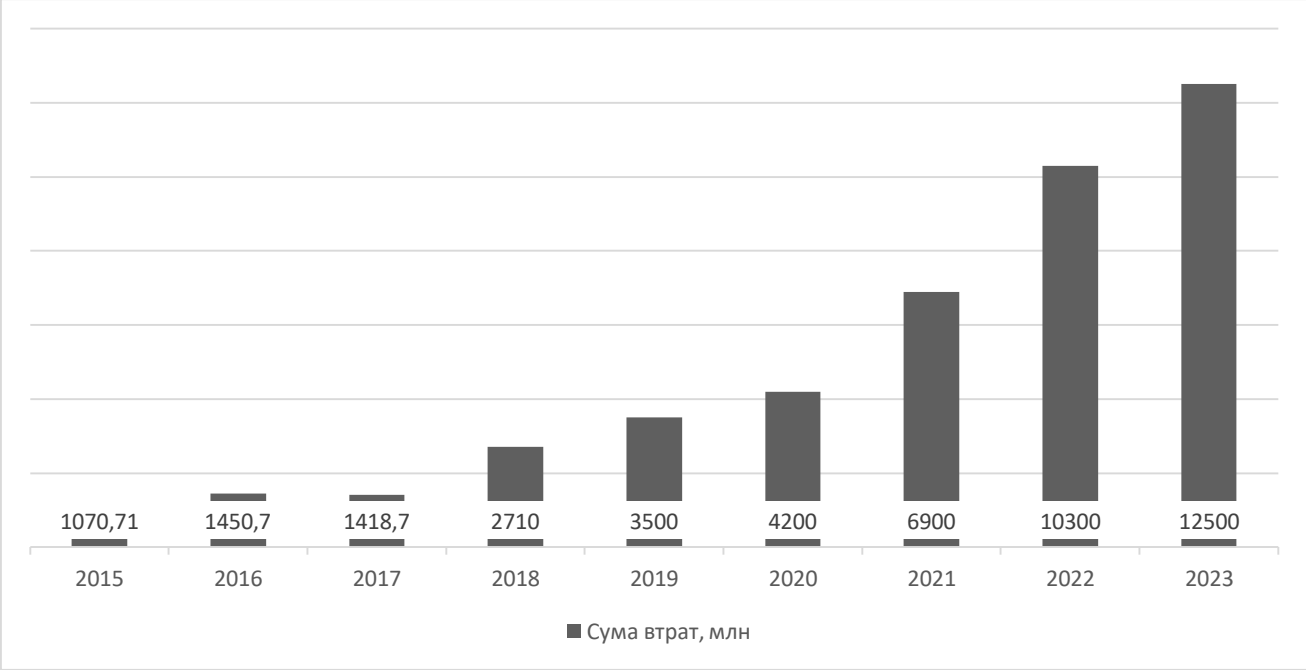

Рис. 2.2. Річна сума грошової шкоди, заподіяної зареєстрованими кіберзлочинами в Сполучених Штатах 2015-2023 рр.

Джерело: складено автором на основі [65]

Суттєвим показників для аналізу впливу кіберризиків на діяльність суб'єктів господарювання та оцінки мінливого ландшафту кіберзагроз є динаміка середнього розміру збитків, понесених організаціями в результаті кібератак. За підсумками 2023 року середня сума збитків, завданих організаціям у США, зросла на 46% порівняно з 2015 роком, досягнувши 9,5 мільйона доларів США (рис. 2.3).

Переважно така тенденція зумовлена цілеспрямованими атаками, які використовують різні інструменти для впливу на кілька систем одночасно та порушення безпеки на кількох рівнях, що свідчить про розвиток кібератак та вразливість IT-систем підприємств.

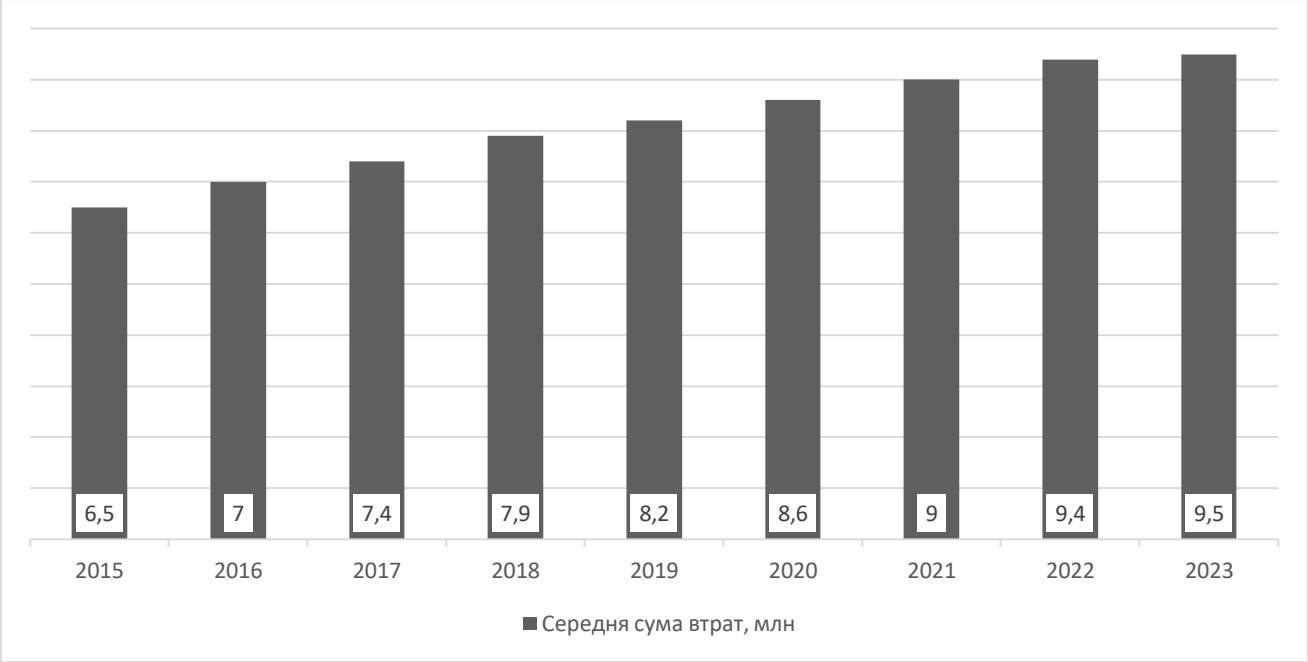

Рис. 2.3. Середня сума втрат організації у США внаслідок кібератак 2015-2023 рр.

Джерело: складено автором на основі [66]

Останнім часом суб'єкти господарювання зіштовхувались зі значною кількістю кібератак, зокрема таких, які вплинули на діяльність організацій по всьому світу. У таблиці 2.1 наведено інформацію про наймасштабніші кібератаки останніх років та їх наслідки для суб'єктів господарювання.

Таблиця 2.1

Наймасштабніші кіберризики останніх років та їх наслідки для суб'єктів господарювання

Назва кібератаки	Наслідки для суб'єктів господарювання
1	2
WannaCry (травень 2017 року)	Зловмисники розповсюдили шифрувальник WannaCry, який заразив понад 200 000 комп'ютерів у 150 країнах світу. Жертвами атаки стали державні установи, лікарні, банки, транспортні компанії та інші організації. Зловмисники вимагали викуп за розшифровку даних. Наслідки: – Припинення роботи тисяч підприємств у 150 країнах світу; – Фінансові втрати через простої системи та втрату даних; – Шкода репутації та втрата довіри клієнтів.

Продовження табл. 2.1

1	2
NotPetya (червень 2017 року)	Зловмисники розповсюдили шифрувальник NotPetya, який заразив понад 100 000 комп'ютерів в Україні, Росії, інших країнах. Жертвами атаки стали державні установи, банки, транспортні компанії та інші організації. Зловмисники не вимагали викуп, а ставили за мету завдати шкоди комп'ютерним системам. Наслідки: – Величезні фінансові втрати, які оцінюються в мільярди доларів США; – Порушення глобальних ланцюгів постачання та виробничих операцій; – Необоротна шкода даним та IT-інфраструктурі.
SolarWinds (виявлено в грудні 2020 року, вплив триває)	Зловмисники зламали програмне забезпечення SolarWinds Orion, яке використовується багатьма державними установами та підприємствами США. Зловмисники отримали доступ до комп'ютерних систем жертв і могли красти дані, шпигувати за ними, проводити інші кібератаки. Наслідки: – Крадіжка даних, шпигунство, збитки репутації; – Розслідування та заходи щодо відновлення тривають досі.
Colonial Pipeline (травень 2021 року)	Зловмисники з групи DarkSide здійснили кібератаку на Colonial Pipeline, найбільший нафтопровід в Східних США. Зловмисники зашифрували дані на комп'ютерах компанії, що призвело до зупинки роботи нафтопроводу. Colonial Pipeline виплатила зловмисникам викуп у розмірі 4,4 мільйона доларів США, щоб розшифрувати дані. Наслідки: – Зупинка роботи, дефіцит пального, зростання цін, збитки понад 5 мільярдів доларів США.

Джерело: складено автором на основі [40,63,69,71,70]

Основний тягар хакерських атак на сьогодні несуть не окремі користувачі, а великі підприємства, які зазнають значних фінансових втрат. Серед найбільш вразливих цілей є фінансові установи, зокрема банки, і реєстратори цінних паперів, враховуючи їхню сильну залежність від сучасної IT-інфраструктури. Крім того, будь-яка організація, яка зберігає електронні дані клієнтів, вразлива до ризику, включаючи аудиторів, роздрібних торговців, брокерських контор, туристичних агентств, транспортних компаній, страхових фірм і розважальних закладів.

Враховуючи мінливий характер кіберзагроз і зростаючу частоту кіберінцидентів, кіберризик став одним із головних глобальних ризиків. Приміром, результати тринадцятого щорічного опитування Allianz Risk Barometer, опублікованого на початку 2024 року, в якому взяли участь 3069 фахівців з управління ризиками з 92 країн, включаючи керівників, спеціалістів зі страхування, брокерів і менеджерів з ризиків, підкреслюють цю тенденцію. Кіберризики, включаючи кіберзлочинність, збої в роботі IT-систем та вразливість даних, стабільно очолюють список глобальних ризиків протягом останніх трьох років. Водночас ризик перебоїв у роботі, які в тому числі можуть бути викликані кібератаками займає друге місце в рейтингу [44].

Згідно зі Звітом про кіберзлочинність за 2023 рік, підготовленим Cybersecurity Ventures, прогнозується різке зростання фінансових втрат від кіберризиків. Очікується, що до 2025 року кіберризики завдуть збитків на суму 10,5 трильйонів доларів США, що значно більше, ніж 3 трильйони доларів США задокументовані у 2015 році. Ці витрати охоплюють цілу низку наслідків, включаючи витрати, пов'язані з витоком даних, фінансовими втратами, крадіжкою інтелектуальної власності, перебоями в роботі і подальшими зусиллями з відновлення [53].

Останніми роками Україна зіткнулася зі зростанням поширеності кіберризиків та їх негативних наслідків. Як свідчить соціологічне дослідження, проведене авторитетною міжнародною консалтинговою компанією PricewaterhouseCoopers (PwC) під назвою «Всесвітнє дослідження економічних злочинів та шахрайства», кіберзлочинність незмінно входить до п'ятірки економічних злочинів, що завдають фінансової шкоди українським підприємствам. Починаючи з 2011 року, це дослідження вказує на значну присутність кіберзлочинності в українському бізнес-середовищі. Зокрема, у 2016 році кіберзлочинність посідала другу позицію в рейтингу, а у 2018 році - п'яте місце

серед інших економічних злочинів. Крім того, дослідження 2020 року підтвердило значний вплив кіберризиків, включивши кіберзлочинність до п'ятірки найпоширеніших видів шахрайства [7].

За даними Національного банку України збитки від шахрайства в інтернеті та з використанням методів соціальної інженерії в Україні постійно зростають, та у 2023 році зафіксовано 272 тис. незаконних операцій з банківськими картками, що на 25% більше, ніж роком раніше. Сума збитків постачальників платіжних послуг, продавців (торговельних мереж та онлайн-магазинів), а також власників банківських карток від дій шахраїв торік сягнула майже 833 млн грн, що на 73% більше, ніж у 2022 році. Середня величина однієї незаконної транзакції у 2023 році зросла до 3065 грн, що на 39% більше порівняно з 2022 роком [24].

Загалом в Україні спостерігається постійне зростання злочинної діяльності у сфері інформаційних технологій. За даними річних звітів Національної поліції України за 2023 рік в Україні було зареєстровано понад 60 тис кіберзлочинів, що в 4,1 рази більше ніж у 2022 році (Рис 2.4).

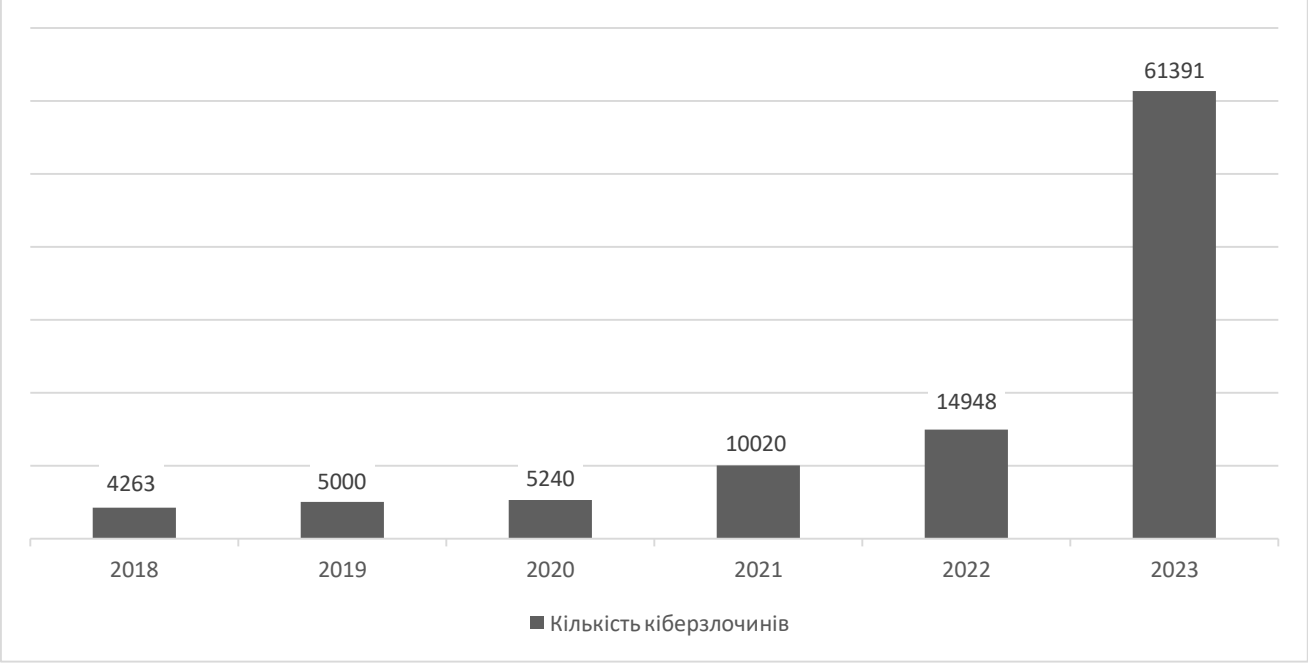

Рис. 2.4. Кількість кіберзлочинів зареєстрованих в Україні за період 2018-2023 рр.

Джерело: складено автором на основі [34]

Крім того масштабні кібератаки росії на українську ІТ-інфраструктуру та бізнес завдають значних збитків українським підприємствам та державним установам. Зокрема в результаті масованої кібератаки, яка сталася 12 грудня 2023 року на одного з найбільших операторів мобільного зв'язку України «Київстар» було завдано збитків на суму приблизно 3,6 млрд гривень (близько 95 млн доларів США). Збитки були пов'язані із заходами, вжитими компанією, для компенсації клієнтам незручностей, спричинених збоями у роботі мережі "Київстар" [51].

Глибокий вплив кіберризиків на суб'єкти господарювання незаперечний, оскільки швидкий розвиток технологій сприяє дедалі складнішій кіберзлочинній діяльності. Такі атаки, від зловмисного програмного забезпечення та програм-вимагачів до складних схем соціальної інженерії, становлять значні фінансові та репутаційні ризики для компаній у всьому світі. Статистичні дані показують, що збитки світової економіки через кібератаки зростають з кожним роком, незважаючи на впровадження традиційних заходів безпеки, кіберзлочинці продовжують використовувати вразливості, що призводить до сплеску кібератак на бізнес.

Така ситуація підкреслює нагальну потребу в надійних заходах управління кіберризиками, яким може виступати страхування, яке допомагає мінімізувати фінансові втрати та пом'якшити наслідки настання кіберінцидентів.

Отже тенденція до зростання кіберризиків та стрімке збільшення розмірів втрат організацій спричинених даними ризиками підкреслює недостатню ефективність традиційних заходів з кібербезпеки. Страхування кіберризиків стає критично важливим інструментом для суб'єктів господарювання, пропонуючи фінансовий захист і пом'якшуючи негативні наслідки кіберінцидентів. Оскільки кіберризики продовжують зростати в усьому світі, компаніям необхідно активно

інвестувати в комплексні стратегії кібербезпеки та використовувати страхування кіберризиків, щоб захистити свою діяльність і зменшити потенційні фінансові втрати.

2.3. Тенденції розвитку страхування кіберризиків в Україні та світі

Страхування кіберризиків – це сектор світового страхового ринку, що швидко розвивається і характеризується інноваційними продуктами, спрямованими на пом'якшення наслідків кіберінцидентів. Це відносно нове явище набуло популярності на початку 2010-х років, коли приватні компанії в США почали підписувати перші договори страхування кіберризиків як засіб пом'якшення своєї відповідальності за збереження та захист даних своїх клієнтів. Згодом, після 2013 року, сектор зазнав значного зростання, спричиненого гучними кібератаками, спрямованими як на корпоративні структури, так і на державну інфраструктуру США.

Починаючи з 2015 року сума страхових премій почала щорічно зростати і в 2023 році становила 16,46 млрд доларів США, що майже в вісім разів більше від суми 2015 року. Страхування кіберризиків стало більш популярним у 2020-2023 роках порівняно з 2015-2019 роками через поширення загроз, спричинених кіберризиками, що прослідковується збільшенням темпів зростання валових страхових премій. Загалом обсяг ринку страхування кіберризиків демонструє середній темп зростання на рівні 25 % протягом 2015-2023 років (рис. 2.5).

Подальшими факторами зростання залишаються триваюча цифрова трансформація та технологічний прогрес у всіх секторах.

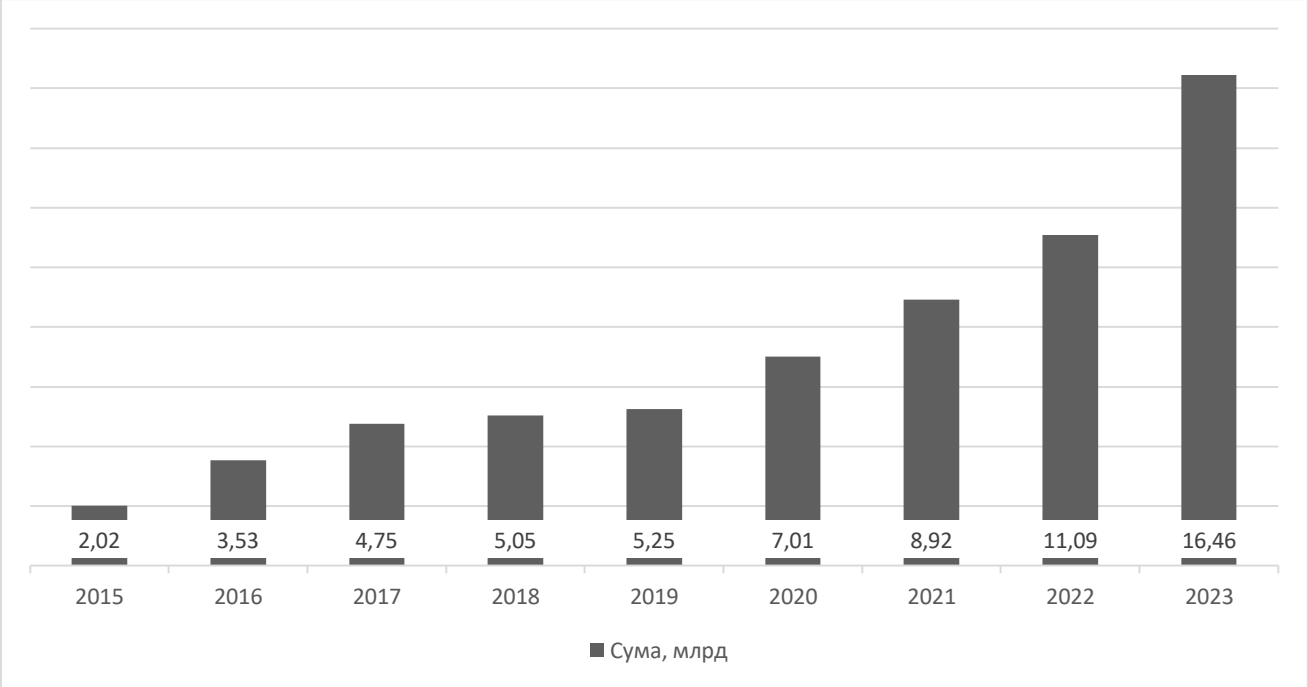

Рис. 2.5. Динаміка росту премій зі страхування кіберризиків у 2015-2023 рр.

Джерело: складено авторамом на основі [50,57]

Найбільша частка премій припадає саме на великі компанії, малі та середні підприємства здебільшого самостійно керують своїми кіберризиками.

Незважаючи на стрімке зростання страхування кіберризиків, поліси покривають лише невелику частину потенційних ризиків. Найпоширенішими витратами, які сьогодні покривають поліси страхування кіберризиків є втрати в результаті нападів програм-вимагачів, підробки корпоративнії пошти, хакерських та фішингових атак (рис. 2.6).

Лідером у сфері страхування кіберризиків на сьогодні є США, які маючи потужну IT-інфраструктуру стали першими, хто зіткнувся зі значними кіберризиками для бізнесу. Крім того, у США діє сувора законодавча база щодо захисту персональних електронних даних. За оцінками Insurance Information Institute у 2023 році на компанії США припадає 56% сплачених премій зі страхування кіберризиків у світі [46]. Тим не менш, на тлі зростання частоти кібератак і поширеного висвітлення в ЗМІ випадків, коли великі корпорації стають

жертвами крадіжки або втрати даних, необхідність придбання ефективних послуг зі страхування кіберризиків набуває все більшого значення серед компаній по всьому світу.

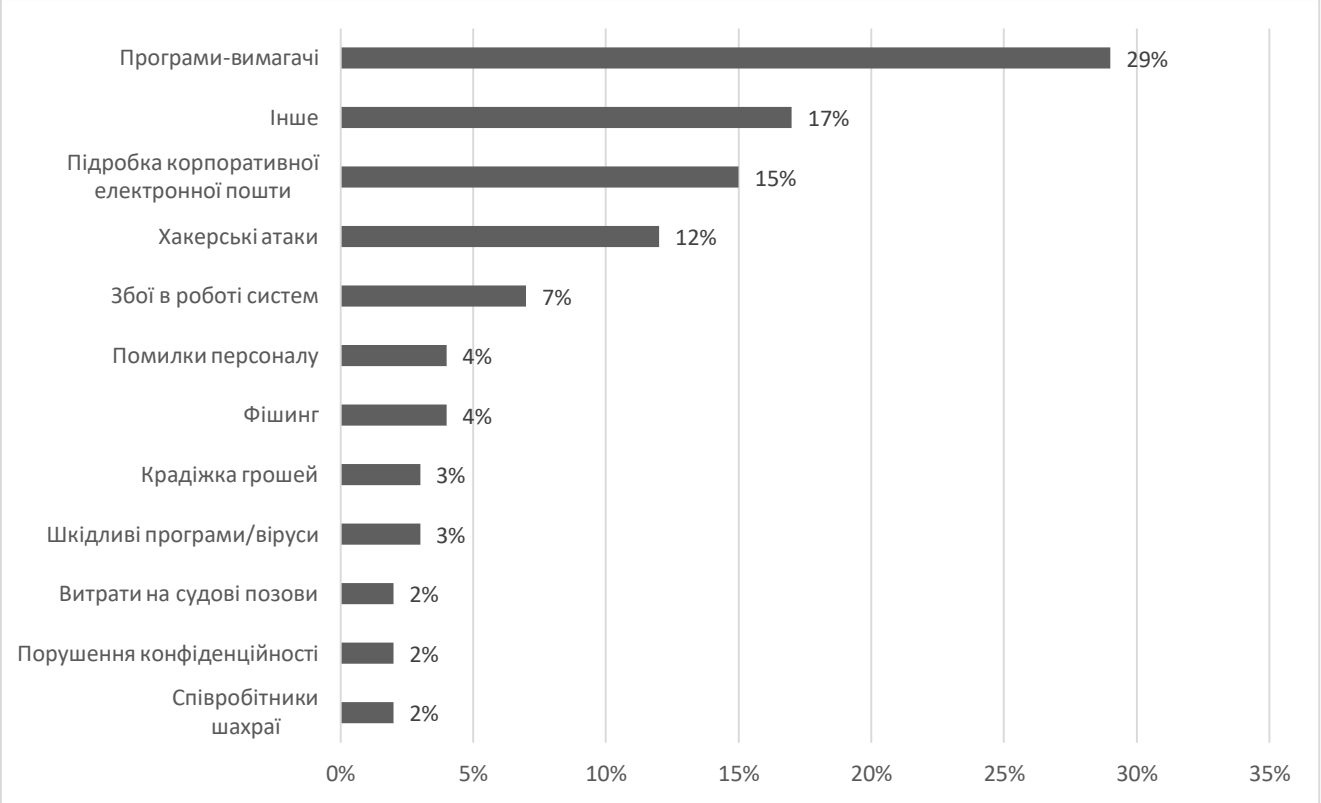

Рис. 2.6. Структура витрат, що покривалися полісами страхування у 2023 р.

Джерело: складено автором на основі [62]

Загалом для розуміння довгострокових тенденцій розвитку даного виду страхування було проведено розрахунки прогнозних значень глобальних страхових премій зі страхування кіберризиків протягом наступних восьми років.

Прогнозування значень показників премій зі страхування кіберризиків здійснено за допомогою статистичного методу екстраполяції на основі плинної середньої, який ґрунтується на припущенні, що тенденція змін показника, яка була виявлена в минулому буде перенесена на майбутні періоди, тобто базується на використанні залежності [8]:

$$\hat{y}_{n+1} = y_n + \Delta\hat{y}_{n+1}, \quad (2.1)$$

де $\hat{y}_{n+1}$ – прогноз показника на основі плинної середньої;

y_n – останнє значення динамічного ряду;

$\Delta\hat{y}_{n+1}$ – прогнозний приріст показника, який визначається за формулою:

$$\Delta\hat{y}_{n+1} = \lambda_n \cdot \Delta y_n + \lambda_{n-1} \cdot \Delta y_{n-1} + \lambda_{n-2} \cdot \Delta y_{n-2} + ... + \lambda_1 \cdot \Delta y_1, \quad (2.2)$$

де n – кількість періодів "передісторії", дані за які будуть використовуватись як база для складання прогнозів на майбутнє;

$\Delta y_n,\ \Delta y_{n-1},\ \Delta y_{n-2},\ \Delta y_1$ – ланцюгові абсолютні прирости статистичних даних;

$\lambda_n\ , \lambda_{n-1}\ , \lambda_{n-2},\ \lambda_1$ – коефіцієнти, розраховані для кожного періоду.

Коефіцієнт λ розраховується за формулою:

$$\lambda_i = \frac{i \cdot \varepsilon}{n}, \quad (2.3)$$

де i — число, яке відображає послідовний натуральний ряд періодів "передісторії" (починаючи з найбільш раннього - i=1 і до останнього - i=n);

ε - визначається залежно від n. таблиці 2.2.

Таблиця 2.2

Розрахункові значення показника ε

n	3	4	5	6	7	8	9	10
ε	0,500	0,400	0,333	0,286	0,250	0,222	0,198	0,180

Джерело: [8]

Вибір даного методу прогнозування обумовлено тим, що головною його особливістю є те, що рівень показників, який знаходиться ближче до прогнозованого періоду, чинить більший вплив на значення прогнозованих показників, порівняно з віддаленими періодами. Досягається це завдяки коефіцієнту λ, що розраховується за формулою (2.3) [8].

Перед проведенням розрахунків, за допомогою програмного забезпечення Microsoft Excel було знайдено коефіцієнт детермінації (R-квадрат), який дорівнює 93%, що свідчить про високу прогнозну здатність моделі.

Вхідними даними для прогнозу є річні обсяги премій зі страхування кіберризиків у світі за період 2015-2023 років, що наведено у таблиці 2.3.

Таблиця 2.3

Вхідні дані для розрахунку прогнозних значень премій зі страхування кіберризиків

Рік	Період спостереження	Премії зі страхування кіберризиків, млрд дол. США
	i	*y*
2015	1	2,0
2016	2	3,5
2017	3	4,8
2018	4	5,1
2019	5	5,3
2020	6	7,0
2021	7	8,9
2022	8	11,1
2023	9	16,6

Джерело: складено автором на основі [50,57]

Згідно з даними наведеними в таблиці 2.2 при n=9 ε=0,198. Звідси за формулою (2.3) розрахуємо коефіцієнти λ:

$$\lambda_1 = \frac{1 \cdot 0{,}198}{9} = 0{,}022 \qquad \lambda_2 = \frac{2 \cdot 0{,}198}{9} = 0{,}044 \qquad \lambda_3 = \frac{3 \cdot 0{,}198}{9} = 0{,}066$$

$$\lambda_4 = \frac{4 \cdot 0{,}198}{9} = 0{,}088 \qquad \lambda_5 = \frac{5 \cdot 0{,}198}{9} = 0{,}110 \qquad \lambda_6 = \frac{6 \cdot 0{,}198}{9} = 0{,}132$$

$$\lambda_7 = \frac{7 \cdot 0{,}198}{9} = 0{,}154 \qquad \lambda_8 = \frac{8 \cdot 0{,}198}{9} = 0{,}176 \qquad \lambda_9 = \frac{9 \cdot 0{,}198}{9} = 0{,}198$$

Результати розрахунку ланцюгових абсолютних приростів премій зі страхування кіберризиків у світі представлено у таблиці 2.4.

Таблиця 2.4

Ланцюгові абсолютні прирости премій зі страхування кіберризиків протягом 2015-2023рр.

Рік	Премії зі страхування кіберризиків, млрд дол. США	Ланцюговий абсолютний приріст, млрд дол. США
2015	2,0	-
2016	3,5	1,5
2017	4,8	1,2
2018	5,1	0,3
2019	5,3	0,2
2020	7,0	1,8
2021	8,9	1,9
2022	11,1	2,2
2023	16,5	5,4

Джерело: складено та розраховано автором на основі [50,57]

Наявні статистичні дані дозволяють обчислити вісім приростів, однак для підстановки у формулу (2.2) їх необхідно 9. За відсутності реального значення приймемо Δy_1 рівним першому відомому приросту, тобто Δy_2=1,5. Підставивши обчислені значення λ_i і Δy_i у формулу (2.2), отримаємо прогнозні прирости премій зі страхування кіберризиків на наступні вісім років та за допомогою формули (2.1) обчислимо прогнозні значення премій зі страхування кіберризиків на період 2024-2031 рр. (табл. 2.5).

Таблиця 2.5

Прогноз премій зі страхування кіберризиків у світі на 2024-2031 рр.

Рік	Прогнозний приріст премій зі страхування кіберризиків, млрд дол. США	Прогноз премій зі страхування кіберризиків, млрд дол. США
2024	2,20	18,7
2025	2,17	20,8
2026	2,10	22,9
2027	2,02	24,9
2028	1,99	26,9

Продовження табл. 2.5

2029	1,97	28,9
2030	1,74	30,7
2031	1,45	32,1

Джерело: складено та розраховано авторами на основі [50,57]

На рис. 2.7 зображено графічний прогноз обсягів премій зі страхування кіберризиків у світі, що був розрахований на основі вхідних даних за період 2015-2023 рр.

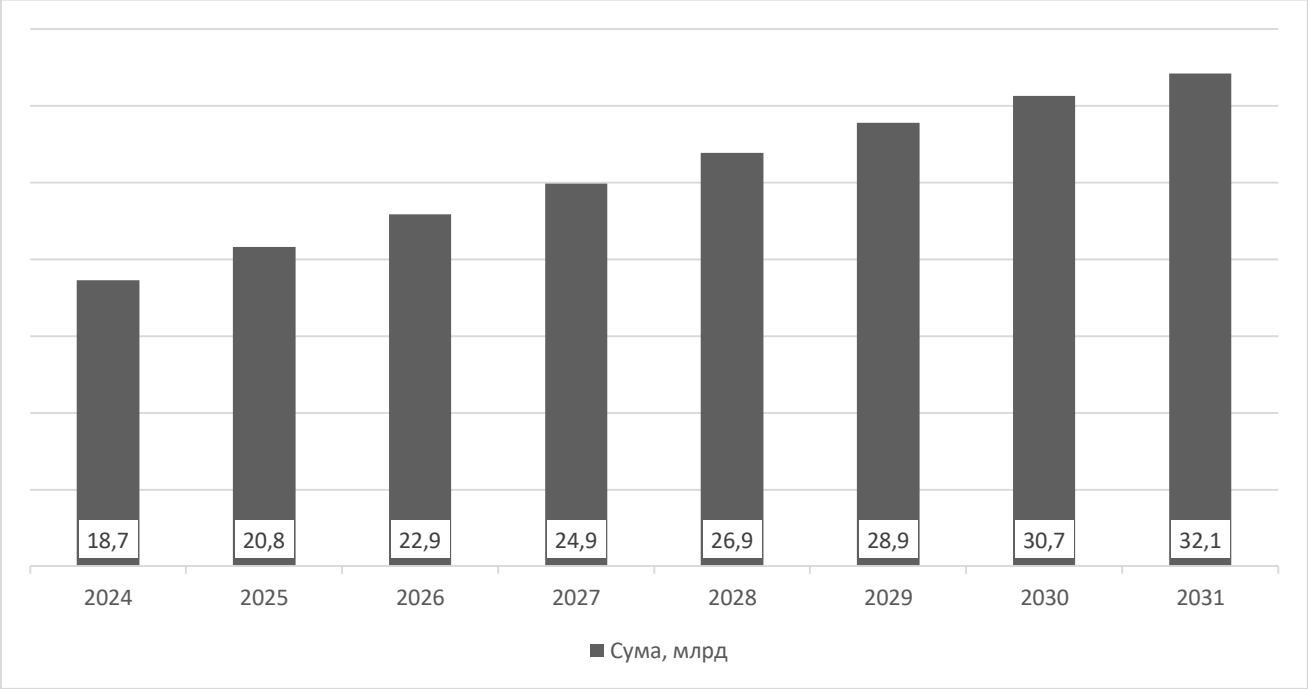

Рис. 2.7. Прогноз росту глобального ринку страхування кіберризиків 2024-2031 рр.

Джерело: складено автором

Таким чином, прогнозовані значення світових премій зі страхування кіберризиків у період з 2024 по 2031 рік вказують на стійку та суттєву траєкторію зростання. Ця тенденція відображає зростаючу важливість кібербезпеки та відповідне зростання попиту на страхові продукти, призначені для пом'якшення наслідків кіберризиків. Прогноз вказує на те, що ринок страхування кіберризиків

буде продовжувати розширюватися, що зумовлено зростанням частоти та складності кіберзагроз у всьому світі.

Страхування кіберризиків стає одним із секторів страхового ринку, що розвивається найбільш динамічно. Темпи розвитку страхування кіберризиків у кожній країні залежать від її соціально-економічного ландшафту, технологічного прогресу, інтеграції IT-технологій та рівня діджиталізації суспільства. В Україні, однак, ринок страхування кіберризиків все ще перебуває на стадії зародження. Інтерес до послуг страхування кіберризиків почав з'являтися приблизно в 2017 році, коли компанії оцінювали втрати та зниження прибутку після атаки вірусу Petya.

Страхування кіберризиків в Україні залишається новою і недостатньо використовуваною концепцією. Хоча сьогодні керівництво підприємств визнає його необхідність, існують певні перешкоди на шляху його широкого впровадження у найближчому майбутньому, такі як фінансові обмеження в компаніях. Крім того, базова інфраструктура, необхідна для просування цієї категорії страхування, все ще перебуває на стадії розвитку.

У контексті України експерти відзначають складнощі у проведенні оцінок інформаційних систем клієнтів через різні обмеження. Як наслідок, не всі страховики готові пропонувати комплексні програми страхування кіберризиків в країні. Серед тих, хто активно займається розробкою та впровадженням таких ініціатив в Україні: СК «АСКА», СК «УПСК» та Центр обробки даних COSMONOVA|NET спільно зі «Страховим брокером «Інсарт». У таблиці 2.6 наведено страховий захист від кіберризиків, який пропонують вищезгадані страхові компанії в Україні.

Таблиця 2.6

Кіберризки, які покривають страхові компанії в Україні

Вид ризику	СК «АСКА»	СК «УПСК»	Центр обробки даних COSMONOVA|NET та «Страховий брокер «Інсарт»
Збитки, пов'язані з порушенням бази даних (цільова атака)	Так	Так	Так
Адміністративне розслідування щодо втрати даних	Так	Ні	Ні
Витрати на реагування при порушенні даних (кіберінцидент)	Так	Так	Так
Відповідальність за контент інформації	Так	Ні	Ні
Віртуальне вимагання	Так	Так	Так
Перерва в процесі виробництва	Так	Так	Так
Соціальная інженерія (нецільова атака)	Так	Так	Так
Витрати на антикризовий PR	Ні	Так	Ні
Витрати на відновлення репутації після кібератаки	Ні	Так	Ні

Джерело: складено автором на основі [17,18,19]

СК «АСКА» пропонує комплексне страхування від кіберризиків на індивідуальних умовах, з урахуванням побажань страхувальника та специфіки його бізнесу. Страховик компенсує прямі збитки від кіберінцідентів, втрати пов'язані з перервою в роботі компанії та відповідальність за витік даних перед партнерами з ЄС. Крім того, поліси страхування покривають витрати на антикризовий PR і витрати на відновлення репутації після кібератаки [17].

Компанія «УПСК» пропонує теж пропонує комплексне рішення зі страхування кіберризиків, що може покриви потенційні збитки від пошкодження, знищення або крадіжки як корпоративних, так і клієнтських даних. Крім того, це рішення допомагає впоратися з потенційними бізнес-кризами, які можуть виникнути в результаті дії кіберризиків [18].

Центр обробки даних COSMONOVA|NET спільно із компанією «Страховий брокер «Інсарт» надають спеціалізовані послуги з оцінки кіберризиків, пропонують

міжнародні умови страхування та сприяють укладанню угод з провідними страховими компаніями по всьому світу, в тому числі зі США та Європи [19].

Загалом менше 5 компаній готові надати послуги страхування від кіберризиків в Україні.

До причин, що зумовлюють гальмування розвитку страхування кіберризиків в Україні можна віднести:

1. Недостатній рівень обізнаності. Багато українських підприємств недооцінюють серйозність кіберризиків і не розуміють переваг, які пропонує кіберстрахування. Відсутність доступних ресурсів, що пояснюють природу кіберстрахування та його потенційні переваги, може перешкоджати зростанню ринку;

2. Прогалини в нормативно-правовій базі. Українське законодавство та регулювання у сфері кібербезпеки все ще перебуває на стадії розвитку. Відсутність чіткого та узгодженого визначення кіберризиків та правил щодо їх страхування може ускладнити роботу страховиків та перешкоджати розширенню ринку;

3. Нестача досвіду та знань у сфері кібербезпеки. Страховим компаніям може не вистачати кваліфікованих фахівців, добре обізнаних у питаннях кібербезпеки та кіберризиків. Цей дефіцит може ускладнити оцінку ризиків, розробку продуктів та обслуговування клієнтів;

4. Низький рівень довіри до страхових компаній. Історично склалося так, що довіра до українських страхових компаній була недостатньою. Цей брак довіри може стримувати бізнес від придбання полісів страхування кіберризиків, навіть якщо вони визнають їх присутність.

5. Небажання страхувальників розкривати інформацію про безпеку. Небажання страховиків надавати доступ до своїх інформаційних систем, життєво важливих для виявлення страхових випадків, у поєднанні з необхідністю

проведення ІТ-аудиту та розкриття інформації про безпеку створюють додаткові перешкоди.

6. Висока вартість страхових продуктів. Через підвищені кіберризики страховики можуть стягувати високі премії за їх страхування, що робить його недоступним для малих та середніх підприємств.

7. Недостатня кількість статистичних даних. Відсутність достовірних даних про кібератаки та їхні наслідки в Україні ускладнює оцінку ризиків страховиками. Це може призвести до неточних цінових стратегій та невідповідності страхових продуктів потребам ринку.

8. Відсутність наукових методик. Відсутність наукового підґрунтя для визначення показників оцінки кіберризиків та розрахунку потенційних втрат, а також стандартів для оцінки збитків та визначення суми відшкодувань.

9. Недостатня культура кібербезпеки. Багато українських компаній нехтують питаннями кібербезпеки, що призводить до частих кібератак та підвищених ризиків для страховиків.

Щоб подолати ці перешкоди та стимулювати розвиток кіберстрахування в Україні, потрібні узгоджені зусилля державних установ, страхових компаній, експертів з кібербезпеки та зацікавлених сторін бізнесу.

Отже, страхування кіберризиків стрімко розвивається у всьому світі завдяки інноваційним продуктам, спрямованим на пом’якшення впливу настання кіберінцидентів. Прогнозі значення обсягу глобальних страхових премій на наступні вісім років свідчать про на стійку та суттєву траєкторію зростання ринку страхування кіберризиків. Лідером на світовому ринку страхування кіберризиків є США, на них припадає більше половини премій, сплачених у всьому світі. Проте все більше компаній у світі визнають необхідність та потребу в страхуванні кіберризиків. В Україні ринок страхування кіберризиків все ще перебуває на стадії формування, йому заважають різні виклики, зокрема недостатня обізнаність,

нормативні прогалини та недостатній досвід. Для сприяння розвитку страхування кіберризиків в Україні необхідні спільні зусилля. Урядові установи, страхові компанії, експерти з кібербезпеки та бізнес-стейкхолдери повинні працювати разом, щоб усунути нормативні прогалини, підвищити обізнаність і набути досвіду в кібербезпеці. Подолання цих перешкод матиме вирішальне значення для просування впровадження страхування кіберризиків та забезпечення належного захисту бізнесу від кіберзагроз.

РОЗДІЛ 3
НАПРЯМИ РОЗВИТКУ СТРАХУВАННЯ КІБЕРРИЗИКІВ В УКРАЇНІ

3.1. Удосконалення інституційно-правового забезпечення страхування кіберризиків

Удосконалення інституційної-правової бази для страхування кіберризиків в Україні є вкрай необхідним з огляду на кілька нагальних факторів. По-перше, зростаюча частота та витонченість кібератак створюють значні загрози як для бізнесу, так і для державних установ та приватних осіб. Зі стрімкою цифровізацією суспільства та економіки Україна, як і багато інших країн, стає все більш залежною від інформаційних технологій та цифрової інфраструктури. Однак ця цифрова трансформація також виявила вразливі місця, зробивши українські підприємства більш чутливими до кіберризиків, таких як витік даних, атаки з вимогою викупу та збої в роботі систем.

Недостатні заходи кібербезпеки та відсутність надійних стратегій управління кіберризиками посилюють ці слабкі місця, залишаючи організації вразливими до фінансових втрат, репутаційних збитків та операційних перебоїв у разі кіберінциденту. Враховуючи взаємопов'язаний характер глобальних кіберзагроз, одна кібератака може мати далекосяжні наслідки, впливаючи не лише на організацію-мішень, але й на її партнерів, клієнтів та економіку в цілому.

Крім того, стан ринку страхування кіберризиків в Україні, що перебуває на стадії становлення, підкреслює нагальну потребу в регуляторному втручанні та інституційній підтримці. Хоча страхування кіберризиків може слугувати важливим

інструментом пом'якшення критичних ризиків, його використання залишається обмеженим через різні проблеми.

Без надійної інституційної та правової бази, яка б регулювала розвиток та функціонування ринку страхування кіберризиків, український бізнес може продовжувати недоінвестувати в кібербезпеку та залишатися вразливим до значних фінансових та операційних ризиків. Крім того, відсутність чітких правил та стандартів для продуктів страхування кіберризиків може перешкоджати зростанню ринку та інноваціям, обмежуючи доступність та вартість варіантів страхування для підприємств усіх розмірів.

Вдосконалюючи інституційну та правову базу для страхування кіберризиків, Україна може вирішити ці проблеми та розкрити весь потенціал страхування як інструменту управління кіберризиками. Зрештою, добре функціонуючий ринок страхування кіберризиків може сприяти підвищенню стійкості до кіберзагроз, підтримці економічного зростання та підвищенню конкурентоспроможності України в цифрову епоху.

Для удосконалення інституційно правового забезпечення страхування кіберризиків в Україні необхідний комплексний підхід, який включатиме ряд заходів (рис. 3.1).

Першим важливим кроком для удосконалення інституційно-правового забезпечення є «визначення на законодавчому рівні сутності поняття «кіберризик». Це передбачає чітке розмежування того, що є кіберризиками, включаючи різні форми кіберзагроз та їх потенційні наслідки. Надаючи точне визначення кіберризиків, законодавство може допомогти забезпечити послідовність і чіткість у тлумаченні та застосуванні вимог і правил кібербезпеки.

Визначення поняття кіберризику на законодавчому рівні має вирішальне значення з кількох причин. По-перше, це допомагає сформувати спільне розуміння природи і масштабів кіберзагроз серед політиків, регуляторів, бізнесу та інших

зацікавлених сторін. Таке спільне розуміння має важливе значення для розробки ефективних стратегій кібербезпеки, розподілу ресурсів та визначення пріоритетів для пом'якшення кіберризиків.

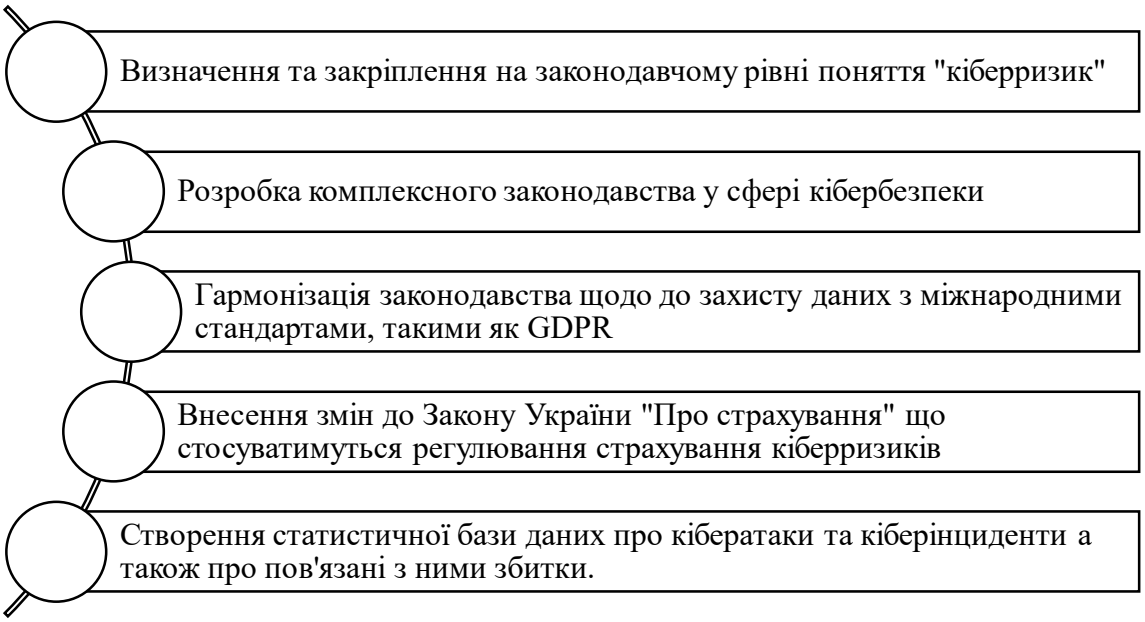

Рис. 3.1. Комплекс заходів для удосконалення інституційно правового забезпечення страхування кіберризиків в Україні.

Джерело: складено автором

Крім того, визначення поняття кіберризику у законодавстві забезпечує юридичну ясність і визначеність для організацій, які прагнуть оцінити та управляти своїм станом кібербезпеки. Це допомагає прояснити типи загроз і вразливостей, які необхідно усунути, а також потенційні наслідки кіберінцидентів. Така ясність може сприяти розробці політики і практик управління кіберризиками, а також вибору відповідних засобів контролю і захисту кібербезпеки.

Крім того, визначення поняття кіберризику на законодавчому рівні дозволяє встановити стандарти та вимоги до продуктів і послуг зі страхування кіберризиків. Це дозволяє політикам визначити типи кіберризиків, які можуть бути покриті страхуванням, а також умови та обмеження покриття. Така ясність є важливою як

для страховиків, так і для страхувальників, оскільки допомагає гарантувати, що поліси страхування кіберризиків забезпечують належний захист від найбільш значущих кіберзагроз та вразливостей.

Ще одним важливим кроком на шляху до вдосконалення інституційної та правової бази для страхування кіберризиків в Україні є «розробка комплексного законодавства у сфері кібербезпеки». Цей крок передбачає розробку та прийняття законів, нормативно-правових актів та політик, які стосуються різних аспектів кібербезпеки, включаючи управління ризиками, захист даних, реагування на інциденти та запобігання кіберзлочинності.

Однією з ключових цілей комплексного законодавства з кібербезпеки є встановлення чітких керівних принципів і стандартів для організацій, яких вони повинні дотримуватися для забезпечення безпеки своїх інформаційних систем і захисту конфіденційних даних. Це можуть бути вимоги щодо впровадження заходів кібербезпеки, таких як шифрування, контроль доступу та системи виявлення вторгнень, а також рекомендації щодо проведення оцінки ризиків та розробки планів реагування на інциденти. Встановлюючи ці вимоги, законодавство має на меті сприяти розвитку культури обізнаності та дотримання вимог кібербезпеки серед бізнесу та державних установ.

Крім того, комплексне законодавство у сфері кібербезпеки має включати положення про правозастосування та підзвітність, у тому числі штрафи за недотримання вимог і правил кібербезпеки. Це може передбачати надання регуляторним органам повноважень проводити аудити та розслідування, накладати штрафи та санкції, а також вживати інших примусових заходів щодо організацій, які не виконують свої зобов'язання з кібербезпеки.

Окрім розробки комплексного законодавства у сфері кібербезпеки, для України вкрай важлива «гармонізація законодавство щодо вимог до захисту даних з міжнародними стандартами, такими як Загальноєвропейський регламент про

захист персональних даних (GDPR)», в рамках вдосконалення інституційного та правового забезпечення страхування кіберризиків. GDPR встановлює суворі вимоги до захисту персональних даних та накладає значні зобов'язання на організації, які обробляють такі дані. Приведення українського законодавства про захист персональних даних у відповідність до GDPR може сприяти зміцненню системи кібербезпеки та розвитку страхування кіберризиків.

Гармонізація українського законодавства з GDPR важлива з кількох причин. Перш за все, це гарантує, що український бізнес, який працює в цифровій економіці, дотримується міжнародно визнаних стандартів захисту даних. Таке узгодження сприяє зміцненню довіри серед споживачів, інвесторів та торговельних партнерів, тим самим підвищуючи конкурентоспроможність України на світовому ринку. Крім того, гармонізація з GDPR сприяє інтероперабельності та полегшує транскордонні потоки даних, що є важливим для сучасного бізнесу, який бере участь у міжнародній торгівлі та співробітництві.

Крім того, прийняття законів про захист даних, узгоджених з GDPR, зміцнює правову базу для страхування кіберризиків в Україні. GDPR накладає на організації суворі вимоги щодо відповідальності та підзвітності у разі витоку даних або порушення принципів захисту даних. Дотримуючись подібних стандартів, український бізнес може краще оцінювати свої кіберризики та відповідальність, а страховикам буде легше укладати поліси страхування кіберризиків. Узгодженість між українським та європейським законодавством про захист даних також спрощує дотримання вимог законодавства для міжнародних компаній, що працюють в Україні, тим самим сприяючи поширенню продуктів страхування кіберризиків.

Крім того, гармонізація з GDPR сприяє підвищенню культури захисту даних та обізнаності щодо кібербезпеки в Україні. Привівши свою законодавчу базу у відповідність до європейських стандартів, Україна може скористатися досвідом та ресурсами, доступними в ЄС, щоб посилити свої можливості та стійкість у сфері

кібербезпеки. Такий спільний підхід зміцнює загальну позицію України у сфері кібербезпеки та сприяє розвитку надійного ринку страхування кіберризиків.

Ще одним важливим кроком є «створення нормативно-правової бази, що регулює страхування кіберризиків, та внесення відповідних правок до Закону України «Про страхування» в рамках удосконалення інституційного-правового забезпечення страхування кіберризиків в Україні. Внесення спеціальних правок до Закону України «Про страхування», які визначатимуть та регулюватимуть страхування кіберризиків є важливим кроком для забезпечення чіткості, послідовності та підзвітності у наданні та регулюванні продуктів страхування кіберризиків.

Такі заходи допоможуть вирішити унікальні проблеми та складнощі, пов'язані зі страхуванням кіберризиків в Україні. Ці правки повинні окреслити сферу покриття кіберстрахування, включаючи типи кіберризиків, що покриваються, умови полісів, процедури відшкодування збитків та регуляторні вимоги. Чіткі та стандартизовані визначення ключових понять, таких як кіберризики та кіберінциденти, витік даних та параметри страхового покриття, мають важливе значення для підвищення прозорості та зменшення двозначності договорів страхування кіберризиків.

Крім того, внесення змін до Закону України «Про страхування» щодо страхування кіберризиків є необхідним для адаптації існуючої нормативно-правової бази до мінливого ландшафту кіберризиків. Ці зміни повинні включати положення, специфічні для кіберстрахування, такі як вимоги до оцінки ризиків, критерії андеррайтингу, методи розрахунку премій та вимоги щодо величини капіталу для страховиків, що пропонують продукти страхування кіберризиків. Крім того, зміни повинні стосуватися питань, пов'язаних із захистом даних, конфіденційністю та вимогами до розкриття інформації, щоб забезпечити

відповідність чинному законодавству та нормативним актам, включаючи міжнародні стандарти, такі як GDPR.

Створення правової бази для страхування кіберризиків у рамках ширшого страхового законодавства посилює регуляторний нагляд та захист прав споживачів, сприяючи підвищенню довіри до продуктів страхування. Чіткі регуляторні настанови допомагають страховикам і страхувальникам орієнтуватися в складнощах страхування кіберризиків, зменшують кількість суперечок і забезпечують справедливе та рівне ставлення до них у разі кіберінцидентів.

Створення правової бази для страхування кіберризиків може сприяти розвитку ринку та інноваціям, забезпечуючи стабільне та передбачуване регуляторне середовище. Чіткість регуляторних вимог заохочує страховиків розробляти інноваційні продукти страхування кіберризиків, пристосовані до мінливих потреб бізнесу та фізичних осіб. Це також приваблює нових учасників ринку, включаючи як вітчизняних, так і іноземних страховиків, тим самим підвищуючи конкуренцію і розширюючи можливості страхування для споживачів.

Важливим заходом також є «створення статистичної бази даних, в якій збиратимуться дані про кібератаки та кіберінциденти, класифіковані за різними типами, а також про пов'язані з ними збитки». Така база даних відіграватиме ключову роль у вдосконаленні інституційного та правового забезпечення страхування кіберризиків, надаючи страховикам надійну інформацію для точної оцінки масштабів та наслідків кіберзагроз.

Створення централізованої статистичної бази даних, щодо кіберінцидентів, дозволятиме систематично збирати, аналізувати та повідомляти дані про різні типи кібератак, включаючи зараження шкідливим програмним забезпеченням, фішингове шахрайство, атаки з вимогами викупу, витік даних та інші форми кіберризиків. Класифікуючи кіберінциденти за їхніми характеристиками та

ступенем серйозності, база даних дозволятиме страховикам виявляти нові тенденції, закономірності та вразливі місця в ландшафті кібербезпеки.

Крім того, статистична база даних полегшує оцінку фінансових наслідків кіберінцидентів, документуючи збитки, понесені бізнесом, державними установами та приватними особами в результаті кібератак. Зібравши вичерпні статистичні дані про прямі та непрямі витрати, пов'язані з кіберризиками, включаючи фінансові втрати, репутаційні збитки та регуляторні штрафи, база даних надасть страховикам цінну інформацію про економічні наслідки кіберризиків.

Наявність точної та актуальної статистики про кібератаки та збитки від кіберінцидентів дозволяє страховикам розробляти моделі ризиків на основі даних та стратегії ціноутворення для продуктів страхування кіберризиків. Аналізуючи історичні дані про кіберінциденти, страховики можуть оцінити ймовірність і серйозність майбутніх кіберзагроз, оцінити потенційну схильність страхувальників до кіберризиків і визначити відповідний рівень страхового покриття та премій.

Удосконалення інституційної та правової бази для страхування кіберризиків в Україні має вирішальне значення для подолання зростаючих кіберзагроз, з якими стикаються підприємства та громадяни. Визначивши кіберризики на законодавчому рівні, гармонізувавши українське законодавство з міжнародними стандартами, такими як GDPR, та розробивши комплексне законодавство з кібербезпеки, Україна може посилити свою кібербезпеку та створити сприятливе середовище для страхування кіберризиків. Створення статистичної бази даних сприятиме подальшому розвитку ринку страхування кіберризиків.

3.2. Підвищення рівня охоплення страхуванням кіберризиків суб’єктів господарювання

Підвищення рівня страхового покриття кіберризиків серед суб'єктів господарювання в Україні є вкрай необхідним з кількох вагомих причин.

По-перше, мінливий ландшафт кіберзагроз створює значні виклики для бізнесу всіх розмірів та галузей в Україні. З поширенням складних кібератак, таких як програми-вимагачі, витоки даних та фішинг-шахрайство, бізнес стикається з підвищеними ризиками фінансових втрат, репутаційних збитків та зупинок в роботі. Ці кіберризики можуть призвести до значних збитків, включаючи витрати на усунення наслідків, судові витрати, регуляторні штрафи та втрату доходу. Отримавши належне страхове покриття, бізнес може зменшити ці фінансові ризики та забезпечити свою довгострокову життєздатність.

По-друге, цифровізація економіки та зростаюча залежність від інфраструктури інформаційних технологій посилили вразливість українського бізнесу до кіберризиків. У міру того, як організації впроваджують ініціативи цифрової трансформації, вони стають більш взаємопов'язаними та залежними від цифрових систем, що тим самим розширює поле для атак кіберзлочинців. Як наслідок, потенційний вплив кіберризиків на бізнес-операції, довіру клієнтів та загальну стійкість зростає. Страхування кіберризиків забезпечує важливу систему безпеки, пропонуючи фінансовий захист і підтримку компаніям, які постраждали від кіберризиків, дозволяючи їм швидко відновитися і мінімізувати перебої в роботі.

По-третє, повномасштабне вторгнення росії в Україну загострило ситуацію з кібербезпекою, що призвело до зростання кіберризиків та кібератак на українські підприємства. Війна, що триває, створила сприятливий ґрунт для використання кіберпротивниками вразливостей та початку зловмисної діяльності, спрямованої на порушення роботи критичної інфраструктури, викрадення конфіденційної інформації та поширення дезінформації.

Український організації, особливо ті, що працюють у критично важливих для національної безпеки секторах, таких як енергетика, фінанси та державне управління, стають все більш вразливим до кіберризиків в умовах війни. Як наслідок, потреба в надійних заходах кібербезпеки та комплексному страховому захисті стала більш відчутною, ніж будь-коли раніше.

Страхування кіберризиків відіграє ключову роль у пом'якшенні фінансових наслідків кіберінцидентів, дозволяючи бізнесу швидко відновлюватися і продовжувати свою діяльність в умовах постійних загроз. Тому підвищення рівня страхового покриття кіберризиків стає стратегічним засобом для забезпечення стійкості та безперервності українського бізнесу в умовах повномасштабної війни.

На рисунку 3.2 зображено систему заходів для підвищення рівня охоплення страхуванням кіберризиків суб’єктів господарювання в Україні.

Першим важливим кроком є «підвищення рівня обізнаності серед підприємств про кіберризики та їх наслідки». Чим краще підприємці розуміють загрози, які становлять кіберризики, та потенційний збиток, який вони можуть завдати, тим ймовірніше, що вони будуть вживати заходів для захисту своїх даних та систем. Щоб підвищити обізнаність компаній, вони повинні бути поінформовані про:

- Різні види кіберризиків, з якими вони можуть зустрітись, включаючи витік даних, атаки програм-вимагачів, фішинг та DDoS-атаки;
- Методи, які використовують кіберзлочинці, наприклад тактики соціальної інженерії або розповсюдження зловмисного програмного забезпечення;
- Наслідки кіберінцидентів, що можуть виходити за межі фінансових втрат і включати шкоду репутації, юридичну відповідальність, регуляторні штрафи та порушення критичних бізнес-функцій.
- Можливі засоби захисту та мінімізації кіберризиків.

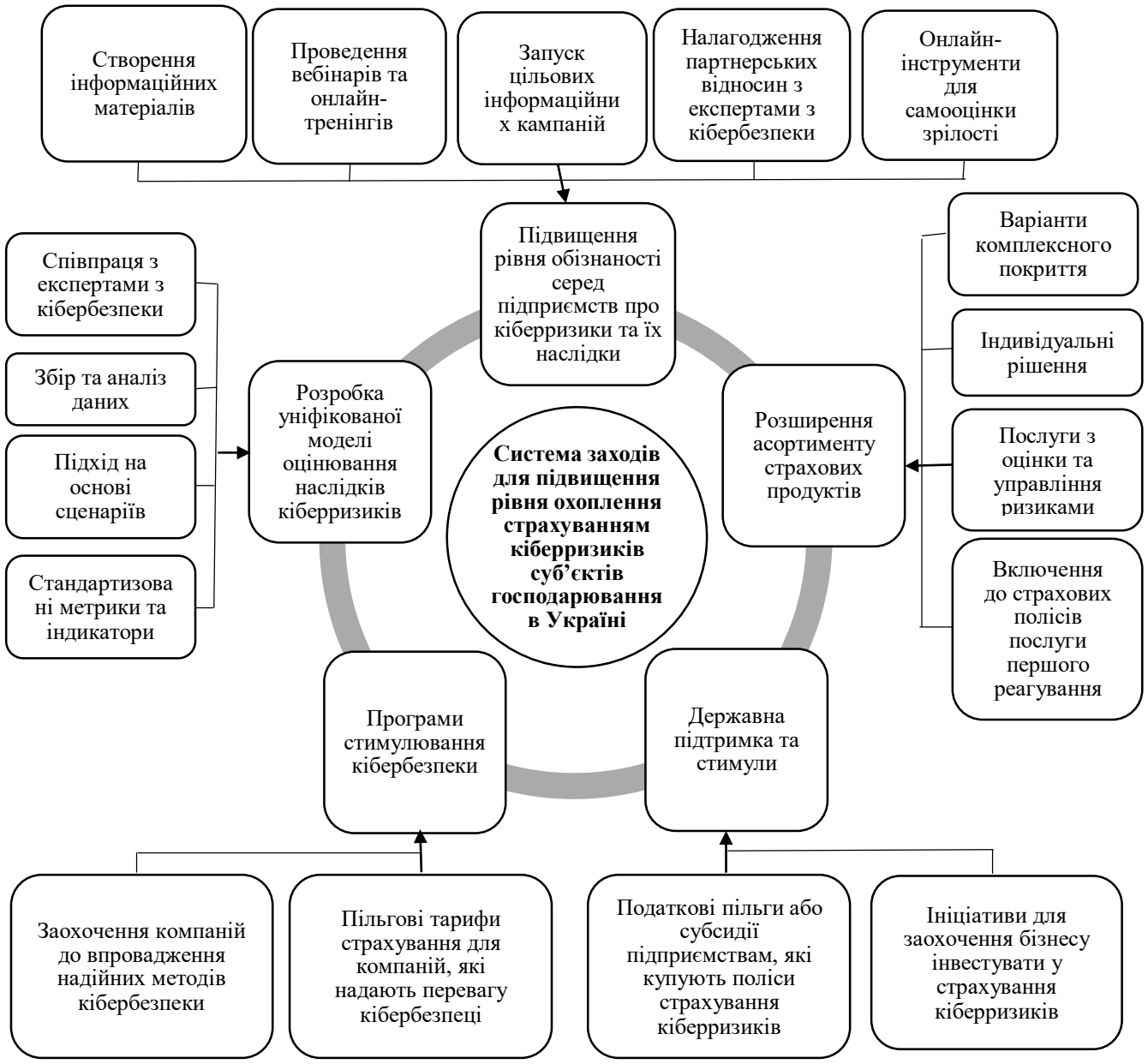

Рис. 3.2. Система заходів для підвищення рівня охоплення страхуванням кіберризиків суб'єктів господарювання в Україні

Джерело: складено автором

Щоб поширювати інформацію та підвищувати обізнаність, можна використовувати різні канали та засоби, серед яких можуть бути:

1. Створення інформаційних матеріалів, таких як: цікавий мультимедійний вміст, зокрема відео, інфографіка та подкасти, які висвітлюватимуть ключову інформацію про кіберризики в доступному форматі;

2. Проведення вебінарів та онлайн-тренінгів за участю експертів у галузі кібербезпеки, де обговорюватимуться нові кіберзагрози, тенденції кібербезпеки та стратегії управління кіберризиками;

3. Запуск цільових інформаційних кампаній, з використання соціальних мереж, інформаційних бюлетенів електронною поштою та галузевих форумів для поширення інформації про кіберризики та кібербезпеку.

4. Налагодження партнерських відносин з експертами з кібербезпеки, щоб спільно проводити заходи та ініціативи з підвищення обізнаності.

5. Онлайн-інструменти для самооцінки зрілості кібербезпеки компанії, щоб допомогти компаніям оцінити їх поточний стан безпеки.

Підвищення обізнаності про кіберризики та їх наслідки, стимулюватиме підприємства приймати обґрунтовані рішення щодо страхового покриття від кіберризиків і визначати пріоритетність інвестицій у заходи кібербезпеки, які відповідають їх схильності до ризику та бізнес-цілям.

«Розширення асортименту страхових продуктів, які відповідають потребам українських підприємств» є важливим інструментом підвищення рівня страхового покриття кіберризиків. Цей крок передбачає розробку та пропонування страхових продуктів, адаптованих до конкретних потреб у сфері кібербезпеки та профілів ризиків українського бізнесу. Для цього необхідно дослідити кіберризики, з якими найчастіше зіштовхуються українські підприємства та організації.

Згідно з висновками звіту CyberPeace Institute, протягом третього кварталу 2023 року український бізнес та державні установи зіткнулися з низкою кібератак, серед яких DDoS-атаки, зараження шкідливим програмним забезпеченням, спроби фішингу, інциденти з підміною сторінок веб-сайтів (дефейс) та wiper-атаки (атаки,

що мають на меті стерти дані з жорсткого диска жертви). Серед них DDoS-атаки становили більшість - 89,7% від усіх кіберзлочинів (рис. 3.3).

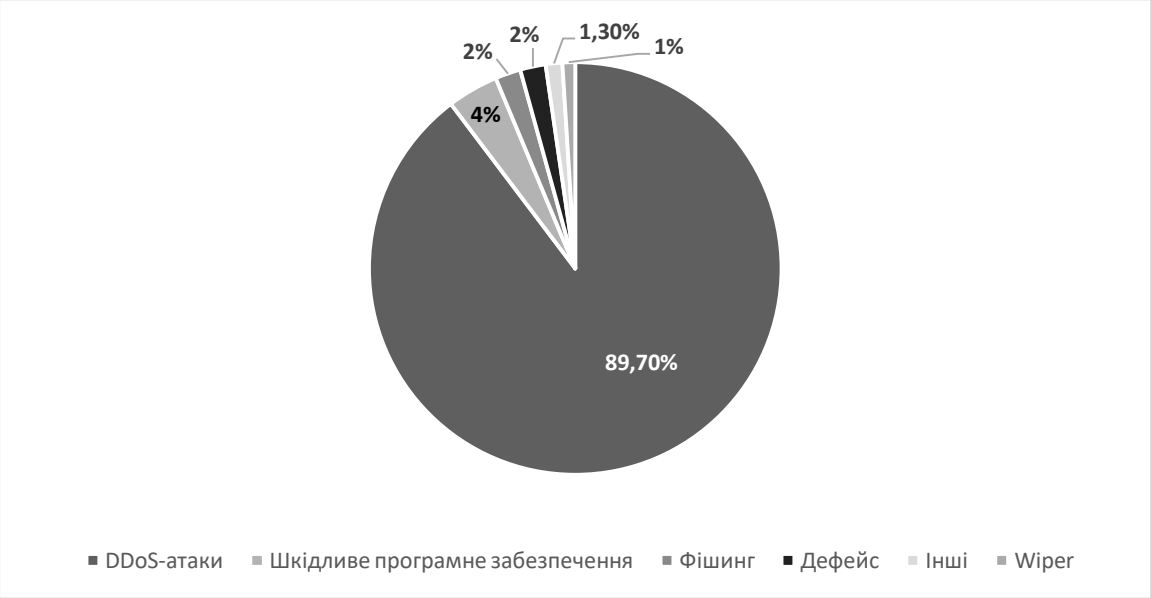

Рис. 3.3. Види кібератак спрямованих на українських суб'єктів у липні-вересні 2023р.

Джерело: складено автором на основі [49]

Крім того, слід зазначити, що такі сектори, як державне управління, засоби масової інформації, інформаційно-комунікаційні технології (ІКТ), фінанси та торгівля зазнали найбільшої кількості кібератак [49].

Розширенню асортименту страхових продуктів, може сприяти створення:

- Варіантів комплексного покриття. Постачальникам страхових послуг необхідно розробити варіанти комплексного страхового покриття кіберризиків, які охоплюватимуть широкий спектр потенційних загроз та інцидентів, з якими стикаються українські підприємства. Такі поліси мають передбачати покриття найбільш поширених кіберризиків, таких як випадки витоку даних, атаки програм-вимагачів, перерви в бізнесі, відповідальність за безпеку мережі, а також регуляторні штрафи і пені;

- Індивідуальні рішення. Страхові продукти повинні бути гнучкими, щоб відповідати різноманітним потребам і схильності до ризику різних підприємств. Це може передбачати гнучкі умови полісів та лімітів покриття, щоб дозволити компаніям адаптувати страховий захист до своїх конкретних ризиків кібербезпеки та бюджетних обмежень;
- Послуги з оцінки та управління ризиками. Страхові компанії можуть запропонувати додаткові послуги, такі як оцінка ризиків, консультації з кібербезпеки та планування реагування на інциденти, щоб допомогти підприємствам завчасно виявляти та зменшувати кіберризики. Ці послуги можуть допомогти підприємствам посилити свою кібербезпеку та зменшити ймовірність і серйозність кіберінцидентів, а також зробити послуги страхування кіберризиків більш привабливими;
- Включення до страхових полісів послуги першого реагування на кіберінцидент. Такі послуги можуть підвищити загальну цінність і ефективність страхового покриття кіберризиків, крім того вони також дають страховим компаніям певний контроль якості управління інцидентами, полегшуючи прогнозування та управління витратами. Така послуга, як правило, має форму телефонної служби «єдиного вікна», куди застрахований телефонує, коли трапляється кіберінцидент. Страхові компанії не надають цю послугу власними силами, а співпрацюють із IT-консультантами, юридичними фірмами, PR-консультантами тощо, які надають фактичні послуги першого реагування. Як правило, першу відповідь координує юридична фірма або спеціальна фірма з управління претензіями, яка за потреби залучає інших консультантів [68].

«Розробка уніфікованої моделі оцінювання наслідків кіберризиків» є важливим засобом для підвищення рівня страхового захисту кіберризиків серед суб’єктів господарювання. Такий структурований підход страховики зможуть використовувати для кількісної оцінки потенційних збитків у результаті різних

типів кібератак. Ця модель повинна враховувати такі фактори, як тип і серйозність атаки, ступінь компрометації даних, фінансові втрати, збої в роботі, репутаційні збитки та регуляторні санкції. Процес розробки моделі оцінювання наслідків кіберризиків включає:

1. Співпрацю з експертами з кібербезпеки. Страхові компанії можуть співпрацювати з експертами з кібербезпеки, аналітиками даних, аналітиками ризиків та урядовими установами для розробки комплексної моделі оцінки наслідків кіберінцидентів, такими наприклад як CERT-UA, що є урядовою командою реагування на комп'ютерні надзвичайні події в Україні. Співпраця з CERT-UA може допомогти у отриманні інформації про нові кіберзагрози, галузеві вразливості та найкращі практики оцінки збитків в Україні [14].

2. Збір та аналіз даних. Створення централізованої бази даних для збору та аналізу даних про минулі кіберінциденти може стати основою для розробки моделі оцінки. Вивчаючи історичні дані, страховики можуть виявити закономірності, тенденції та спільні риси кібератак, що дасть їм змогу вдосконалити свої критерії оцінки ризиків.

3. Підхід на основі сценаріїв. Розробка сценарного підходу може допомогти страховикам змоделювати різні сценарії кібератак та їхній потенційний вплив на бізнес. Моделюючи різні сценарії атак, страховики можуть оцінити ймовірність і серйозність потенційних збитків, що дозволить їм адаптувати страхове покриття до конкретних потреб різних підприємств.

4. Стандартизовані метрики та індикатори. Впровадження стандартизованих показників та індикаторів для оцінки наслідків кіберінцидентів може покращити узгодженість та порівнянність між страховими полісами. Ці показники можуть включати оцінку фінансових втрат, цілі щодо часу відновлення, вплив на репутацію бренду та витрати на дотримання нормативних вимог.

Впроваджуючи уніфіковану модель оцінки наслідків кіберінцидентів, страхові компанії можуть розширити свої можливості з управління ризиками, надавати більш точні варіанти страхового захисту бізнесу і, в кінцевому підсумку, підвищити рівень страхового покриття кіберризиків.

«Державна підтримка та стимули» відіграють важливу роль у заохоченні компаній інвестувати в страхування кіберризиків, тим самим підвищуючи загальний рівень охоплення суб'єктів господарювання. Державна підтримка може включати:

– Запровадження державних ініціатив для заохочення бізнесу інвестувати у страхування кіберризиків;

– Надання податкових пільг або субсидій підприємствам, які купують поліси страхування кіберризиків або інвестують у заходи з кібербезпеки.

Сьогодні страхові компанії не готові страхувати будь-які кіберризики, навіть за умови, що сплачена премія є достатньо високою, якщо рівень кібербезпеки підприємства не відповідає певним мінімально-допустимим критеріям. Залежно від результатів оцінки клієнта іноді не робиться жодної пропозиції, а іноді пропонується лише частковий захист, якщо клієнт не відповідає певним вимогам. Наприклад, клієнтам без визначеного процесу реагування на кіберінциденти можуть взагалі відмовляти у послугах страхування, або пропонувати привести їх рівень кібербезпеки до мінімальних вимог для можливості купівлі полісу страхування кіберризиків [68].

Тому «програми стимулювання кібербезпеки» спрямовані на заохочення компаній інвестувати в надійні заходи кібербезпеки є важливим засобом для підвищення рівня покриття страхуванням кіберризиків суб'єктів господарювання. Пропонуючи винагороди та переваги за впровадження ефективних методів безпеки, такі програми стимулюватимуть проактивні зусилля компаній із захисту своїх цифрових активів і даних від кіберзагроз і надаватимуть стимули для сприяння

постійному вдосконаленню стану кібербезпеки, що надасть можливість цим компанія купувати поліси з більш широким страховим покриттям.

Основним компонентом програм стимулювання кібербезпеки є:

– Розробка програм заохочення, які винагороджуватимуть компанії за впровадження надійних методів кібербезпеки.

– Надання пільгових тарифів страхування або розширені варіанти покриття для компаній, які надають перевагу кібербезпеці.

Отже, підвищення рівня страхового покриття кіберризиків має важливе значення для українського бізнесу, щоб протистояти мінливому ландшафту загроз, захистити свої фінансові інтереси, відповідати регуляторним вимогам та підвищити свою стійкість у світі, що стає все більш цифровим. Сприяти поширенню страхування кіберризиків можна за допомогою системи заходів, таких як підвищення рівня обізнаності, розширення асортименту страхових продуктів, розробка уніфікованої моделі оцінювання наслідків кіберризиків, державна підтримка та програми стимулювання кібербезпеки.

ВИСНОВКИ

Дослідження актуальної проблеми розвитку страхування кіберризиків в Україні, дозволило зробити наступні висновки та надати такі пропозиції:

1. Кіберризики стають все більш серйозною загрозою для сучасного суспільства, адже вони можуть призвести до значних фінансових збитків, шкоди репутації, розголошення конфіденційних даних та інших негативних наслідків. Існує також безліч типів кіберзагроз, таких як шкідливе програмне забезпечення, програми-вимагачі, переривання діяльності, мережева безпека, відповідальність за конфіденційність, кібервимагання, шахрайські перекази, відповідальність перед третіми особами, штрафи регуляторних органів та реагування на інциденти. Основними подіями, що спричиняють появу кіберризиків є зловмисні дії, технічні збої в роботі та людські помилки. Розуміння основних типів кіберризиків та їх наслідків є важливою складовою для розроблення ефективних стратегій управління ними.

2. Страхування кіберризиків є ефективним інструментом мінімізації фінансових втрат та пом’якшення негативних наслідків настання кіберінциденту. Поліси страхування кіберризиків можуть покривати прямі збитки, збитки завдані третім особам, додаткові витрати, такі як витрати на юридичний супровід або сплату штрафів, та витрати на додаткові послуги пов’язані з врегулюванням наслідків кіберінциденту. Страхування кіберризиків доповнюючи традиційні технічні заходи безпеки, надає організаціям фінансовий захист від потенційних фінансових втрат і зобов’язань, пов’язаних з кіберінцидентами.

3. Розвиток страхування кіберризиків можна умовно розділити на кілька ключових етапів: зародження цифрових технологій, масове виробництво цифрових технологій, фактичне створення страхування кіберризиків, розширення та

вдосконалення інструментів страхування кіберризиків та імплементація нормативно-правового забезпечення для страхування кіберризиків. Кожен з цих етапів відображає еволюцію відповіді страхової галузі на нові виклики та складності кібербезпеки. Ці етапи підкреслюють поступове дозрівання страхування кіберризиків від його початку до його нинішнього статусу як життєво важливого компонента комплексних стратегій управління ризиками.

4. Страхування кіберризиків в Україні наразі чітко не врегульовано на законодавчому рівні, хоча здійснено певні кроки у даному напрямку. Законом України «Про страхування» визначає основні принципи та засади його здійснення, однак даний нормативно-правовий акт не містить визначення кіберризиків та конкретних правил щодо їх страхування. Крім того в Україні діє низка законів, що стосуються сфери кібербезпеки, однак неузгодженість термінології в даних документах ускладнює їх практичне застосування. Вдосконалення законодавчої бази для страхування кіберризиків сприятиме його розвитку та поліпшенню інформаційної безпеки України.

5. Швидке зростання збитків спричинених кіберінцидентами протягом останніх років підкреслює значний вплив кіберризиків на діяльність організацій та урядових установ по всьому світу. За результатами останніх щорічних опитуваннь Allianz Risk Barometer кіберризики вже протягом трьох років очолюють список глобальних ризиків. В Україні кіберризик входять в топ-5 найбільш економічних злочинів, що завдають фінансової шкоди підприємствам, а кількість кримінальних правопорушень у сфері інформаційних технологій має стійку тенденцію до зростання. Поширення негативного впливу кіберризиків на суб’єкти господарювання підкреслює нагальну потребу в надійних заходах управління ними, яким може виступати страхування.

6. Страхування кіберризиків є сектором світового страхового ринку, що характеризується швидкими темпами розвитку. Протягом останніх років сума

річних премій зі страхування кіберризиків в світі збільшилась майже в вісім разів, а прогноз їх обсягу на наступні вісім років свідчить про стійку та суттєву траєкторію зростання ринку страхування кіберризиків. Основними факторами, що стимулюють розвиток даного виду страхування є триваюча цифрова трансформація та технологічний прогрес у всіх секторах. В Україні страхування кіберризиків перебуває на стадії розвитку і на даному етапі такі послуги пропонують менше 5 компаній. Така ситуація обумовлена рядом причин, серед яких недостатня обізнаність, прогалини у нормативно-правовій базі, висока вартість страхових продуктів, недостатність статистичних даних та ін.

7. Стан ринку страхування кіберризиків в Україні, що перебуває на стадії становлення, підкреслює нагальну потребу в регуляторному втручанні та інституційній підтримці. Для удосконалення інституційно правового забезпечення страхування кіберризиків в Україні необхідний комплексний підхід, що включає визначення на законодачому рівні поняття «кіберризику», розробку комплексного законодавства у сфері кібербезпеки, гармонізацію законодавства щодо до захисту даних з міжнародними стандартами та створення статистичної бази даних про кібератаки та кіберінциденти. Впровадження таких заходів може свою кібербезпеку України та створити сприятливе середовище для страхування кіберризиків.

8. Підвищення рівня охоплення страховим покриттям кіберризиків суб'єктів господарювання стає стратегічним засобом для забезпечення стійкості та безперервності українського бізнесу в умовах сучасних викликів. Підвищення рівня охоплення включає в себе систему заходів, серед яких підвищення рівня обізнаності, розширення асортименту страхових продуктів, розробка уніфікованої моделі оцінювання наслідків кіберризиків, державна підтримка та програми стимулювання кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бараненко Р.С. Токарєв В.О. Кібер-страхування в умовах цифрової економіки. Сучасні гроші, банківські послуги та фінансові інновації в цифровій економіці: матеріали наук.-практ. інтерн. конф. студ. аспір. і молод. вчених — Дніпро: Середняк Т. К., 2021, с. 175 — 176.

2. Беспалова Ю.Ю. Кібер-страхування як інструмент управління ризиками в умовах цифрової трансформації. *Шевченківська весна 2024. Стратегії економічного зростання: погляд у майбутнє для України*, матеріали Міжнародної науковопрактичної конференції студентів, аспірантів та молодих вчених / За заг. ред. Л.А. Анісімової: - К., Інтерсервіс, 2024. – Вип. XXII. С.173-174.

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

4. Відшкодування збитків після кібер-атаки. Страховий адвокат. 2017. URL: https://www.insa.com.ua/blog/kiberataki-kak-zashhitit-biznes-ot-novogooruzhiya/ (дата звернення 27.04.2024) (дата звернення: 27.04.2024)

5. Віннікова І.І., Марчук С.В. Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними. *Східна Європа: економіка, бізнес та управління.* 2018. Випуск 5 (16). С. 110–114. URL: http://easterneurope-ebm.in.ua/journal/16_2018/21.pdf (дата звернення: 27.04.2024)

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

7. Всесвітнє дослідження економічних злочинів та шахрайства 2020. PwC. URL: https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf (дата звернення: 27.04.2024)

8. Галущак М. П., Галущак О. Я., Кужда Т. І. Прогнозування соціально-економічних процесів: навчальний посібник для економічних спеціальностей. – Тернопіль: ФОП Паляниця, 2021. – 160 с.

9. Гудзь О. Розвиток страхування: нові інструменти та методи управління ризиками в цифровій економіці. *Економіка. Менеджмент. Бізнес.* № 3 (29). 2019. Ст. 4—12. DOI: 10.31673/2415-8089.2019.030412.

10. Іванова Т. Г. Перспективи розвитку ринку кіберстрахування в Україні. *Проривні інновації на страховому ринку України*: Збірник матеріалів V Міжн. науково-практичної інтернет-конференції, м. Київ, 27 жовтня 2021 р. К.: КНЕУ, 2021. — 263 с. ISBN 978-966-926-397-1 URL: https://econom.lnu.edu.ua/wp-content/uploads/2016/09/Zbirnyk_materialiv_Proryvni_innovatsii_na_strakhovomu_rynku_Ukrainy.pdf (дата звернення: 27.04.2024)

11. Івашина Н. В. Кібер-страхування: новий інструмент страхового ринку. *Інформаційні технології: наука, техніка, технологія, освіта, здоров'я*: наук. вид. : тези доп. 25-ї міжнар. наук.-практ. конф. MicroCAD–2017, [17-19 травня 2017 р.] : у 4 ч. Ч. 4 / ред. Є. І. Сокол. – Харків : НТУ "ХПІ", 2017. С. 208

12. Конвенція про кіберзлочинність. *Рада Європи*; Конвенція, Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 27.04.2024)

13. Новий регламент ЄС про персональні дані. Olans Group. URL: https://www.olans.com.ua/novij-reglament-yes-pro-personalni (дата звернення 27.04.2024)

14. Офіційний сайт CERT-UA. URL: https://cert.gov.ua/ (дата звернення: 27.04.2024)

15. Офіційний сайт DGPR. URL: https://gdpr-info.eu/ (дата звернення: 27.04.2024)

16. Офіційний сайт PCI SSC. URL: https://www.pcisecuritystandards.org/ (дата звернення: 27.04.2024)

17. Офіційний сайт СК «АСКА». URL: https://aska.ua/ua/business-insurance/industry/cyber-insurance (дата звернення: 27.04.2024)

18. Офіційний сайт СК «УПСК». URL: https://upsk.com.ua/service/corporate/cyberriskua (дата звернення: 27.04.2024)

19. Офіційний сайт Центру обробки даних COSMONOVA|NET. URL: https://cosmonova.net/ua/page/open-new-cyber-ins (дата звернення: 27.04.2024)

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

21. Попович, Д., Бундз, Н., & Іванків, В. (2023). ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СТРАХУВАННЯ КІБЕРРИЗИКІВ НА НАЦІОНАЛЬНОМУ РИНКУ. *Молодий вчений*, 4 (116), 168-172. https://doi.org/10.32839/2304-5809/2023-4-116-33

22. Приказюк Н. В., Гуменюк Л. С. Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка.* 2020. № 4. DOI: 10.32702/2307-2105-2020.4.6

23. Приказюк Н. В., Гуменюк Л. С. Передумови розвитку кібер-страхування. Інвестиції: практика та досвід. 2020. № 15-16. С. 28-34. DOI: 10.32702/2306-6814.2020.15-16.28

24. Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами. НБУ. URL: https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami (дата звернення: 27.04.2024)

25. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. *Відомості Верховної Ради України (ВВР)*, 2006, № 30, ст.258

26. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. *Відомості Верховної Ради України (ВВР)*, 1994, № 31, ст.286

27. Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України (ВВР)*, 1992, № 48, ст.650.

28. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради (ВВР)*, 2018, № 31, ст.241

29. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради (ВВР)*, 2017, № 45, ст.403.

30. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України; Стратегія від 14.09.2020 № 392/2020

31. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України; Доктрина від 25.02.2017 № 47/2017

32. Про страхування: Закон України від 18.11.2021 № 1909-IX. *Відомості Верховної Ради України (ВВР)*, 2023, № 12-13, ст.28.

33. Прокоф'єва О.В., Беспалова Ю.Ю. Кібер-ризики та управління ними в умовах глобалізації та цифрової трансформації. *Інвестиції: практика та досвід.* 2024. №10.

34. Річні звіти Національної поліції України. URL: https://www.npu.gov.ua/diyalnist/zvitnist/richni-zviti (дата звернення: 27.04.2024)

35. Селіверстова Л. С., Трухан Д. А. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку. *Економіка та держава.* 2020. № 1. С. 23–26. DOI: 10.32702/2306-6806.2020.1.23

36. Сєдов Є. С. Деякі аспекти страхування кібер-ризиків / Є. С. Сєдов // Інноваційні напрямки розвитку страхового ринку України : зб. матеріалів III Міжнар. наук.-практ. конф. (19–20 квіт. 2016 р., м. Київ) / М-во освіти і науки

України, ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана» ; [редкол.: О. О. Гаманкова (голова) та ін.]. – Київ : КТ «Забєліна-Фільковська Т. С. і компанія Київська нотна фабрика», 2016. – С. 288–291. URL: https://ir.kneu.edu.ua:443/handle/2010/22228 (дата звернення: 27.04.2024)

37. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" від 26 серпня 2021 року № 447/2021". URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 27.04.2024)

38. Федорович І.М., Вегера С.І. Напрями розвитку кіберстрахування в Україні. *Євразійська наукова дискусія* : матеріали міжнар. наук.-практ. конф., м. Барселона, 2022. С. 520-523. URL: https://sci-conf.com.ua/wp-content/uploads/2022/11/EURASIAN-SCIENTIFICDISCUSSIONS-21-23.11.22.pdf#page=520 (дата звернення: 27.04.2024)

39. Шолойко А. С. Актуалізація кіберстрахування в умовах цифровізації економіки. *Науковий вісник Одеського національного економічного університету.* 2023, № 9 (310), с. 98-106. DOI: 10.32680/2409-9260-2023-9-310-98-106

40. 10 Biggest Cyber Attacks in History. Clear Insurance. 2021. URL: https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/ (дата звернення: 27.04.2024)

41. 2023 Cyberthreat Defense Report URL: https://www.humansecurity.com/hubfs/HUMAN_Report_2023-Cyberthreat-Defense-Report.pdf (дата звернення: 27.04.2024).

42. A new look at the Budapest Convention on Cybercrime. ICTLC Australia. 2024. URL: https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en (дата звернення: 27.04.2024)

43. A short history of the Web. URL: https://home.cern/science/computing/birth-web/short-history-web (дата звернення: 27.04.2024)

44. Allianz Risk Barometer 2024. Allianz Commercial. URL: https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf (дата звернення: 27.04.2024)

45. Badman A. Types of cyberthreats. 2023. URL: https://www.ibm.com/blog/types-of-cyberthreats/ (дата звернення: 27.04.2024)

46. Barry M. Cyber Insurance Market Growing Dramatically, Triple-I Finds. 2024. URL: https://www.iii.org/press-release/cyber-insurance-market-growing-dramatically-triple-i-finds-020724 (дата звернення: 27.04.2024)

47. Bohme R., Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework. *Conference.* 2020. URL: https://informationsecurity.uibk.ac.at/pdfs/BS2010_Modeling_Cyber-Insurance_WEIS.pdf (дата звернення 27.04.2024)

48. CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk. CRO Forum. June 2016. URL: https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web.pdf (дата звернення: 27.04.2024)

49. Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q3 July to September 2023. URL: https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf (дата звернення: 27.04.2024)

50. Cyber Insurance Market Research Report 2024. URL: https://www.insightaceanalytic.com/report/cyber-insurance-market/1634 (дата звернення: 27.04.2024)

51. Cyberattack on Ukraine's Kyivstar will cost parent Veon almost $100 mln in sales. Reuters. URL: https://www.reuters.com/business/media-telecom/cyberattack-on-ukraines-kyivstar-will-cost-parent-veon-almost-100-mln-sales-2024-01-18/ (дата звернення: 27.04.2024)

52. Cybersecurity Threats. Imperva Learning Center. URL: https://www.imperva.com/learn/application-security/cyber-security-threats/ (дата звернення 27.04.2024)

53. Cybersecurity Ventures Report on Cybercrime. ESentire. Managed detection and response glossary. URL: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime (дата звернення: 27.04.2024)

54. Darem, A.A., Alhashmi, A.A., Alkhaldi, T.M., Alashjaee, A.M., Alanazi, S.M., & Ebad, S.A.Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. *In IEEE Access*, vol. 11, pp. 125138-125158, 2023, doi: 10.1109/ACCESS.2023.3327016. URL: https://ieeexplore.ieee.org/abstract/document/10292652 (дата звернення: 27.04.2024)

55. Framework for Improving Critical Infrastructure Cybersecurity. URL: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf (дата звернення: 27.04.2024)

56. Global Conficker worm outbreak, millions of computers fallen. HKCERT. 2009. URL: https://www.hkcert.org/blog/global-conficker-worm-outbreak-millions-of-computers-fallen (дата звернення: 27.04.2024)

57. GlobalData, 2022. Cyber insurance industry. URL: https://www.globaldata.com/cyber-insurance-industry-exceed-20bn-2025- says-globaldata (дата звернення: 27.04.2024)

58. Goodman, M.D., Brenner, S.W. (2012). The Emerging Consensus on Criminal Conduct in Cyberspace. UCLA J.L. & Tech., No 3 // URL: www.lawtechjournal.com (дата звернення: 27.04.2024)

59. Internet Crime Report 2023. Federal Bureau of Investigation. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (дата звернення: 28.04.2024)

60. ISO 27001 standard – ISMS –Information Security Management System. URL: https://www.northgrc.com/resources/iso-27001 (дата звернення: 27.04.2024)

61. Mosaic Launches an Internet Revolution. URL: https://new.nsf.gov/news/mosaic-launches-internet-revolution (дата звернення: 27.04.2024)

62. Nathaniel Cole. 23 Eye-Opening Cybersecurity Insurance Statistics (2023). URL: https://networkassured.com/security/cybersecurity-insurance-statistics/ (дата звернення: 27.04.2024)

63. Saheed O., Sean M. SolarWinds hack explained: Everything you need to know. TechTarget. 2023. URL: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (дата звернення: 27.04.2024)

64. Second Additional Protocol to the Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence. European Union Agency for Criminal Justice Cooperation. 2024. URL: https://www.eurojust.europa.eu/publication/second-additional-protocol-budapest-convention-cybercrime-and-cross-border-access (дата звернення: 27.04.2024)

65. Statista (2024), “ Annual amount of monetary damage caused by reported cybercrime in the United States 2001-2022”. URL: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/ (дата звернення: 27.04.2024)

66. Statista (2024), “ Average cost of a data breach in the United States 2006-2023”. URL: https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/ (дата звернення: 27.04.2024)

67. The Melissa Virus. FBI Federal Bureau of Investigationurl. 2019. URL: https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519 (дата звернення: 27.04.2024)

68. Ulrik Franke, The cyber insurance market in Sweden, Computers & Security, Volume 68, 2017, Pages 130-144, ISSN 0167-4048,

https://doi.org/10.1016/j.cose.2017.04.010. URL: https://www.sciencedirect.com/science/article/pii/S0167404817300883) (дата звернення: 27.04.2024)

69. What happened in the colonial pipeline ransomware attack. WALLIX. URL: https://www.wallix.com/what-happened-in-the-colonial-pipeline-ransomware-attack-2/ (дата звернення: 27.04.2024)

70. What is NotPetya ransomware? URL: https://www.cloudflare.com/en-gb/learning/security/ransomware/petya-notpetya-ransomware/ (дата звернення: 27.04.2024)

71. What was the WannaCry ransomware attack. Cloudflare. URL: https://www.cloudflare.com/en-gb/learning/security/ransomware/wannacry-ransomware/ (дата звернення: 27.04.2024)

72. Wolff J. A Brief History of Cyberinsurance. 2022. A Brief History of Cyberinsurance. URL: https://slate.com/technology/2022/08/cyberinsurance-history-regulation.html (дата звернення: 27.04.2024)