Шифр «Весна»

«РОЗВИТОК КІБЕРСТРАХУВАННЯ: СВІТОВІ ТЕНДЕНЦІЇ ТА ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ»

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У сучасному світі цифрові технології стали основою для діяльності бізнесу, державних установ і фінансових організацій. Разом із цим стрімко зростає рівень кіберзагроз, що створює серйозні ризики для безперебійної роботи компаній та захисту конфіденційних даних. Хакерські атаки, витоки інформації, фінансове шахрайство та збої в ІТ-системах можуть спричинити значні фінансові втрати та репутаційні ризики. У відповідь на ці виклики, ринок кіберстрахування набуває все більшої актуальності, а його дослідження є необхідним для розуміння тенденцій, викликів та перспектив цього сегмента. Вивчення ринку кіберстрахування дозволяє оцінити попит на страхові продукти, дослідити сутність ключових загроз, з якими стикаються компанії, а також проаналізувати ефективність страхових механізмів у різних секторах економіки. З огляду на зростання кількості кібератак у світі та Україні, ринок кіберстрахування має значний потенціал для розвитку. Регулярний моніторинг стану справ на ринку стимулює впровадження інноваційних страхових рішень і забезпечує рівень цифрової безпеки загалом. Таким чином, дослідження ринку кіберстрахування є не лише актуальним, а й необхідним кроком для адаптації до сучасних викликів та ефективного управління кіберризиками.

Розвиток ринку кіберстрахування є актуальним напрямом досліджень як вітчизняних, так і зарубіжних науковців. В Україні значний вклад у вивчення цієї теми зробили такі дослідники, як Л. Бабенко, Н. Внукова, О. Гаманкова, О. Гудзь, С. Кучерівська, Г. Мамонова, Р. Пікус, Л. Позднякова, Н. Приказюк, Л. Селіверстова, О. Сергієнкова та ін. На міжнародному рівні теоретичні та практичні аспекти кіберстрахування активно досліджувались такими науковцями, як Дж. Арчі, С. Бренер, М. Гудмен, Дж. Фінкл та ін. Їхні роботи сприяють формуванню загальних підходів до оцінки кіберризиків та розробки ефективних страхових продуктів.

Метою наукової роботи є комплексний аналіз сучасного стану ринку кіберстрахування та перспектив його розвитку з урахуванням міжнародного досвіду та особливостей впровадження в Україні. Дослідження сфери спрямоване на визначення основних тенденцій у страхуванні кіберризиків, оцінку правових та організаційних аспектів його регулювання, а також на вирішення проблем й обґрунтування подальшого розвитку цього сегмента страхового ринку.

Відповідно до поставленої мети було визначено та виконано наступні завдання: проаналізувати теоретичні основи кіберстрахування; провести оцінку сучасного стану ринку кіберстрахування; дослідити міжнародний досвід у сфері кіберстрахування; виявити проблеми і перспективи розвитку кіберстрахування в Україні; сформувати рекомендації щодо вдосконалення ринку кіберстрахування.

Об’єктом дослідження є ринок кіберстрахування.

Предметом дослідження є теоретичні та практичні аспекти розвитку ринку кіберстрахування на національному та міжнародному рівнях, а також ключові виклики та напрями його вдосконалення.

Методи дослідження. У дослідженні теоретичних основ кіберстрахування було використано системний підхід, діалектичний метод пізнання, а також методи аналізу, синтезу та узагальнення. Для вивчення тенденцій сучасного стану ринку кіберстрахування, оцінки його проблем і перспектив розвитку застосовувались статистичні та емпіричні методи.

Інформаційна база дослідження. Дослідження ґрунтується на наукових роботах вітчизняних фахівців у сфері кіберстрахування, нормативно-правових актах, аналітичних матеріалах Національного банку України, страхових компаній, а також на даних міжнародних статистичних і рейтингових агентств, спеціалізованих інтернет-видань, зокрема Forinsurer. Додатковими джерелами інформації стали звітно-аналітичні дані міжнародних і національних фінансових організацій.

Наукова новизна роботи полягає в комплексній оцінці сучасних тенденцій розвитку кіберстрахування як актуального вектора страхового ринку. У роботі досліджуються новітні підходи до управління ризиками у сфері кібербезпеки, включаючи порівняльний аналіз міжнародного та національного досвіду за цим напрямом. Також, увага приділяється оцінці ефективності існуючих страхових продуктів, механізмів регулювання кіберстрахування на міжнародному рівні та перспективам адаптації цих підходів в Україні.

Обсяг і структура роботи. Наукова робота складається зі змісту, вступу, трьох розділів, висновків та списку використаних джерел. Основний текст роботи викладений на 29 сторінках. Робота містить список використаних джерел із 23 найменувань та додатки.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ РОЗВИТКУ КІБЕРСТРАХУВАННЯ

Сучасний світ дедалі більше залежить від інформаційних технологій та цифрових систем. Оцифрування бізнесу, зростання обсягів електронної комерції, поширення віддаленої роботи та розширення використання хмарних сервісів сприяють розвитку цифрової економіки. Водночас із цими позитивними змінами збільшується кількість і складність кіберзагроз, що можуть завдавати значних фінансових та репутаційних збитків компаніям й окремим особам. Розвиток глобальної економіки завдяки інтенсивному впровадженню інформаційно-комунікаційних технологій і систем зумовлює масштабну цифрову модернізацію різних сфер господарської діяльності. Однак, поряд із соціально-економічними вигодами такої трансформації, підприємницька діяльність зазнає значних кіберзагроз, які порушують стабільне функціонування інформаційної інфраструктури національної економіки. У відповідь на ці виклики з’явилася та активно розвивається сфера кіберстрахування.

Кіберстрахування – це вид страхування, який передбачає фінансовий захист від ризиків, пов’язаних із кібератаками, витоком даних, зломом інформаційних систем, шкідливим програмним забезпеченням та іншими кіберінцидентами [13]. Основна мета кіберстрахування – мінімізувати фінансові втрати організацій у разі зазнання кібератак та сприяти швидкому відновленню їхньої діяльності. Людство стає більш вразливим до кібератак, особливо в умовах активного впровадження новітніх технологій у повсякденне життя та бізнес-процеси. Будь-яка компанія, що володіє цифровими активами, може стати жертвою програм-вимагачів, зараження вірусним програмним забезпеченням, фішингу та інших форм кіберзлочинності. Наслідки таких атак, у тому числі витік конфіденційної інформації з серверів, можуть мати серйозні наслідки, які виходять далеко за межі прямих фінансових витрат на відновлення зламаних систем.

Кіберстрахування надає компанії фінансову підтримку для подолання наслідків, таких як значні збитки, допомагає зберегти фінансову стійкість та мінімізувати витрати, спричинені простоєм бізнесу через кіберзагрози.

З огляду на стрімке зростання масштабів кіберзлочинності, компаніям необхідно розширити ризик-менеджмент, включивши до нього загрози, яким раніше не надавали належної уваги. Це передбачає розробку заходів для підвищення рівня кібербезпеки, включаючи впровадження технологічного захисту, навчання персоналу щодо методів протидії кіберзлочинам та їхньої профілактики, а також застосування кіберстрахування [10].

Зростаючий інтерес бізнесу до механізмів фінансового захисту, особливо в умовах масових загроз, що охоплюють як Україну, так і світ загалом, робить кіберстрахування прибутковим інструментом у сфері страхових послуг. Відповідаючи на ці виклики, страхові компанії зосереджуються на розробці сучасних практик кіберстрахування, формуванні відповідних страхових продуктів та впровадженні дієвих механізмів компенсації втрат, спричинених кіберінцидентами.

Кіберстрахування – це відносно новий сегмент страхового ринку, який динамічно розвивається у відповідь на зростаючі загрози кіберзлочинності та цифрових ризиків. Його розвиток залежить від низки економічних, технологічних, правових та соціальних чинників. Одним із головних факторів є зростання кількості та складності кібератак. Кіберзлочинність постійно розвивається, зокрема через збільшення програм-вимагачів, які блокують доступ до даних підприємств і вимагають викупу, атак на критично важливу цифрову інфраструктуру, розробку нових фішингових схем, а також кібершпигунство. Усі ці загрози створюють значний ризик для бізнесу та державних установ, що спонукає компанії звертатися до страхових компаній за фінансовим захистом.

Другим чинником є активна цифрова трансформація бізнесу та державного сектора. Таким чином, перехід компаній на віддалену роботу створює ризики кібератаки через використання особистих пристроїв та

незахищених мереж, а впровадження хмарних технологій та Інтернету речей створює додаткові зони вразливості. Крім того, обсяг персональних даних, які обробляються компаніями, значно збільшується, що вимагає підвищеного рівня захисту від можливих витоків інформації.

Наявність та розвиток нормативно-правової бази також визначають вирішальну роль у розширеному ринку кіберстрахування. У різних країнах запроваджуються закони, які зобов'язують компанії забезпечувати достатній рівень захисту від існуючих загроз. Наприклад, європейський регламент GDPR (англ. General Data Protection Regulation) накладає великі штрафи за витік персональних даних, що стимулює бізнес до страхування відповідних ризиків. У США також діють жорсткі нормативні вимоги, як-от CCPA (англ. California Consumer Privacy Act), що регулює захист персональної інформації. В Україні, з огляду на зростання кіберзагрози, активно ведеться робота над законодавчими ініціативами для посилення кібербезпеки.

Одним із ключових факторів розвитку кіберстрахування є рівень обізнаності бізнесу щодо кіберризиків. Попри те, що масштабні атаки, такі як вірус Petya, звертають увагу на цю проблему, багато компаній все ще недооцінюють загрозу кібератак. Тому розширення страхових продуктів у цій сфері гальмується, оскільки компанії недостатньо зацікавлені у запровадженні страхового захисту від таких загроз.

Важливим аспектом є також стан страхового ринку та фінансової системи загалом. Для ефективного розвитку кіберстрахування необхідна адаптація страхових продуктів, враховуючи специфіку кіберризиків. Водночас, підписання єдиних стандартів оцінки ризиків ускладнює розрахунок тарифів та умов страхових полісів, що може призвести до надто високої ціни або низької прибутковості для страхових компаній.

Економічна та політична ситуація в країні також значною мірою впливає на розвиток кіберстрахування. У періоди економічних криз компанії скорочують витрати, зокрема на страхування, що може гальмувати розвиток цього ринку. Водночас у країнах, які перебувають у стані військових

конфліктів або політичної нестабільності, зростають ризики кібератак, що актуалізує потребу в додатковому страхуванні. У такому випадку кіберстрахування може стати елементом національної безпеки, особливо в умовах гібридних загроз.

Розвиток кіберстрахування залежить від багатьох взаємопов'язаних факторів, серед яких: зростаюча кіберзлочинність; цифрова трансформація бізнесу; розвиток законодавства; рівень обізнаності підприємців; стан фінансової системи та економічна стабільність. Усі ці аспекти впливають на швидкість впровадження страхових продуктів у сферу кібербезпеки. З огляду на зростання цифрової економіки та посилення кіберзагрози, попит на цей вид страхування збільшується, а його ефективність залежить від співпраці з державою, бізнесом та страховим сектором.

Інструментом активізації діяльності страхових компаній при страхуванні кіберризиків може бути, наприклад, проактивність, яка забезпечує не тільки компенсацію збитків, а й запобігання кібератакам шляхом впровадження профілактичних заходів, моніторингу загроз та аналізу виявлених вразливостей клієнтів. Важливим є навчання, що включає проведення освітніх програм для компаній-клієнтів, публікацію аналітичних звітів та організацію тестувань на стійкість до кібератак [6].

Співпраця для збирання даних є ще одним ключовим аспектом, що включає обмін інформацією між страховими компаніями та державними органами, а також доступ до бази даних про кібератаки. Для кращого прогнозування ризиків може бути застосоване використання штучного інтелекту. Орієнтованість на мікроклієнтів дозволяє адаптувати страхові продукти для малого бізнесу, включаючи страхові пакети з вбудованими послугами кібербезпеки та автоматизованим оцінюванням кіберризиків [6].

Крім того, ефективність страхування кіберризиків досягається завдяки інтеграції з кібербезпекою, що забезпечує надання клієнтам антивірусного програмного забезпечення та послуг реагування на інциденти. Використання штучного інтелекту та аналітики дозволяє точніше оцінювати ризики та

прогнозувати загрози, аналізуючи поведінку користувачів та оцінюючи рівень кіберстійкості клієнта на основі великих даних. Комплексний підхід до страхування кіберризиків, який включає проактивну політику, навчання, співпрацю в зборі даних та використання сучасних технологій, забезпечує не лише фінансовий захист клієнтів, а й мінімізацію самих ризиків.

Кіберстрахування виступає ефективним механізмом управління ризиками, допомагаючи компаніям і організаціям мінімізувати наслідки кібератак. Основними цілями кіберстрахування є не лише покриття фінансових збитків, а й створення комплексного підходу до кібербезпеки, що охоплює профілактику, реагування та відновлення після інцидентів. Відтак, основними завданнями кіберстрахування є:

- фінансовий захист від збитків, спричинених кіберзлочинністю. Кіберстрахування дозволяє компенсувати витрати та зменшити фінансовий удар для компанії;

- забезпечення безперервності бізнес-процесів. Страхові механізми дозволяють компанії швидко відновити свою діяльність після інциденту, компенсуючи витрати на усунення наслідків атак, відновлення інформаційних ресурсів та покриття збитків, викликаних простоєм;

- репутаційний захист і довіра клієнтів. Хакерська атака може суттєво підірвати довіру клієнтів і партнерів до компанії. Поліс кіберстрахування може покривати витрати на антикризові заходи, юридичну підтримку та комунікаційні стратегії з відновлення довіри;

- зниження загального рівня кіберризиків в економіці. Широке впровадження кіберстрахування сприяє формуванню культури кібербезпеки серед бізнесу. Це стимулює розвиток нових стандартів безпеки та забезпечує загальну стійкість економіки до кіберзагроз.

Протидія кіберзагрозам стає одним із ключових викликів для сучасного бізнесу, державних установ і приватних осіб. У відповідь на ці загрози кіберстрахування формується як важливий механізм фінансового захисту від негативних збитків, пов’язаних із витоком даних, збоєм у роботі інформаційних систем, шахрайством або іншими кіберінцидентами. В основі

ефективного страхового захисту лежать певні принципи, які визначають особливості управління ризиками, оцінку загроз і механізми компенсації. Саме ці принципи вирішують роль у формуванні стійкої системи кіберстрахування та забезпечують його дієвість у сучасному цифровому світі (рис. 1).

Рисунок 1 – **Принципи формування системи кіберстрахування**

Джерело: розроблено авторами з використанням [3]

Отже, кіберстрахування є невід’ємним елементом сучасної системи управління ризиками, що спрямоване на захист бізнесу, державних установ та окремих користувачів від фінансових втрат, спричинених кібератаками. Кіберстрахування на сьогодні виконує подвійну функцію: з одного боку забезпечує фінансовий захист, а з іншого – сприяє загальному підвищенню кіберстійкості компаній та організацій. Його подальший розвиток та адаптація до нових загроз є необхідними умовами стабільного функціонування цифрової економіки в глобальному масштабі.

РОЗДІЛ 2
СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРСТРАХУВАННЯ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

Ще донедавна кіберстрахування розглядалося як новаторське рішення. Однак сьогодні це стало актуальною тенденцією для бізнесу, оскільки пандемія суттєво прискорила цифрову еволюцію, а разом із нею значно розрослися й кіберзагрози. Вони здійснюються як через активне впровадження Інтернет-речей, зокрема на виробничих підприємствах, так і через підвищення значущості так званих «нематеріальних активів» - об'єктів інтелектуальної власності.

У 2020 році кіберзлочинність завдала світовій економіці збитків на суму понад 820 мільярдів євро. На цьому тлі кіберстрахування перетворюється на важливий інструмент мінімізації фінансових втрат від подібних атак. Україна також активно залучена в ці процеси. Завдяки глибокій інтеграції у світову економіку попит на кіберстрахові поліси в країні з’явився і набирає обертів значно швидше, ніж це можна було прогнозувати [7].

З кожним роком хакерські атаки стають дедалі складнішими та завдають все більшого збитку не лише фінансовим установам і державним органам, а й звичайним громадянам. Необхідно підкреслити критичну важливість розробки та впровадження ефективних механізмів кібербезпеки, міжнародного співробітництва в цій сфері та підвищення рівня цифрової грамотності серед населення.

У сучасному цифровому середовищі кіберзагрози стали серйозною проблемою для економічної та національної безпеки України. За останнє десятиліття країна відзначила низку потужних хакерських атак, які спричинили значні фінансові збитки, дестабілізацію роботи державних установ та підприємств, а також порушення критично важливих процесів. Вплив цих атак відчули як державний сектор, так і бізнес, що підкреслює необхідність посилення заходів кіберзахисту. Наведена таблиця узагальнює

найбільш значущі кібератаки, які мали суттєвий негативний вплив на українську економіку.

Таблиця 2.1 **Найбільші кібератаки на українську економіку, 2014-2022 рр.**

Роки	Тип кібератаки	Наслідки та вплив на економіку
2014	DDoS-атака на Центральну виборчу комісію	Злом офіційного сайту ЦВК під час президентських виборів, що могло вплинути на довіру до виборчого процесу та стабільність політичної ситуації.
2015	Кібератака на об'єкти критичної інфраструктури	Порушення роботи об'єктів критичної інфраструктури в Києві, Чернівцях та на Прикарпатті.
2016	Вторгнення до державних фінансових систем	Атака на інформаційні системи Державної казначейської служби, Пенсійного фонду та Міністерства фінансів, що могло призвести до збою у фінансових операціях та розподілі бюджетних коштів.
2017	Атака вірусами Petya, NotPetya	Масштабне порушення роботи державних і приватних установ, фінансових організацій, банків, медіа та мобільних операторів. Втрати від атаки вірусу Petya оцінили в 0,4-0,5% річного ВВП України.
2022	Масована атака на урядові сайти вірусом October CMS	Знищення MBR та вмісту файлів на державних серверах, що призвело до значних порушень у функціонуванні урядових веб-ресурсів.

Джерело: побудовано з використанням [13]

У грудні 2024 року Україна зіткнулася з безпрецедентною за масштабами кібератакою, яка паралізувала роботу ключових державних реєстрів. Міністерка юстиції України Ольга Стефанішина повідомила, що це була найсерйозніша зовнішня атака за останній час, що спричинила призупинення функціонування Єдиних та Державних реєстрів Міністерства юстиції. Через цю атаку суттєво постраждала робота багатьох державних систем, які взаємодіють із реєстрами. Громадяни та бізнес втратили доступ до послуг, що потребують перевірки особистих даних, зокрема було зупинено роботу електронного нотаріату. Як зазначила президентка Асоціації фахівців з нерухомості Олена Гайдамаха, призупинилися операції, пов'язані з реєстрацією юридичних осіб та підприємців, а також із

реєстрацією прав на нерухомість, що унеможливило проведення операцій із нерухомістю. Частково порушено роботу порталу «Дія» - початкові повідомлення про оновлення реєстрів пізніше змінилися на інформацію про їх відновлення [16].

Відразу після атаки Верховна Рада створила спеціальну робочу групу для розслідування інциденту. Під час «години запитань до уряду» прем'єр-міністр Денис Шмигаль запевнив, що систему «Дія» вдалося вчасно відключити від реєстрів, що допомогло уникнути її компрометації. Однак через атаку тимчасово вийшли з ладу реєстри, пов'язані з національними інформаційними системами.

Кібератака на державні реєстри стала серйозним викликом для кібербезпеки країни. Влада та силові структури активно працюють над зміцненням захисту критичної інфраструктури, щоб запобігти подібним інцидентам у майбутньому. Відтак, все більшої актуальності набуває страховий захист від кіберризиків.

Страховий поліс передбачає відшкодування фінансових втрат, спричинених кібератаками, несанкціонованим доступом, вимаганням або крадіжкою конфіденційної інформації. Також покриваються збитки, пов'язані з перервою у функціонуванні бізнесу та зменшенням доходів унаслідок кібератаки, а також відповідальність компанії перед клієнтами або партнерами у разі неналежного захисту даних. Крім того, розширене страхове покриття може включати аудит кібербезпеки після інциденту, витрати на розслідування причин атаки та заходи зі збереження ділової репутації. Комплексна програма страхування від кіберзагроз та цифрових ризиків дає змогу мінімізувати можливість фінансових втрат через знищення, викрадення або компрометацію корпоративної чи клієнтської інформації. Вона також допомагає швидкому відновленню бізнесу після кризи, викликаної кібератаками. Кіберстрахування поділяється на два основних типи: захист компанії як постраждалої сторони («страхування першої особи»

– A, F, E) та страхування відповідальності перед іншими особами («страхування третіх осіб» – B, C, D) [15].

Національний банк України запропонував для громадського обговорення проєкт Положення, що регулює організацію заходів із кіберзахисту та забезпечення інформаційної безпеки для постачальників фінансових послуг. Це дозволить посилити надійність і стабільність небанківського фінансового сектора, особливо в умовах воєнного стану.

Основна мета ініціативи – підвищення рівня кіберзахисту та інформаційної безпеки серед страхових компаній, кредитних спілок, фінансових установ та ломбардів. Ці заходи НБУ передбачають:

- розробку та впровадження механізмів управління кіберризиками;

- визначення ключових заходів щодо забезпечення інформаційної безпеки;

- впорядкування процесу реагування на кіберінциденти;

- встановлення правил контролю за доступом до інформаційних та комунікаційних систем фінансових установ [8].

Фінансові установи мають можливість виконувати ці вимоги в межах своєї операційної діяльності, без додаткового фінансового навантаження на регулятора. Обсяг витрат на реалізацію заходів залежить від рішень самих компаній – вони можуть використовувати наявну інфраструктуру або інвестувати в сучасні технології для підвищення рівня кібербезпеки.

Останнім часом програми-вимагачі набули значного поширення, тоді як шахрайство з фінансовими переказами (FTF) дещо втратило актуальність. Частота таких звернень скоротилася на 2%, а масові збитки зменшилися на 15 відсотків. Водночас, однією з ключових тенденцій кібербезпеки, стало зростання страхових виплат за шкоду, завдану програмами-вимагачами, – на 68 відсотків. Середній збиток у таких випадках зріс до 353 тис. дол, що свідчить про серйозний фінансовий тягар для компаній та страхових організацій [3].

Яскравим прикладом руйнівного впливу атак кіберзлочинців є атака на компанію Change Healthcare, яка у 2024 році призвела до масштабних збоїв у сфері охорони здоров’я. Через цю кібератаку значна частина медичних установ виявила проблему з обробкою медичних вимог. У США понад 90% аптек постраждали від цієї атаки, а загальні втрати склали 1,6 млрд дол Аналогічна ситуація сталася з CDK Global – постачальником програмного забезпечення для автодилерів, що спричинило зупинку роботи 15 тисяч автосалонів та фінансові збитки в 1 млрд доларів. Атака на Change Healthcare суттєво позначилася на великих медичних компаніях: 23% організацій із доходом понад 100 млн дол відчули її негативні наслідки, а серед компаній із доходом від 25 до 100 млн дол постраждало 11 відсотків. У сфері автомобільного бізнесу 75% автодилерів із доходом понад 100 млн дол також відзначили серйозні втрати через кібератаку на CDK Global [3].

Кіберзагрози в медичному секторі також продовжують наростати. Відповідно до звіту Beinsure, щорічно в галузі фіксується близько 133 мільйонів випадків звернення щодо витоку даних, що робить охорону здоров'я одним із найбільш уразливих секторів [3].

Рівень збитковості компаній із доходом понад 100 млн дол зріс на 140%, а середній розмір втрат досягає історичного максимуму в 307 тис. доларів. Основним чинником цього зростання стало поширення програм-вимагачів, хоча майже третина страхових звернень стосувалася компрометації бізнесових електронних листів (BEC). У відповідь на такі виклики страхові компанії впроваджують ефективні механізми роботи з клієнтами, зокрема: розробляють стратегії мінімізації операційних ризиків; впроваджують альтернативні методи реагування на загрози та допомагають зменшити фінансові втрати [3].

У 2024 р. групи кіберзлочинців, що розробляють програми-вимагачі, зосередилися на максимізації прибутку. Хоча частота атак трохи знизилася з 0,31% до 0,28%, загальна сума втрат зросла на 68%, досягнувши середнього показника в 353 тис. доларів. У 2023 р. цей показник тимчасово знизився із

402 тис. дол до 239 тис. дол, проте вже в першій половині 2024 р. зловмисники відновили активність. При загальній тенденції до посилення кібербезпеки середні вимоги викупу з боку хакерів зросли на 1% і досягли 1,3 млн доларів. У тих випадках, коли компаніям доводилося сплачувати викуп, страхові компанії намагалися зменшити його розмір, в середньому це вдавалося на 57 відсотків [3].

До 2019 р. зростання ринкових премій значною мірою було зумовлено розширенням страхового покриття в Північній Америці та Європі, після чого більше компаній уклали угоди про кіберстрахування. Однак у період з 2020 р. по 2022 р. основний фактор розвитку ринку зазнав суттєвих змін. Так, сплеск атак із використанням програм-вимагачів спричинив значні фінансові втрати, що змусило страховий сектор реагувати підвищенням тарифів для врахування зростаючих ризиків (додаток А).

У сфері страхування в Україні діють компанії, які надають різноманітні послуги для забезпечення фінансової безпеки клієнтів. Крім того, інфраструктуру для обробки даних забезпечують сучасні дата-центри. Наприклад, MO Group спеціалізується на забезпеченні інформаційної безпеки та кіберзахисту. Компанія пропонує послуги кіберстрахування, які покривають прямі збитки від кібератак. MO Group є сертифікованим партнером таких брендів, як Sophos, Forcepoint і Splunk, що підтверджує її компетентність у сфері кібербезпеки [4]. Компанія «Експерт» є провідним українським страховим брокером з понад 20-річним досвідом. Вона надає консультації та допомогу в підборі оптимальних страхових продуктів від найкращих страхових компаній. Компанія прагне забезпечити надійний страховий захист та індивідуальний підхід до кожного клієнта [5].

COSMONOVA – це сучасний дата-центр, який відповідає сучасним стандартам безпеки, надійності та масштабованості. Він пропонує хмарні рішення в Україні та Європі [9].

Ці компанії роблять вагомий внесок у розвиток страхового ринку та інфраструктури обробки даних в Україні, забезпечуючи клієнтам широкий

спектр послуг для їхньої фінансової та інформаційної безпеки. Зважаючи на зростання кіберзагроз, очікується, що кількість страхових компаній, які пропонують послуги кіберстрахування в Україні, буде збільшуватися. Водночас, підприємства прагнуть оцінювати умови страхових полісів та обирати ті, які найбільше відповідають їхнім потребам у сфері кібербезпеки вже зараз. В табл. 2.2. наведено класифікацію кіберризиків та основні українські страхові компанії, які займаються покриттям таких ризиків.

Таблиця 2.2 **Види покриття вітчизняними страховими компаніями витрат від кіберризиків**

Класифікація кіберризиків	Страхові компанії (посередники)			
	VUSO	УПСК	Aon	ІНГО
Витрати, пов'язані з реагуванням на кіберінцидент	+	+	+	+
Адміністративне розслідування відносно втрати даних	-	+	+	-
Збитки, пов'язані з порушенням бази даних	+	+	+	+
Відповідальність за контент інформації	+	+	+	+
Соціальна інженерія	+	+	+	-
Перерва в процесі виробництва	+	+	+	+
Віртуальне вимагання	+	+	+	+

Джерело: побудовано з використанням даних [18, 19, 20, 21]

Таким чином, кіберзагрози в сучасних умовах продовжують розвиватися, стимулюючи як суб'єкти господарювання, так і страхові компанії вдосконалювати свої підходи до управління ризиками та посилювати заходи безпеки. Кіберстрахування набуває все більшого значення, оскільки допомагає не лише компенсувати фінансові втрати, а й стимулює бізнес до впровадження проактивних заходів захисту.

Відзначимо, що глобальний ринок кіберстрахування переживає період значних змін, що супроводжуються зростанням конкуренції та трансформацією ризик-профілів. Згідно зі звітом компанії Amwins, спостерігається зміщення динаміки ринку, яке впливає на тарифи, страхові

ліміти та стратегії учасників ринку. Однією з ключових тенденцій є стабілізація або навіть зниження тарифів на продовженні договори кіберстрахування. Водночас до нових клієнтів можуть активно застосовуватись агресивні цінові стратегії, оскільки страхові компанії намагаються збільшити свою частку ринку. Такий підхід сприяє зростанню конкуренції серед компаній, які розділяються на три основні групи:

1. Нові учасники ринку. До неї належать страховики, які не мають великого досвіду та історії ризиків, пропонують значно нижчі ціни, щоб швидко залучити клієнтів.

2. Досвідчені компанії. До цієї групи входять страховики, що працюють понад 10 років, використовують власні портфелі клієнтів та перевірені методи управління ризиками, щоб залишатися конкурентоспроможними.

3. Страховики середнього рівня. Ці учасники ринку прагнуть чітко окреслити свої пропозиції, часто спеціалізуючись на певних сегментах ринку та впроваджуючи унікальні стратегії розповсюдження страхових послуг [2].

Ще одним важливим фактором, що формує сучасний ринок кіберстрахування, є поява нових гравців та трансформація структури ризиків. Незважаючи на те, що більшість страховиків готові працювати з кіберризиками у різних галузях, існують сектори, які викликають підвищену обережність. Зокрема, сфера охорони здоров’я стикається з регуляторними викликами, що ускладнюють процес андеррайтингу [2].

Поряд з цим, відзначимо, що попри постійну загрозу атак програм-вимагачів, ринок поки що не реагує на цей ризик у повній мірі. Проте вдосконалення протоколів кібербезпеки серед страхувальників сприяє зниженню потенційних фінансових втрат і може вплинути на зміну умов страхування в майбутньому. На рис. 2 наведено основні види кіберризиків, які турбують більшість компаній в сучасних умовах.

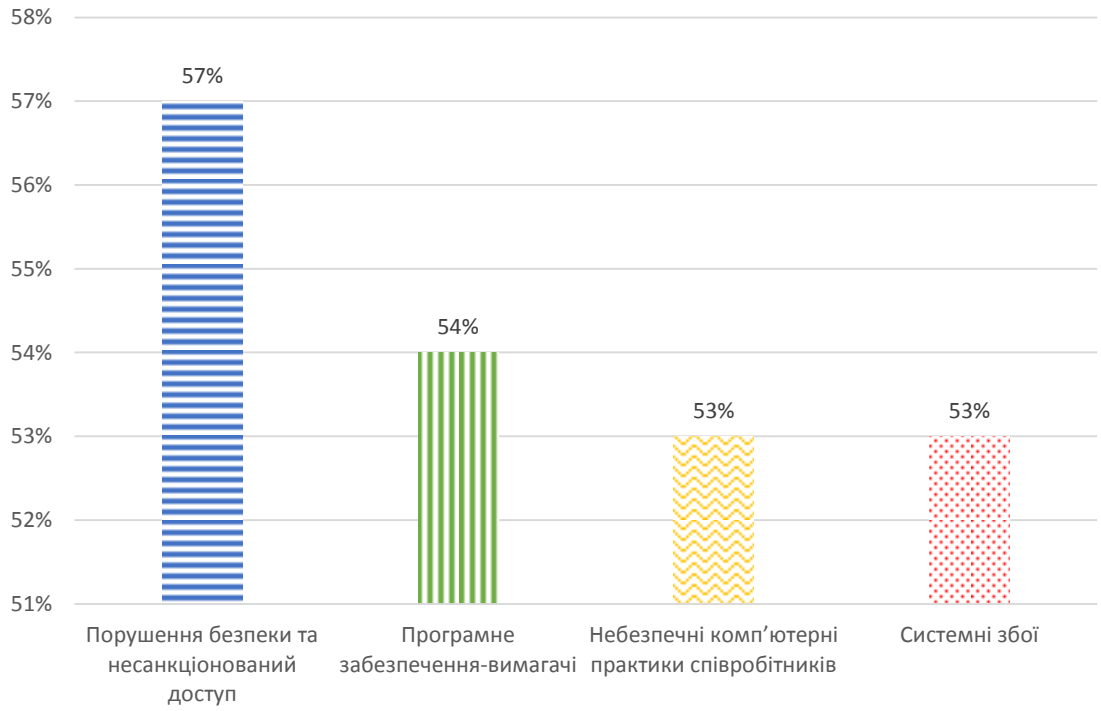

Рисунок 2 – **Перелік кіберризиків, які є основною проблемою світових компаній у 2024 році**

Джерело: побудовано з використанням [23]

Отже, ринок кіберстрахування на сьогодні перебуває в активній фазі розвитку, що супроводжується конкурентною боротьбою, переглядом тарифної політики та адаптацією до нових викликів. Компанії, які впроваджують ефективні заходи з управління ризиками, можуть не лише отримати більш вигідні умови страхування, а й підвищити загальний рівень кіберзахисту.

РОЗДІЛ 3
ПЕРСПЕКТИВИ ТА НАПРЯМИ УДОСКОНАЛЕННЯ СИСТЕМИ КІБЕРСТРАХУВАННЯ В УКРАЇНІ

Сучасні дослідження глобальних ризиків підприємств і фінансового сектора свідчать, що збитки світової економіки від кібератак щороку зростають. Ця негативна тенденція дедалі частіше змушує керівництво компаній замислюватися над важливістю страхування кіберризиків. Так, за даними страхової групи Allianz [1], ринок кіберстрахування зростає щороку на 25-50 відсотків.

Від атак хакерів страждають передусім не пересічні користувачі, а великий бізнес, який зазнає значних фінансових втрат. Найбільший інтерес для кіберзлочинців становлять фінансово-кредитні установи, зокрема банки, що активно застосовують сучасні ІТ-технології, а також реєстроутримувачі цінних паперів. Зокрема, кількість незаконних дій з платіжними картками, за якими були понесені збитки, протягом 2024 року зросла на чверть в порівнянні з минулим роком та становила 272 тис доларів [11] .

Через такі втручання в банківську систему інститут банківської таємниці стає більш вразливим, що спричиняє втрату ділової репутації фінансових установ та зниження довіри як фізичних, так і юридичних осіб до фінансової системи країни в цілому. Однією з ключових проблем у взаємодії банків і страхових компаній в контексті мінімізації наслідків кіберзлочинності є недостатня фінансова грамотність населення щодо захисту своїх банківських рахунків та можливостей страхування кіберризиків. У разі впровадження відповідних механізмів страхові виплати могли б покрити значну частину втрат відповідно до умов договору. Це вказує на необхідність створення спільних інформаційно-просвітницьких платформ. Страхові компанії повинні розробляти спільні ініціативи та координувати програми, включно зі створенням єдиних баз даних про кіберзагрози та кіберризики, що сприяють активному залученню підприємств та установ до заходів з управління

ризиками. Не менш важливим є впровадження сертифікованого програмного забезпечення для кіберзахисту, ефективність якого доведена на практиці.

Такий підхід вже довів свою ефективність у інших сферах страхування, зокрема в галузі охорони здоров'я, автострахування та пожежної безпеки, де застосування превентивних заходів дозволило значно знизити рівень страхових випадків та фінансових втрат. Це дозволить клієнтам легко визначити, з якими банками співпрацюють страхові компанії та які послуги у сфері кіберстрахування вони пропонують.

Українське законодавство також відіграє значну роль у посиленні цієї галузі страхування та захисту бізнесу і громадян від кіберзагроз. В Україні набув чинності закон «Про основні засади забезпечення кібербезпеки України» у травні 2018 року [12], а Державний центр реагування на кіберзагрози був створений у лютому 2018 року. Проте, як великий так і малий бізнес потребує посилення захисту від кіберзлочинців та впевненості, що якщо станеться витік інформації через кібератаку, його збитки покриють та цей механізм буде захищений законодавством. Тому в Україні слід визначити чіткі правові основи кіберстрахування, обов’язки страхових компаній і страхувальників та імплементувати міжнародні стандарти у цій сфері, такі як NIS2 (Network and Information Security Directive) та ISO 27001.

Також для підвищення активності суб’єктів господарювання пропонуємо ввести додаткові податкові пільги компаніям, які застрахують свої кіберризики та впровадити такі самі стимули для страхових компаній, що розробляють нові страхові продукти у сфері кібербезпеки.

Враховуючи сучасні тенденції, коли Україна перебуває в умовах воєнного стану, уряд має впровадити обов’язкове страхування в оборонному секторі економіки для державних та фінансових установ (купівлю полісів кіберстрахування), які відповідають мінімальним стандартам. При цьому уряд повинен гарантувати, що політика, якої дотримуються підприємства, сприяє впровадженню передових практик кібербезпеки. Зокрема, страхові програми мають передбачати достатній рівень покриття та широкий спектр

дії, визначений на основі аналізу прогнозованих витрат, пов’язаних із кібератаками.

Крім того, механізм оцінки страхових премій повинен бути спрямований на стимулювання компаній до впровадження заходів, що мінімізують кіберризики, особливо у державному та фінансовому секторах. Запровадження таких удосконалених страхових політик може стати орієнтиром для компаній приватного сектору, мотивуючи їх розглянути можливість придбання полісів кіберстрахування, якщо вони раніше не зверталися за цими послугами.

На сьогодні більшість страхових компаній України не пропонують спеціалізованих полісів кіберстрахування, а наявні пропозиції є обмеженими за покриттям [6]. Тому, на нашу думку, доцільно запровадити такі нові продукти:

1. Персональне кіберстрахування для фізичних осіб, що покриватиме втрати від шахрайства в онлайн-банкінгу, крадіжки персональних даних, незаконного використання банківських карток тощо.

2. Кіберстрахування для малого та середнього бізнесу – з адаптованими умовами покриття, яке включатиме захист від атак на веб-сайти, втрати прибутку через збої в системах, відшкодування витрат на відновлення даних.

3. Кіберстрахування корпоративних клієнтів для великих підприємств, що охоплюватиме втрати через хакерські атаки, витік комерційної інформації, судові витрати у разі відповідальності перед клієнтами за порушення захисту персональних даних.

4. Страхування відповідальності за витік даних (Cyber Liability Insurance) – покриття штрафів, судових витрат та інших фінансових наслідків, якщо компанія допустила витік або незаконне використання даних своїх клієнтів.

5. Страхування бізнесу від кібератак (Cyber Business Interruption Insurance) – компенсація втрат компаній через простої внаслідок кібератак або збоїв у ІТ-системах.

Одним із перспективних напрямів розвитку є створення комплексних страхових продуктів, що поєднують кіберстрахування з іншими видами страхування. Наприклад:

- поєднання кіберстрахування з майновим страхуванням – для захисту не лише від фізичних загроз (пожеж, крадіжок), але й від цифрових атак, які можуть вплинути на бізнес;
- комбінація кіберстрахування зі страхуванням відповідальності – забезпечить покриття втрат через претензії з боку клієнтів, чиї дані були скомпрометовані;
- кіберстрахування як додаткова послуга при банківському обслуговуванні – наприклад, страхування онлайн-транзакцій або банківських рахунків від кібератак.

Вважаємо, що такі продукти дадуть можливість підприємствам та фізичним особам отримувати надійний захист без значного збільшення вартості страхових полісів.

Відзначимо, що деякі страхові компанії вже впроваджують подібний підхід, коли поліс кіберстрахування включається до комплексних страхових продуктів для банків та фінансових установ у вигляді доповнення до полісу страхування від кримінальних ризиків банку [17]. Щоб мінімізувати або уникнути фінансових втрат банківських установ через кіберзлочинність, у багатьох країнах були розроблені спеціалізовані страхові продукти. Серед них виділено страхування від комп’ютерних злочинів (CCI – Computer Crime Insurance) та страхування від хакерських атак (HI – Hacker Insurance).

Основна суть цих страхових продуктів полягає у відшкодуванні збитків банку, що виникли внаслідок несанкціонованого доступу до комп’ютерних та комунікаційних систем фінансової установи, введення неправомірних даних або команд, а також знищення інформації та програмного забезпечення через віруси. У міжнародній практиці ризики, пов’язані з комп’ютерними злочинами та хакерськими атаками, обов’язково покриваються як додатковий

елемент до основного полісу комплексного страхування банків – BBB (Banker’s Blanket Bond) [14].

Головною особливістю страхових полісів Computer Crime Insurance та Hacker Insurance є те, що у разі виникнення страхового випадку страхова компанія компенсує не тільки фінансові втрати банку, а й збитки, завдані третім особам, зокрема клієнтам банківської установи. Таким чином, саме кіберстрахування у банківському секторі має значний потенціал для розвитку, оскільки воно базується на передових міжнародних практиках, ефективних підходах та перевірених методах страхового захисту.

Для ефективного управління кіберризиками пропонуємо визначити єдині критерії їх оцінки та впровадити стандартизовані методики аналізу. Для цього потрібно здійснити:

- класифікацію кіберзагроз – поділ ризиків на категорії (зловмисні атаки, витік даних, внутрішні загрози, технічні збої тощо);
- аналіз статистичних даних – оцінка частоти та масштабу попередніх кібератак у конкретній галузі чи компанії;
- аудит інформаційної безпеки підприємств – перевірка рівня кіберзахисту, наявності системи моніторингу та реагування на інциденти;
- розрахунок потенційних фінансових збитків – прогнозування можливих втрат у разі реалізації кіберзагроз.

З цією мето варто адаптувати міжнародні стандарти оцінки кіберризиків, зокрема:

1. ISO/IEC 27001 – система управління інформаційною безпекою;
2. NIST Cybersecurity Framework – підхід до управління кіберризиками;
3. FAIR (Factor Analysis of Information Risk) – модель аналізу ризиків, що дозволяє визначити ймовірність та фінансові наслідки кіберзагроз.

Одним із ефективних інструментів для оцінки кіберризиків є створення системи рейтингів кіберстійкості, яка дозволить страховим компаніям визначати рівень ризикованості клієнта та відповідно формувати страхові тарифи. Для формування рейтингу кіберстійкості слід врахувати:

1. Аналіз IT-інфраструктури – оцінка захищеності серверів, мережевих протоколів, систем резервного копіювання та оновлення програмного забезпечення.

2. Оцінка політики кібербезпеки – перевірка наявності заходів щодо запобігання витоку даних, інструкцій для персоналу, програм навчання кібергігієни.

3. Моніторинг активності в кіберпросторі – аналіз випадків атак на компанію, пошук викрадених даних у «темному вебі», відстеження можливих вразливостей.

4. Сканування на предмет вразливостей – використання спеціалізованого програмного забезпечення для виявлення слабких місць в IT-системах підприємства.

На основі цих показників кожна компанія отримуватиме рівень кіберризику.

Крім того, страховим компаніям слід більше уваги звертати на свою маркетингову кампанію про кіберстрахування. Адже, низький попит на ці продукти через високу вартість, потрібно обґрунтовувати на реальних прикладах і більш детально пояснювати клієнтам яких збитків вони можуть зазнати без покриття страховим захистом. Інша проблема проведення маркетингових заходів полягає в тому, що компанії не зацікавлені надавати доступ до своїх баз даних та інформаційних систем, а клієнти повинні бути впевненими, що їх дані будуть надійно захищені і не станеться їх витоку. Страхові компанії в Україні майже не проводять маркетингову кампанію в засобах масової інформації та соціальних мережах та віддають більшу перевагу B2B сегменту, хоча багато громадян зазнають втрат від кіберзлочинності.

Однією з ключових особливостей кіберстрахування є те, що попит на нього формується здебільшого у відповідь на зростання кіберзагроз або вже після того, як компанія зазнала кібератаки. Це відрізняє кіберстрахування від

традиційних видів страхового захисту, де страхування часто є превентивним заходом.

Пропозиція страхових продуктів у цій сфері значною мірою залежатиме від низки факторів: індивідуальних особливостей виникнення кіберінцидентів у страхувальників; вартості страхових послуг та рівня платоспроможності підприємств; рівня прибутковості страхових компаній, що визначає їхню готовність брати на себе подібні ризики; розміру потенційних страхових виплат у разі реалізації кіберризиків; можливості укладати договори страхування в режимі онлайн, що спрощує доступ до страхових послуг та розширює охоплення ринку.

З огляду на стрімкий розвиток цифрових технологій та збільшення кількості кіберзагроз, страхування кіберризиків перетворюється на невід'ємний елемент ризик-менеджменту для підприємств будь-якої форми власності – як державних, так і приватних. На сьогодні, це не лише ефективний спосіб фінансового захисту, а й дієвий механізм підвищення загального рівня кібербезпеки компаній.

Відтак, на сьогодні постає необхідність у розробці стратегії розвитку кіберстрахування в Україні. Зазначена стратегія представлена нами як комплекс узгоджених дій та заходів, поетапність запровадження яких сприятиме збалансованому розвитку страхових послуг з кіберстрахування в умовах глобалізації та цифровізації економіки (додаток Б).

Таким чином, розширення кіберстрахування як страхового продукту відкриває нові перспективи для розвитку страхового бізнесу. Впровадження страхових програм, спрямованих не лише на компенсацію збитків, а й на превентивний захист від кібератак, дозволяє значно знизити ризики, зменшити фінансові втрати та запобігти потенційному припиненню або знищенню бізнесу. Відтак, кіберстрахування стає стратегічно важливим елементом фінансової та інформаційної безпеки, який забезпечує стійкість підприємств до кіберзагроз та сприяє стабільному розвитку економіки в умовах цифрової трансформації.

ВИСНОВКИ

У ході дослідження проблематики розвитку кіберстрахування було здійснено комплексний аналіз його теоретичних засад, поточного стану та перспектив удосконалення механізмів страхового захисту від кіберризиків в Україні.

Дослідження показало, що кіберстрахування є відносно новим напрямом страхування, але разом з тим стратегічно важливим елементом, спрямованим на фінансовий захист від цифрових загроз. Його розвиток зумовлений стрімкою цифровізацією бізнесу, зростанням кількості кіберінцидентів та посиленням нормативних вимог до захисту інформації. Визначено, що основними об'єктами страхового захисту є фінансові втрати від кібератак, порушення конфіденційності даних, збої в роботі IT-системи та репутаційні ризики компаній. В умовах активного розвитку цифрової економіки та посилення кіберзагроз попит на кіберстрахування зростає, а його ефективність значною мірою залежить від тісної взаємодії держави, бізнесу та страхового сектору.

Одним із ключових інструментів активізації діяльності страхових компаній у сфері кіберстрахування може стати проактивний підхід. Він забезпечує не лише відшкодування збитків, але й запобігання кібератакам завдяки впровадженню профілактичних заходів, постійному моніторингу загроз та аналізу вразливостей клієнтів.

Аналіз українського ринку кіберстрахування засвідчив його недостатню розвиненість, що пов'язано з низьким рівнем проінформованості підприємств про переваги страхового покриття, відсутністю стандартів оцінки кіберризиків та обмеженістю вибору відповідних страхових продуктів. Водночас, окремі українські страхові компанії починають впроваджувати програми кіберстрахування, здебільшого адаптуючи міжнародний досвід. У розвинених країнах кіберстрахування є інструментом фінансового захисту, і його ринок динамічно зростає.

У сучасному цифровому просторі кіберзагрози становлять серйозний виклик для економічної та національної безпеки України. Протягом останнього десятиліття було відзначено низку масштабних хакерських атак, які призвели до значних фінансових втрат, порушення роботи державних установ і підприємств, а також дестабілізації критично важливих процесів. Вплив цих атак відчули як державний сектор, так і бізнес, що свідчить про нагальну потребу у зміцненні системи кіберзахисту.

Обґрунтовано, що розвиток кіберстрахування в Україні потребує комплексного підходу, який сприятиме вдосконаленню нормативно-правового регулювання, розробці ефективних механізмів оцінки та управління кіберризиками, а також створення стимулів для впровадження політики кібербезпеки. Важливим аспектом є активізація міжнародної співпраці, що дозволяє адаптувати найкращі світові практики та інтегрувати український ринок у глобальну систему кіберстрахування. Усе це сприятиме формуванню ефективного страхового середовища, здатного забезпечити фінансовий захист від цифрових загроз. Завдяки впровадженню комплексних страхових рішень суб’єкти господарювання матимуть змогу підвищити рівень своєї кібербезпеки, зменшити кількість фінансових втрат та створити більш стабільну й прогнозовану систему управління ризиками. Водночас активна підтримка з боку держави та бізнес-спільноти стане ключовим чинником для успішного розвитку такого сектору страхування як кіберстрахування в Україні.

Таким чином, розвиток кіберстрахування в Україні є необхідною умовою для зміцнення фінансової безпеки бізнесу та держави в умовах зростаючих кіберзагроз. Формування ефективного страхового ринку потребує вдосконалення законодавчої бази, впровадження міжнародного досвіду та активної взаємодії між державою, страховими компаніями та підприємствами. Комплексний підхід до управління кіберризиками, а також впровадження запропонованої стратегії, дозволять мінімізувати фінансові втрати та підвищити рівень кібербезпеки в країні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Барометр ризиків. Allianz назвав глобальні ризики підприємств і фінансового сектора на 2019 рік. URL: https://forinsurer.com/news.

2. Вартість кіберстрахування може знизитися на 5% через зростання конкуренції - прогноз на 2025 рік. *FORINSURER* (*журнал про страхування, перестрахування та InsurTech*). URL: https://forinsurer.com/news/25/01/21/44597/

3. Збитки страховиків від програм-вимагачів зросли на 68%, середній кіберзбиток $353 тис. *FORINSURER* (*журнал про страхування, перестрахування та InsurTech*). URL: https://forinsurer.com/news/24/11/28/44444.

4. Кіберстрахування. Офіційний сайт компанії «MO Group» (2025). URL: https://www.mogroup.com.ua/?p=873.

5. Кіберстрахування. Офіційний сайт ТОВ «Компанія СБ «Експерт» (2025). URL: https://expertbrok.com.ua/services/cyber-insurance/.

6. Ксьонжик І.В., Жовта Н.А., Павліна А. І. Страхування ризиків кібербезпеки діяльності суб'єктів господарювання в сучасному інформаційному просторі. *ЕКОНОМІКА ТА СУСПІЛЬСТВО*. 2021. Випуск 34. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1042.

7. Кіберстрахування: характеристика та особливості. URL: https://www.lawfirm-pryadko.com/articles/kiberstrahovanie_harakteristika_i_osobennosti.

8. НБУ виступає за підвищення рівня інформаційної безпеки та кіберзахисту страховиків та банків. *FORINSURER* (*журнал про страхування, перестрахування та InsurTech*). URL: https://forinsurer.com/news/25/03/12/44712.

9. Перший український ЦОД з послугою кіберстрахування бізнесу від цифрових ризиків: DC | COSMONOVA. URL: https://cosmonova.net/ua/page/first-cyb-ins.

10. Пікус Р. В., Бабенко Л. Ю. Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава*. 2022. URL: http://www.economy.in.ua/pdf/2_2022/25.pdf.

11. Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами (2024). URL: https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami.

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

13. Найбільші кібератаки в Україні з 2014 року. *Інфографіка*. URL: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

14. Сергієнкова О.В., Мелентьєва О.В. Проблеми та перспективи розвитку страхування банківських ризиків в Україні (2022). URL: http://конференция.com.ua/pages/view/508.

15. Страхування кібер-ризиків. Cyber insurance. *FORINSURER* (*журнал про страхування, перестрахування та InsurTech*). URL: https://forinsurer.com/theme/48.

16. Кібератака на державні реєстри України (2024). URL: https://uk.wikipedia.org/wiki/Кібератака_на_державні_реєстри_України_(2024).

17. Goodman, M.D. & Brenner, S.W. (2023). The Emerging Consensus on Criminal Conduct in Cyberspace. *UCLA J.L. & Tech*, 3 URL: https://lawtechjournal.com/.

18. Каталог страхових продуктів для приватних осіб (2025). Офіційний сайт страхової компанії «VUSO». URL: https://vuso.ua/catalog.

19. Страхування кіберризиків Aon (2024). URL: https://www.aon.com/ukraine/solutions/risk-insurance-solutions/cyber-risk-insurance.jsp.

20. Протиотрута від хакерів: як захистити свій бізнес від кібер-атак. Офіційний сайт Української пожежно-страхової компанії (2025). URL: https://upsk.com.ua/about/news/all/protiotryta-vid-hakeriv-yak-zahistiti-sviy-biznes-vid-kiber-atak/.

21. Страхування підприємців в Києві та всій Україні (2024). Офіційний сайт страхової компанії «ІНГО». URL: https://ingo.ua/dlya-biznesu.

22. Reality check on the future of the cyber insurance market (2025). URL: https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html.

23. Глобальний ринок кіберстрахування. Основні тренди та прогнози на 2025 рік. *FORINSURER* (*журнал про страхування, перестрахування та InsurTech*). URL: https://forinsurer.com/news/24/11/19/44409.

ДОДАТКИ

Додаток А

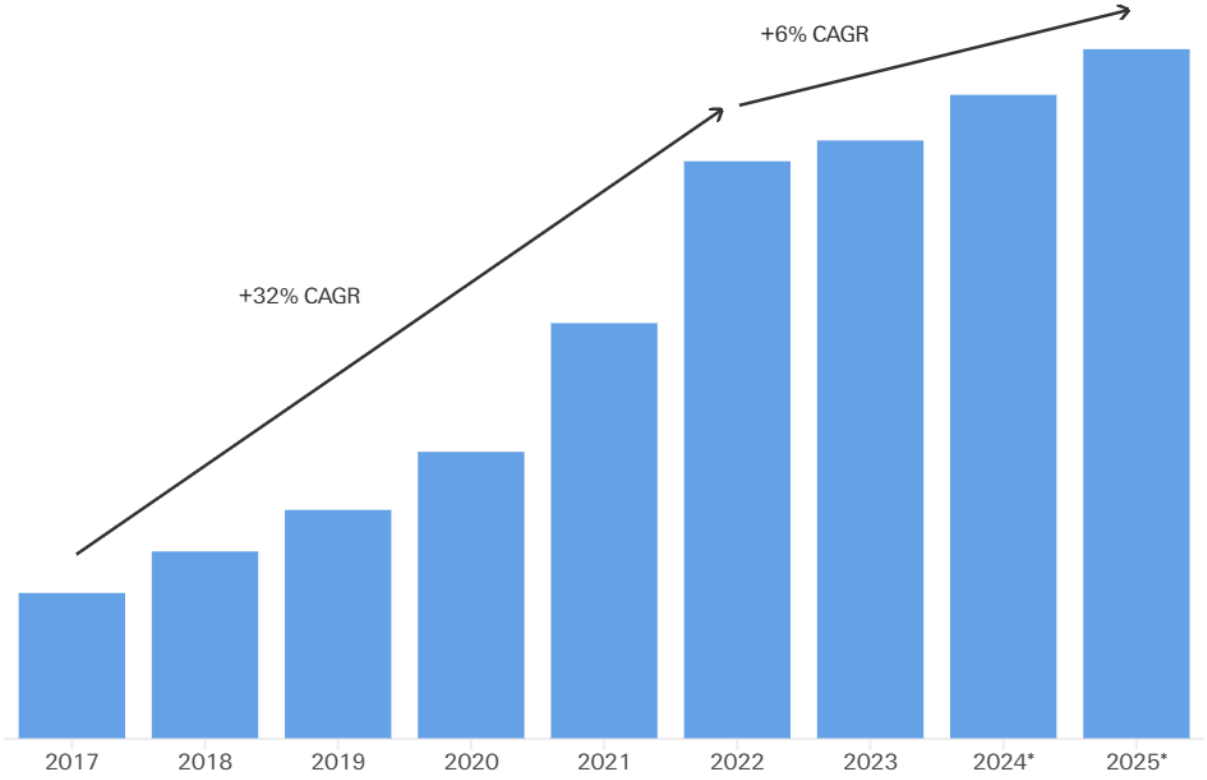

Рисунок А1 – Глобальна премія кіберстрахування за роками андерайтингу

Джерело: побудовано авторами за даними [22]

Додаток Б

Рисунок Б1 – **Етапи розробки стратегії розвитку кіберстрахування в Україні**

Джерело: запропоновано авторами