Київський національний торговельно-економічний університет

Кафедра фінансів

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Страхування кібер-ризиків»

Студента 2 курсу, 6 групи, Лашко Антона

спеціальності 072 Вячеславовича

«Фінанси, банківська справа та страхування»

спеціалізації «Страхування»

Науковий керівник Ротова Тетяна

к.е.н., доцент Анатоліївна

Гарант освітньої програми Волосович Світлана Василівна

д.е.н., професор

Завідувач кафедри фінансів, Чугунов Ігор Якович

заслужений діяч науки і техніки України

д.е.н., професор

Київ 2019

ЗМІСТ

ВСТУП

У наш час складно уявити світовий розвиток або будь-який процес без участі в ньому інформаційних технологій. Інформаційні технології посіли особливе місце і відіграють невід'ємну роль в сучасній економіці. Безумовно, такий наслідок ми отримали через те, що ІТ та економіка – це дві взаємопов'язані сфери, які створюють позитивній економічний ефект, прискорюють розвиток бізнесу і створюють можливості для швидкого обслуговування сотень тисяч будь-яких операцій. Сьогодні весь світ переживає часи, коли кардинально змінюється життя людей.

Ліміт розвитку сфери ІТ обмежується лише уявою самої людини, а отже з розвитком людини, можливості цієї сфери будуть лише зростати.

Проте, не зважаючи на таку кількість позитивних явищ від сфери ІТ, з неменшими від темпів розвитку позитивних явищ, розвиваються і певні негативні прояви від специфіки кібер-сфери. З появою мережі інтернет людство зустрілося з великою кількістю нових за своєю природою ризиків, оскільки кібер-ризик – це невід'ємна складова ІТ сфери. Таке явище як кіберзлочинність – це ще зовсім новий, молодий вид ризику. Кібер-ризики, як і ІТ-технології, мають дуже швидкий характер розвитку. З кожним роком кількість випадків, пов'язаних з кібер-ризиками, невпинно зростають. Відповідно до цього зростають і обсяги можливих і фактичних втрат юридичних, фізичних суб'єктів економічної діяльності, які використовують ІТ технології.

На початок 2019 року загрози кібер-атак становлять чи не найбільшу небезпеку для середнього і великого бізнесу. В опублікованому звіті компанії Trend Micro, світового лідера в області рішень для кібер-безпеки, відмічається сплеск поширення атак, які націлені на приховування шкідливих дій: кількість виявлених загроз такого роду показало 265-відсоткове зростання, порівняно з першою половиною 2018 року. [1]

З кожним роком питання страхування суб'єктів економічної діяльності від кібер-ризиків набуває все більшої актуальності. Кібер-ризики мають чи не найширший спектр негативного впливу на бізнес за своїм характером. Швидкий темп розвитку кібер-сфери дозволяє розглядати страхування кібер-ризків, як самий перспективний від діяльності в сфері страхування.

Дослідженням питання страхування кібер-ризиків займались такі вітчизняні вчені як: В. П. Братюк, С. В. Волосович, Ю. М. Пострелко, Н. В. Приказюк, М. П., Ротова Т. А., Чайковська, та інші.

Зарубіжними авторам публікацій, в яких аналізували ризики і страхові засоби від кібер-загроз були: С. В. Бремен, Ю. В. Бородакій, А. Н. Іващенко, І. А. Шарко.

Об'єктом дослідження дипломної роботи виступає страхування кібер-ризиків в Україні і світі.

Предмет дослідження – процес страхування кібер-ризиків, його розвиток та напрямки вдосконалення.

Мета роботи: проаналізувати та дослідити процес страхування кібер-ризиків та його розвиток, як окремого виду.

Для досягнення поставленої мети роботи поставлено такі завдання:

- розглянути основні види кібер-ризиків
- дослідити втрати спричинені в наслідок настання кібер-ризиків.
- проаналізувати наявні страхові послуги з страхування кібер-ризиків
- визначити переваги і недоліки страхування кібер-ризиків
- визначити можливі шляхи покращення існуючих послуг з страхування від кібер-загроз.

Методи дослідження. Дослідження виконувалось із застосуванням економічного, статистичного і порівняльного методів аналізу та синтезу. При обробці фактичних даних використовувались розрахунково-аналітичні, графічні, прогнозно-математичні методи.

Робота складається з вступу, трьох розділів, що включають в себе 6 підрозділів, висновків та пропозицій, списку використаних джерел із 36

найменувань і 5 додатків. У тексті роботи міститься 7 таблиць, 6 рисунків. Загальний обсяг роботи 50 сторінок.

РОЗДІЛ 1 Теоретичні основи виникнення кібер-страхування.

1.1 Передумови виникнення, розвиток та вплив сучасних ризиків на економіку та соціум

На початку 21 століття весь світ почав свої глибокі системні перетворення через науково-технічну революцію. Поєднання досягнень у сфері новітніх інформаційно-комунікаційних технологій та швидкого розвитку інформаційно-телекомунікаційних систем спричинило появу нового для людства так званого віртуального простору, який згодом отримав нову назву «кіберпростір». Головною особливістю кібер-простору є те, що він не має меж чи будь-яких кордонів. Кібер-простір повноправно може вважатися міжнародним простором.

У сучасному світі розвиток інформаційних технологій набирає все більших обертів. На сучасному етапі світового розвитку вже складно уявити будь-який процес без участі в ньому інформаційних технологій. ІТ-сфера тісно та динамічно інтегрується у всі галузі світової економіки, безпосередньо впливаючи на загальне зростання економічних та соціальних показників підприємств і організацій. Зараз неможливо уявити світ без ІТ. Вже не потребує доказів важливість і корисність інформаційних технологій для формування стійких конкурентних позицій організацій, розвитку усіх напрямів діяльності, покращення якості товарів та якості надання послуг тощо, не потребує доказів і те, як кібер-технології в сфері маркетингу призводить до розширення попиту.

Інформаційні технології посіли особливе місце і відіграють колосальну, і вже невід'ємну, роль в сучасній економіці. Безумовно, такий наслідок ми отримали через те, що ІТ та економіка – це дві взаємопов'язані сфери, які створюють позитивній економічний ефект, збільшують продуктивність роботи будь-якого бізнесу, прискорюють розвиток бізнесу і створюють можливості для швидкого обслуговування сотень тисяч можливих операцій

за мінімальний період часу. Сучасні ІТ-технології в економіці використовуються з метою забезпечення ефективної оперативної комп'ютерної обробки інформаційних ресурсів за чітко визначеними, безпомилковими алгоритмами, для збереження великих обсягів важливої інформації та можливості оперативного пошуку, обміну інформацією в будь-який час, у будь-якому місці і на будь-яку відстань. Отже, інформаційні технології значно полегшують процес прийняття економічно важливих рішень, адже дозволяють аналізувати, прогнозувати і детально прораховувати важливі економічні результати, на основі яких приймаються управлінські рішення. Через це, сучасні ІТ моделі посідають невід'ємне місце у процесі ефективного управління в сфері економічної діяльності. Саме через це формується вагомий вплив ІТ-сфери на економічні галузі у зовнішньому середовищі та транснаціональному масштабі.

Для України ІТ-сфера має особливо важливе значення, адже на фоні певних несталих явищ в економіці, вона здатна згладити їх за допомогою стрімкого розвитку, а також забезпечення функціонування багатьох суміжних галузей.

Можна відзначити такі характеристики українського ІТ-ринку: зростання професіоналізму серед ІТ-фахівців та компаній-замовників, що сприяє більш грамотному вибору технологій виконання бізнес-завдань із урахуванням майбутнього розвитку; зростаючий інтерес організацій та підприємств до бізнес-рішень для підвищення ефективності роботи; усвідомлення необхідності автоматизації процесу управління інформацією та збереженням даних з метою отримання конкурентних переваг; необхідність відповідності до законодавчих вимог; прагнення до збільшення прозорості бізнесу та інвестиційної привабливості [2].

Без застосування нових інноваційних інформаційних технологій економіка не може розвиватися і конкурувати з іншими суб'єктами економічної діяльності, особливо враховуючи розвиток сучасної світової глобалізації. Проте, не зважаючи на таку кількість позитивних явищ або

ефектів від сфери ІТ, з неменшими від темпів розвитку позитивних явищ, розвиваються і певні негативні прояви від специфіки кібер-сфери.

З появою мережі інтернет людство зустрілося з великою кількістю нових за своєю природою ризиків, оскільки кібер-ризик – це невід'ємна складова ІТ сфери. Таке явище як кіберзлочинність – це ще зовсім новий, молодий вид ризику, якщо порівнювати його з класичними видами ризиків, такі як крадіжка, ризик отримання збитків від наслідків стихійного лиха, смерть, хвороба тощо.

Захист інформації є однією з вічних проблем, як зазначається в науковому віснику Ужгородського національного університету, протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми — комп'ютерні злочини стали характерною ознакою сьогодення. [3]

Кібер-ризики та ІТ-технології існують як взаємопов'язані речі. Розвиток інформаційних технологій провокує виникнення нових загроз, нових методів кібер-атак, розширення шляхів кібер-шахрайства, що в же в свою чергу стимулює вдосконалення, і відповідно розвиток, нових технологій. Кібер-ризики, як і ІТ-технології, відповідно мають дуже швидкий характер розвитку.

30 серпня 2019 р. стало відомо, що компанія Trend Micro Incorporated, світовий лідер в області рішень для кібербезпеки, опублікувала звіт за першу половину 2019 р. У ньому відзначається сплеск поширеності безфайлових атак, спрямованих на приховання шкідливих дій : кількість виявлених загроз такого роду показала 265% зростання порівняно з першою половиною 2018 р.

Окрім цього, кількість схем цифрового вимагання показала зростання на 319% з другої половини 2018 року, що відповідає попереднім прогнозам. Компрометація ділової електронної пошти залишається основною загрозою: число виявлення таких загроз виросло на 52% за шість місяців. Кількість

файлів, електронних листів і URL-адрес, пов'язаних з вимагачами, також виросло на 77% за той же період.

Trend Micro виявили і заблокували 1,8 мільярдів загроз вимагачів по всьому світу з січня 2016 по червень 2019 року. В цілому продукти Trend Micro заблокували більше 26,8 мільярдів загроз в першій половині 2019 року, що на 6 мільярдів більше, ніж за аналогічний період минулого року. [4]

Кожного наступного року зловмисники працюють по-іншому. Вони орієнтуються на підприємства і середовища, які забезпечать найбільшу віддачу від вкладених зусиль.

Аналізуючи кібер-злочинність у світі, був сформований рейтинг, який показує кількість атак, які відбулися на території певної держави та відсоток від усіх атак були здійснені на територіях цих країн шляхом зараження файлів на ресурсах. За даними Лабораторії Касперского був сформований Топ 20 найбільш заражених інтернет просторів країн. (табл. 1.1)

Табл. 1.1

Топ-20 країн по кількості розміщеного на ресурсах шкідливого програмного забезпечення

Місце	Країна	Кількість атак	% від усіх атак
1	США	240022553	25,4
2	Росія	138554755	14,6
3	Нідерланди	92652499	9,8
4	Німечина	82544496	8,7
5	Україна	47886774	5,1
6	Китай	46482840	4,9
7	Великобританія	44676036	4,7
8	Британські віргінські острови	26336323	2,8
9	Канада	19723107	2,1
10	Швеція	15472406	1,6
11	Франція	14706167	1,6
12	Румунія	12685394	1,3
13	Корея	7220494	0,8
14	Чехія	6009847	0,6
15	Латвія	5371299	0,6
16	Іспанія	5066469	0,5
17	Японія	3468602	0,4
18	Турція	3150767	0,3

19	Бразилія	2712440	0,3
20	Беліз	2662150	0,3

1.2 Страхування кібер-ризиків як важливий компонент підвищення рівня кібер-захисту

З кожним роком кількість випадків, пов'язаних з кібер-ризиками зростають. Відповідно до цього зростають і обсяги можливих і фактичних втрат юридичних, фізичних суб'єктів економічної діяльності, які використовують IT технології у процесі своєї діяльності.

У лютому 2018 року аналітики антивірусної компанії McAfee підрахували, що в 2017 році світовий збиток від кіберзлочинів склав біля $600 млрд або 0,8% від світового ВВП, збільшившись приблизно на 35% порівняно з оцінкою за 2014 рік в $445 млрд.

Серед чинників, що зумовили зростання, фахівці перерахували усе більш витончені хакерські атаки, розширення ринку кібер-кримінальних послуг і поширення криптовалют.

За даними звітів Cisco Annual Cybersecurity, більше ніж половина всіх атак нанесли фінансовий збиток у розмірі 500 мільйонів доларів, у тому числі втрату доходів, втрачену вигоду, безпосередні витрати і відтік замовників.

Через хакерські атаки, які спровокували витік корпоративних даних, компанії по всьому світу втратили 3 трильйони доларів в 2018 році. Про це говорять дані наведені аналітиками Juniper Research в звіті, опублікованому в серпні 2019 року.

За даними звіту щодо глобальних ризиків 2015 р. Міжнародного економічного форуму (World Economic Forum), віртуальні (кібер) ризики названі одними з найголовніших комерційних ризиків. На початок 2019 року загрози кібер-атак становлять чи не найбільшу небезпеку для середнього і великого бізнесу. За даними однієї з найбільших компаній Trend Micro, за 2018 рік було опрацьовано 2,5 трильйона запитів. Також було відкрито і досліджено 222 нових «сімейств» програм-вимагачів.

Кібер-ризики є найбільш недооціненими ризиками в довгостроковій перспективі в Україні. Яскравим прикладом цього є те, що у 2017 р. під час кібератаки вірусу Petya постраждали понад 1500 компаній, а 13 тисяч комп'ютерів були заражені. За рік український бізнес втратив від кібератак мільярди гривень.

Аналізуючи дані стосовно кібер-ризиків, наслідки від яких відчули організації середнього та малого бізнесу в 2017 р., як в Україні, так і в світі, була сформована таблиця найбільш небезпечних кібер-ризиків (Додаток А)

В наслідок зростання питання серйозності наслідків організації, які відносяться до малого або середнього бізнесу змушені звернути свою увагу на новий вид ризику, який несе чи не найбільшу небезпеку для них – це кібер-ризики. Порівняно з великими компаніями, які також зазнають величезних збитків, але можуть відновитися і продовжити життя, малий та середній бізнес приблизно в 60% випадків змушені закритися протягом півроку після втрати своїх даних.

Настання кібер-ризиків для організацій малого та середнього бізнесу призводить до наслідків, які наведені в таблиці 1.2

Таблиця 1.2

Наслідки для організацій малого та середнього бізнесу від настання кібер-ризиків

Вплив на малий та середній бізнес	Збиток
припинення або уповільнення бізнес-процесів	втрата клієнтів та прибутку
втрата конкурентної переваги	
збиток для бренду та втрата репутації	зниження вартості бізнесу
судові розгляди та позови	витрати на усунення наслідків, штрафи і санкції регулюючих органів

Побудовано автором на підставі [3]

Проаналізувавши інформацію про те, яким шляхом відбуваються збитки в наслідок настання кібер-ризиків, а також до яких наслідків вони призводять, можна скласти визначення.

Кібер-ризик - ризик, пов'язаний з використанням комп'ютерного устаткування і програмного забезпечення, як в місцевих (локальних) мережах, так і у глобальній Інтернет-мережі; у розрахунково-платіжних системах, системах інтернет-торгівлі промислових системах управління; а також ризик пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних.

Інформаційна безпека компаній потребує інвестування великих сум. За оцінками аналітичної компанії Gartner, за 2017 рік у світі було витрачено порядку $86 млрд на превентивні системи і заходи по кібер-безпеці. За прогнозами на 2018 р. витрати зростуть ще на 8-12%, але при цьому не можна гарантувати, що вкладення виявляться ефективними і дозволять уникнути наростаючих загроз.

Так як превентивні заходи не здатні гарантувати 100% успіху внаслідок стрімких темпів розвитку інформаційних технологій, політика риск-менеджменту багатьох компаній Європи і США застосовує інструменти "пізнього реагування" - страхування від кібер-ризиків. На відміну від первинних заходів забезпечення захисту, страхування надає можливість компенсувати втрати від кібер-загроз, що реалізувалася, якщо її так і не вдалося запобігти.

Згідно з даними, представленими в лютому 2018 року по розкриттю потенціалу ринку кібер-страхування, сьогодні рівень використання даних послуг в 37 країнах з розвиненою економікою досягає 50-60% серед компаній-представників великого бізнесу.

Об'єм глобального ринку страхування від кібер-ризиків в 2017 р. оцінювався приблизно в $2, 5 млрд. І він продовжує рости: очікується, що до 2021 року він досягне $10 млрд. [7]

У грудні 2017 року компанія Positive Technologies опублікувала результати свого дослідження на тему «скільки коштує інформаційна безпека». Більшість російських промислових компаній витрачають на інформаційну безпеку менше 50 млн рублів в рік. При цьому 27%

організацій, опитаних фахівцями Positive Technologies в ході дослідження, оцінили в аналогічну суму втрати за один день простою інфраструктури внаслідок кібер-атаки. Третина (33%) промислових організацій оцінила можливий збиток від відмови в роботі корпоративної інфраструктури протягом одного дня в суму від 0,5 до 2 млн руб., 13% - від 2 до 10 млн руб. і 17% - від 10 до 50 млн руб. Більшість промислових компаній (83%) заявили про готовність відновити інфраструктуру, не витративши і 0,5 млн рублів, проте така оцінка здається експертам Positive Technologies заниженою.

Регулярні тести на проникнення (2 рази в рік) проводять лише 13% промислових компаній, в 44% - вони ніколи не проводилися. У 33% компаній інвентаризація і контроль за появою небезпечних ресурсів в периметрі мережі не проводяться ніколи. У 40% організацій ніколи не проводився аналіз захищеності корпоративних безпровідних мереж. У 23% промислових компаній відсутній контроль установки оновлень програмного забезпечення. [8]

Згідно з даними веб-порталу Positive Technologies за IV квартал 2018 року, актуальні кібер-загрози можна виділити об’єкти атак (рис. 1.1), методи атак та категорії жертв

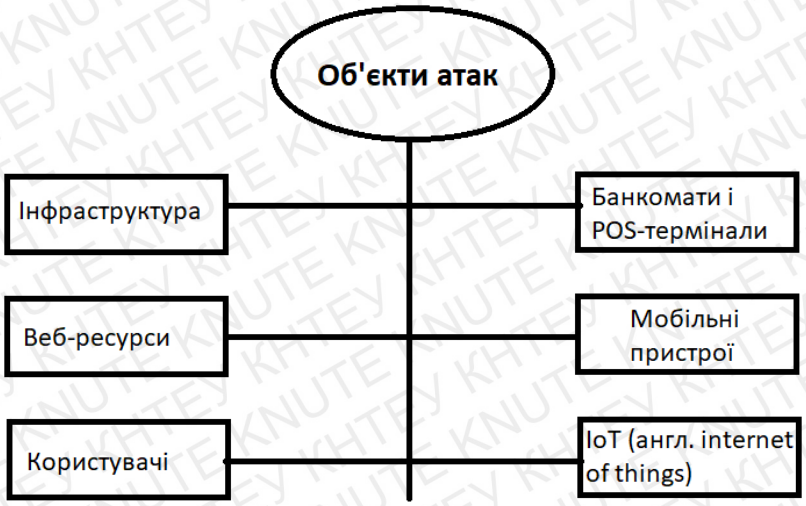


Рис. 1.1 Об’єкти кібер-атак

Методи атак: використання шкідливого програмного забезпечення; підбір облікових записів; соціальна інженерія; хакінг; експлуатація веб-уразливостей; DDoS-атаки.

До категорії жертв можна віднести: фінансовий сектор, державні установи, медичні заклади, промислові компанії, онлайн-сервіси, сфера послуг, транспорт, ІТ-компанії, торгівля, криптовалютні біржі та інші сфери.

РОЗДІЛ 2 Дослідження страхування кібер-ризиків.

2.1 Методи аналізу кібер-ризиків для укладання та супроводження договору страхування

Сучасний світ, в тому числі кібер-простір, потерпає від чисельності і різноманітності загроз. Аналізуючи онлайн інтерактивну карту кібер-загроз «Cybermap.kaspersky» (додаток Б), стає зрозуміло, що вже не існує моменту, коли б світ не зазнавав тиску від кібер-ризиків.

За допомогою роботи різних за своєю дією сканерів та антивірусів, таких як: On-Access Scan, Web Anti-Virus, Vulnerability Scan, Kaspersky Anti-Spam, Botnet Activity Detection, Mail Anti-Virus, On Demand Scanner, Intrusion Detection Scan - у світі щосекунди фіксується в середньому 750 виявлених загроз.

Кількість атак продовжує невпинно зростати. Проведений аналіз статистики атак показав, що найпоширенішими видами кібер-загроз залишилися ті самі методи, як і 5 років тому. Проте, з кожним днем вони розвиваються та прогресують в своїй сутності і приносять все більших збитків бізнесу, державам та цілим регіонам.

Згідно з оприлюдненими звітами компаній, які займаються кібер-безпекою, можна сформувати наступний рейтинг найпопулярніших загроз:

1. Віруси і віруси-вимагачі. Зазвичай вірусом називають шкідливе програмне забезпечення, яке заражає комп'ютер або інший електронний пристрій, коли користувач відкриває вкладення електронної пошти або проходить по посиланню на шкідливий сайт. Вірус-вимагач - це спеціалізований вірус, який при зараженні шифрує усі файли в системі і не віддає користувачеві дані, поки не буде заплачений викуп. Найвідомішими представниками вірусів-вимагачів є «Alcatraz Locker», «Globe», «NoobCrypt» і звісно «WannaCry», який з даними компанії KnowBe4, що спеціалізується на кібербезпеці, вразив від 200 тис. до 300 тис. комп'ютерів у щонайменше 150 країнах. Можливі збитки, завдані WannaCry за перші чотири дні,

перевищили 1 млрд, якщо враховувати викликані цим масштабні простої великих організацій по всьому світу.

2. Потенційно небажані програми (PUP) Потенційно небажані програми - це трояны, програми-шпигуни або рекламне ПЗ. Зазвичай вони встановлюються разом з іншою, корисною програмою, яку вирішив завантажити користувач. Такі програми можуть потайно записувати усі натиснення на клавіші, сканувати файли на жорсткому диску і читати cookie-файли браузеру. Яскравим представником є вірус Petya та сімейство цього вірусу.

3. Фішинг - це спосіб злому за допомогою електронних листів (і не тільки), в яких користувача намагаються обдурити і змусити передати логін і пароль від якого-небудь сервісу або іншу важливу інформацію. Для цього лист може бути оформлений як сповіщення від банку або послання від знайомого. Згідно з аналітичними даними Trend Micro, в Україні за минулий рік зросла кількість випадків фішингового шахрайства. У 2018 році було зафіксовано 491 492 атаки, а в 2017 році таких атак - 465 664.

4. Взлом профіля користувача. Хакер може отримати доступ до облікового запису користувача за допомогою "лобової атаки", коли спеціальна програма перебирає безліч варіантів логіна і пароля - зазвичай з використанням словника і інших паролів, вкрадених раніше.

5. Своєчасно не оновлене або застаріле програмне забезпечення. Один з найпопулярніших шляхів доступу для проникнення. Хакери можуть використати уразливості в системному програмному забезпеченні і веб-застосуваннях для виконання несанкціонованого коду, дістаючи доступ до системи або викрадаючи інформацію. Яскравим прикладом може слугувати компанія Equifax, у якої був встановлений веб-фреймворк Apache Struts, який вчасно не був оновлений, і це привело до ражі 143 млн номерів соціального страхування, адрес, номерів водійських прав і кредитних карт.

6. DDoS атака. Хакерська атака на обчислювальну систему з метою перенавантажити її повністю, тобто створення таких умов, при яких

добросовісні користувачі системи не зможуть отримати доступ до системних ресурсів (серверам), що надаються, або цей доступ буде ускладнений.

Досліджуючи способи настання кібер-ризиків за видами подій, було доцільно виділити:

- нецільові атаки, до яких можна віднести фішинг, кардінг, смс-шахрайство.
- цільові атаки – фінансове шахрайство, розкрадання баз даних, промислове шпигунство, DDoS атаки.
- атаки з внутрішнього середовища – розкрадання, знищення інформації, сприяння цільовій атаці.

Використовуючи зведену статистику, що надана Positive Technologies за перший квартал 2019 року, можна відмітити зростання частки атак, які направлені на отримання даних. Станом на сьогодні, більше половини хакерських атак здійснюються з метою розкрадання інформації (рис. 2.1). Зловмисники зацікавлені в найрізноманітніших даних - від особистого листування до комерційної таємниці (рис. 2.2).

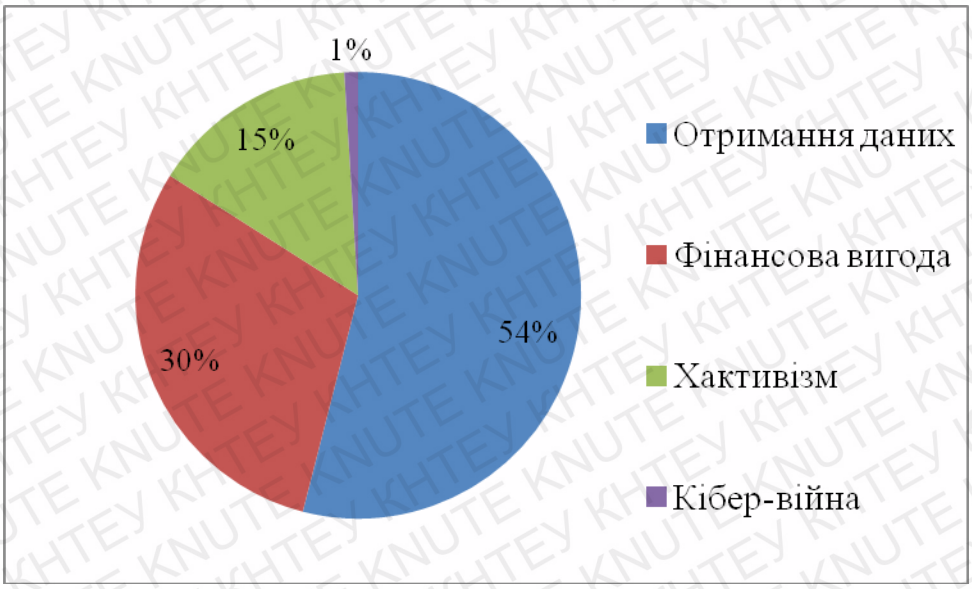


Рис. 2.1 Мотиви кібер-злочинців

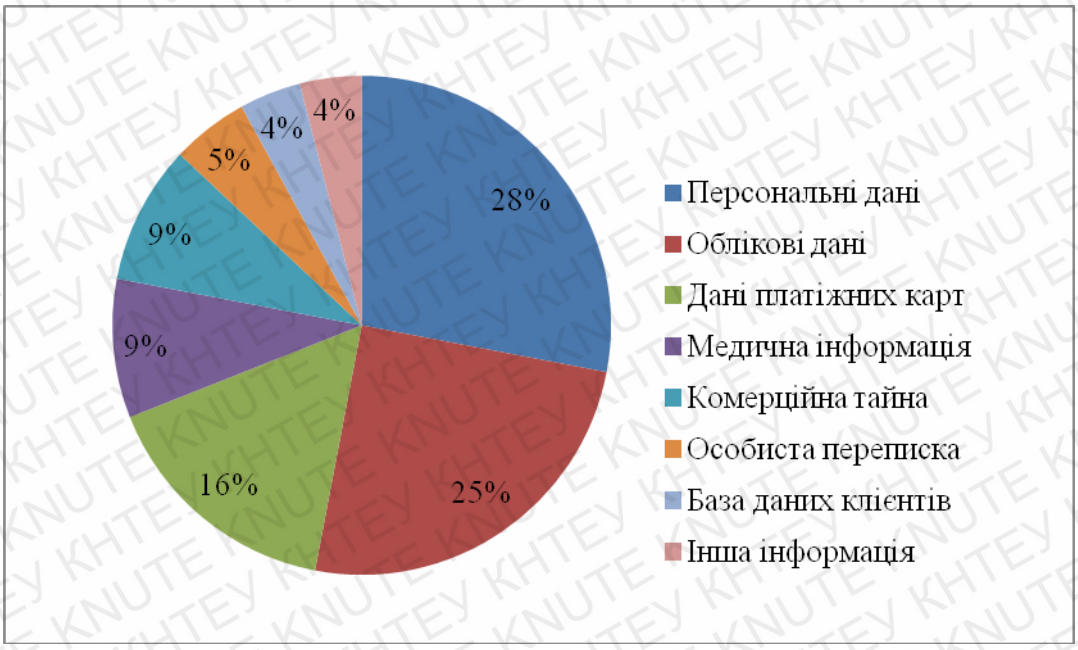


Рис. 2.2 Типи вкрадених даних

У І кварталі 2019 року доля цілеспрямованих атак знизилася в порівнянні з IV кварталом 2018 року і склала 47% проти 62%. Це пов'язано зі збільшенням долі атак, які не прив'язані до конкретної галузі, в основному йдеться про масові шкідливі кампанії. Частка кібер-інцидентів, в результаті яких постраждали приватні особи, практично не змінилася (21% проти 22% в IV кварталі 2018 року). Серед юридичних осіб найчастіше зловмисники атакують державні організації, медичні установи, промислові компанії, банки і інші організації фінансової сфери. [9]

Для забезпечення безпечного функціонування бізнесу в наш час не можливо обійтися без засобів захисту в кібер-сфері. Необхідно виконувати усі можливі превентивні заході. Наприклад, для великих компаній є доцільним проводити тести на захищеність своїх систем, даних та даних своїх клієнтів. Своєчасне оновлення програмного забезпечення, постійна зміна кодів доступу, створення та зберігання резервних сховищ даних, моніторинг навантаження серверів, обслуговування сучасних антивірусів та сканерів загроз – все це має меншу ціну порівняно з втратами великих компаній від кібер-злочинності. Проте, навіть використання всіх

найновітніших, найсучасніших превентивних заходів не може гарантувати сто відсотковий захист бізнесу.

Щороку кіберзлочинність завдає державам та приватним особам дуже великої шкоди.

За даними компанії McAfee, що займається розробкою антивірусного програмного забезпечення, кібер-злочинці щорічно завдають світовій економіці збитків у розмірі $600 млрд. Страховий концерн Lloyd's називає трохи скромнішу цифру – $400 млрд на рік. [11]

На 73-й сесії Генеральної асамблеї ООН генеральний секретар Антониу Гуттереш оцінив щорічні збитки від кіберзлочинності у світі в розмірі 1,5 трлн доларів. На жаль, прогнози експертів з кібербезпеки невтішні. В майбутньому кількість злочинів та збитків від кібератак лише зростатиме, адже зазвичай правопорушники йдуть щонайменше на крок попереду механізмів, які мають державні органи та приватні особи щодо запобігання і розкриття таких злочинів. [10]

Лише атака вірусів WannaCry і Petya у 2017 році зачепила 150 країн і завдала збитків більш ніж на $12 млрд. Тому компанії витрачають на кібер-захист все більше коштів. У дослідженні агентства Markets and Markets йдеться про те, що за підсумками 2018 року витрати бізнесу на захист від хакерів склали майже $153 млрд, а в 2023-му вони перевищать $248 млрд.

У відповідь на кібер-загрози та на такі масштабні втрати страховики запропонували нове покриття, яке б змогло надати захист компаніям і гарантувати мінімізацію втрат при настанні випадку кібер-ризику. Страхування від кібер-ризиків за оцінкою експертів може стати чи на найперспективнішим видом страхування в найближчі роки.

Згідно з дослідженням страхової групи Allianz, ринок кібер-страхування зростає на 25–50% щороку. Договір страхування кібер-ризиків допомагає захиститися від загроз, внаслідок яких може статися витік даних, вихід з ладу різного обладнання, а також збитків, які через ці події несе страхувальник.

Зараз страхові компанії лише починають напрацьовувати свою практику у цій сфері. За підрахунками перестрахової компанії Munich Re, які вони провели в вересні 2019 року, на сьогоднішній день захист такого роду пропонують приблизно 60 страхових компаній. Страхове покриття кібер-ризиків становить лише 5%, але стрімке зростання кібер-загроз змушує розвивати цей продукт. [11]

Такий невеликий відсоток покриття кібер-ризиків спровокований внаслідок декількох причин. Першою причиною, яка сповільнює розвиток даного виду страхування, це необхідність в унікальних андерайтерських підрахунках. За словами андерайтера страхової компанії «ТАС» Заросило Георгія: «Ніхто ще не має чіткого поняття, як прорахувати такі ризики. Не існує чітко виявлених можливих шляхів настання страхового випадку в кібер-сфері, з кожним новим днем ризики зростають. Всі бояться бути першими, оскільки можуть понести великих збитків». Другою причиною є те, що потреби страхувальників частково задовольняються через через придбання додаткових розширень у договорах майна, відповідальності. Але покриття за кібер-ризиками в таких договорах, з огляду на специфіку цих видів страхування, досить обмежене. Таким прикладом може бути покриття фінансових збитків внаслідок припинення діяльності в результаті кібер-інциденту.

Як відмічають учасники українського страхового ринку, говорити про повноцінний сектор кібер-страхування в нашій країні доки ще рано. Інтерес до послуги почав формуватися кілька років тому, коли компанії підрахували збитки і недоотриманий прибуток із-за атаки вірусу Petya.A. Крім того, базова інфраструктура, необхідна для розвитку цього виду страхування, тільки формується. Так, Закон "Про основні принципи забезпечення кібер-безпеки України" набув чинності в травні 2018 року, а Державний центр реагування на кібер-загрози був створений тільки півроку тому.

"Кібер-ризики - дуже актуальна проблема, але для її вирішення через страхові інструменти треба створити умови. Потрібно і законодавчу базу, і

технічні можливості, і готовність клієнтів співпрацювати із страховиком при створенні системи корпоративної кібер-безпеки". Експерти відмічають, що в українських реаліях далеко не завжди можна провести навіть передстраховий аудит інформаційної системи клієнта, і тому є безліч причин. Як результат, не усі страховики готові представити повноцінні програми по страхуванню кібер-ризиків в Україні. Зараз вони є у 5-7 страхових компаній і трьох страхових брокерів. [7]

Проте, вже починають з’являтися випадки страхового рішення в цьому питанні. Вітчизняні страхові компанії спільно зі своїми європейськими партнерами розроблюють програми в сфері кібер-страхування. Наприклад, для страхування кібер-ризику є можливість розмістити їх на популярному лондонському ринку Lloyd's. Крім цього, також можна застрахуватися через програми західних перестраховиків, і використати їхні пакетні рішення по кібер-захисту в різних сферах та умовах ведення бізнесу.

2.2 Методи аналізу кібер-ризиків для укладання та супроводження договору страхування

З огляду на проблему швидкої дифузії кіберзагроз і практично відсутність контролю за їх поширенням варто виділити рівні прояву кіберзлочинів:

- мікрорівень (рівень окремих домогосподарств і підприємств);
- макрорівень (рівень окремих галузей);
- мезорівень (рівень окремих країн чи їх об'єднань). Відповідно до тривалості впливу наслідків ризику, можна виокремити довгострокову та короткострокову дію кіберзлочину. [12]

Консалтингова компанія Phenomenon провела опитування серед 2168 фірм в країнах Європи, Південної Америки, Азії та Африки, які запровадили управління кібер-ризиками як складову системи управління ризиками. Відповіді респондентів показали, що 46 % мали досвід з кібератаками, причому вони носили різний характер – пов'язані з руйнуванням бізнесу та IT-процесів – 46 %, пошкодженням або крадіжками конфіденційних даних фірми (наприклад інтелектуальну власність) – 34 %, з крадіжками конфіденційної інформації приватних осіб – 26 % [13].

Згідно з дослідженнями страхової компанії Allianz, до кіберризиків, що найбільше впливали на діяльність компаній, належать переривання бізнес-процесів, крадіжка інтелектуальної власності та кібервимагання [14]. За даними Центру стратегічних та міжнародних досліджень (Senter for Strategic&International Studies, CSIS) кількість значних кіберінцидентів практично щороку зростає. При цьому спостерігається чітка тенденція до їх зростання впродовж 2014–2018 р.

Спільні дослідження CSIS та компанії McAfee свідчать, що щорічна вартість кібер-злочинів у глобальному масштабі становить 445–600 млрд дол. США. Це складає приблизно 1 % світового ВВП. У структурі мотивацій кібер-атак станом на січень 2018 р. найбільшу частку займають кібер-

злочини (cyber crime) – 81,7 %. Водночас частка кібер-шпигунства (cyber espionage) склала 12,2 %, кібер-війн (cyber warfare) – 4,3 %, хактівізму (hacktivism) – 1,7 %. За векторами дії кібератак станом на січень 2018 р. переважали шкідливі програми – 43,5 %. При цьому частка викрадення облікових записів склала 14,8 %, невідомих – 13 %, цільових атак – 9,6 %, DDoS – 6,1 % [15].

При аналізі розвитку продуктів кібер-страхування, слід враховувати певні фактори. Першим фактором впливу на розвиток і розповсюдження даного страхового продукту є територіальний фактор. Одним з визначальних факторів, від якого залежить формування попиту, є географічне розташування. Наприклад, яскраво відчутна різниця, якщо порівняти розвиток інформаційних технологій на африканському континенті та запровадження і об'єми використання ІТ-рішень на території Австралії або Північної Америки. Одразу стає зрозуміло, що африканська територія суттєво менше залежить від ІТ-підримки. Можливість настання збитків та об'єми можливих втрат через настання кібер-ризиків будуть в багато разів меншими, оскільки хаккінг, аналогічно до розвитку ІТ, на континенті має менш розвинену природу.

Другим фактором, який має найбільший вплив на страхування кібер-ризиків – це законодавча база країни страхувальника.

Неменш важливим фактором впливу є соціально-вікова структура населення на розвиток ІТ технологій в країні страхувальнику. Молодь та доросле населення виступають активними користувачами мережі інтернет. Кількість збереження важливих, цінних файлів, об'єми потоку даних в інтернеті прямопропорційно залежить від кількості користувачів. Наприклад розвиток країн СНГ має тенденцію великої міграції молоді, кваліфікованих кадрів, в сфері інформаційних технологій, в країни з більш розвиненою економікою. Відтік молодого, дорослого, кваліфікованого населення впливає не тільки на об'єми інформації в кібер-просторі, а також створює важливий для нашого часу ефект «необізнаності» населення в кібер-сфері. Цей ефект

«необізнаності» населення суттєво впливає на попит продуктів сфери-кібер захисту, оскільки більшість людей не усвідомлює можливість наслідків кібер-ризиків.

Це формує сукупне хибне враження, що системи розроблені для посилення кібер-захисту це лише не потрібні додаткові витрати. Прикладом впливу вікової структури населення може слугувати проста ситуація: наприклад, людина похилого віку не використовує системи інтернет банкінгу. В свою чергу це зменшує потребу банку в страхуванні кібер-безпеки своїх користувачів. Ще одним прикладом необізнаності населення може бути посилення ризику кібер-загроз, банально коли клієнт або працівник компанії зберігає паролі або важливу, секретну інформацію на телефоні, яка згодом потрапляє до рук шахраїв через фішінгові системи шахрайства. Важливо відмітити те, що більшість кібер-атак залишаються не індентифікованими.

За словами Еллісон Хілл, виконавчого директора Cobb, Decker, Dunphy & Zimmerman: «Не думайте, що ваша компанія не схильна до ризику тільки тому, що це не очевидно. Якщо ви проводите платежі по кредитних картах, у вас є ризик. Якщо ваші дані проходять через електронні носії, у вас є ризики. Якщо у вас є електронна пошта, ви відпадаєте під кібер-ризики. Не існує бізнесу, який був би по-справжньому неприступним для потенційних кібер-загроз. У кінцевому рахунку, у вас є вибір, чи купити страховку або самостійно «страхуватися», але визнання потенційної можливості втрати є найбільш важливим елементом цього процесу ».

Незважаючи на очевидний ризик для підприємств усіх розмірів і у всіх галузях, більшість власників малого бізнесу тільки починають дізнаватися про таке явище кібер-безпека. Так само як і більшість маленьких страхових компаній все ще намагаються знайти найкращий спосіб андеррайтерських підрахунків, щоб впровадити та закріпити в себе найвигідніший для себе поліс кібер-страхування, що робить ще більш важливим освіту з боку власника бізнесу.

Проаналізовані можливості настання ризиків і їхні обсяги, наштовхують на логічне питання: скільки повинно коштувати страхове покриття від кібер-ризиків? Для цього слід виділити основні фактори, від яких залежить сума страхових премій.

Вартість кібер-страхування залежить від декількох факторів ризику, які варіюються відповідно до газузі, в якій працює бізнес. Наприклад, деякі договори страхування можуть коштувати близько 500 доларів, а інші - 5000 доларів і більше. Вартість кібер-страхування залежить від безлічі факторів, які оцінюються андеррайтерами у процесі формування продукту кібер-страхування.

Крім того, слід враховувати покриття і визначення лімітів страхування. Вартість вашого кібер-страхування збільшиться при збільшенні лімітів покриття. Наприклад, згідно зі зарубіжною статистикою, поліс з страховою сумою в 3 мільйони доларів буде коштувати, в середньому, більше 25 тисяч доларів. Також, якщо у вас є партнерський договір, який потребує більш високих лімітів покриття, можна обрати різні умови покриття і платити тільки за те, що для бізнесу актуально.

Важливім фактором є і доступ до даних. Вартість вашого полісу страхування від кібер-ризиків напряму залежить від того, хто має доступ до систем або даних страхувальника. Наприклад, найм стороннього партнера по IT або обслуговування веб-сайту – все це може піддавати бізнес клієнта більшому ризику, ніж наймання корпоративного співробітника. Крім того, також при оцінюванні ризиків має місце запровадження обмеження доступу до інформації тільки для необхідних співробітників, партнерів і клієнтів – це може допомогти мінімізувати кібер-ризик, а відповідно, і ціну. [16]

Розглянемо такий фактор як мережева безпека. Зберігання конфіденційної інформації в незахищеній мережі збільшує ризик кібер-загроз, таких як злом даних, комп'ютерні атаки і електронне вимагання. Ваша ціна на страхування від кібер-ризику може бути меншою, якщо ви зможете показати, що працюєте в середині захищеної мережі. Це може включати в

себе якісного антивірусного програмного забезпечення, використання мережевих брандмауерів і регулярне оновлення паролів.

Також слід врахувати галузь в якій працює бізнес. Бухгалтери, медичні компанії та ІТ-компанії є одними з багатьох галузей, які за своєю суттю повинні працювати зі збором зберіганням великих обсягів даних. Компанії пов’язані з цією роботою, як правило, платять більше за страхування від кіберпростору, тому що відновлення після настання кібер-інциденту, пов'язаного з великою кількістю конфіденційної інформації, зазвичай обходиться страховій компанії дорожче. [17]

Не менш важливим для укладання договору страхування - історія кібер-інцидентів. Як і в більшості інших сферах страхування, враховуються певні коефіцієнти, що збільшують вартість вашої премії за страхування кібер-ризиків, якщо в недавньому минулому у вас були випадки порушення вашого кібер-простору, якщо ваша компанія була пов’язана з кібер-інцидентами. Вважається, що бізнес, який в минулому стикався з кібер-ризиками, має більш високий ризик порушень в майбутньому, ніж бізнес без попередніх пригод.

Страхування кібер-ризиків - це програма, призначена для того, щоб допомогти компаніям пережити витік даних, покриваючи відповідальність компанії і збитки, які можуть виникнути. Програму кібер-страхування слід ділити на дві категорії.

Перша категорія включає первинне покриття, яке призначене для відшкодування збитків та шкоди, завданої вашому бізнесу, тобто першій особі. Другою можна вважати стороннє покриття - для збитків, яких зазнають ваші клієнти або шкоди, яку понесуть клієнти в наслідок кібер-події.

Власники малого бізнесу зазвичай потребують страхування з первинним покриттям. Проте, компанії, які хочуть захистити конфіденційну інформацію, що зберігається у вигляді електронних даних, зберіганні даних про клієнтів, часто в формі номерів кредитних карт або адресів електронної пошти можуть також захотіти отримати стороннє покриття. Стороннє

покриття зазвичай резервується для підприємств інформаційних технологій (IT), які відповідають за безпечне зберігання даних, таких як розробники програмного забезпечення і адміністрування баз даних.

Страхування від кібер-ризиків першої особи покриває проблеми, які пов'язані з витоком даних і іншими кібер-інцидентами у компанії. Будь-якому власнику бізнесу, який зберігає, відправляє або отримує електронні дані, даний вид страхування буде актуальним, оскільки є можливість отримання страхового відшкодування від кибер-загроз. Це допоможе мінімізувати витрати, якщо кібер-злочинець проникне в їх мережу.

Зазначимо, що витрати, які оплачує первинне покриття кібер-страхування, включають:

- витрати на повідомлення клієнтів;
- послуги кредитного моніторингу для бізнесу;
- зв'язки з громадськістю та маркетинг доброї волі;
- дохід бізнесу втрачений через порушення;
- викуп (в разі кібер-вимагання).

Залежно від своєї бізнес-моделі, деякі компанії можуть придбати страховку від кібер-ризиків з покриттям відповідальності. Таке страхування покриває відповідальность перед третьою особою покриває вашу відповідальність за дані ваших клієнтів. Зазвичай його купують компанії, які встановлюють або обслуговують IT-інфраструктуру для інших компаній. Проте, іншим сферам також може знадобитися захист своєї відповідальності, у тому числі бухгалтерам, ретейлерам, страховим агентам. Претензії щодо стороннього покриття можуть бути викликані звинуваченнями в тому, що вашому бізнесу не вдалося запобігти поширенню вірусу або розкриттю конфіденційної інформації.

Також страхування від кібер-страхування може включати, за домовленістю сторін, оплату: адвокатських витрат; врегулювання або рішення проти вашого бізнесу; державні штрафи і пені; захист перед регулюючими органами.

Страховий захист кібер-ризиків ще не набув чіткої стандартизації страховій галузі, тому термінологія покриттів може відрізнятися. Тим не менш, є кілька покриттів, які користуються найбільшим попитом серед клієнтів, які вирішили придбати поліс покриття кібер-ризиків. В таблиці 2.1 вказано перелік найпоширеніших покриттів, вказано, що кожен з них покриває, і чи є це покриттям первинним або страхуванням кібер-відповідальності перед третьою особою.

Яке покриття має ваша кібер-страховка, залежить головним чином від того, що ваш страховик готовий вам запропонувати. В сучасних реаліях, лише в деяких випадках страховик може дозволити вибрати один з цих або інших варіантів покриття, більшість «провайдерів» страхових послуг можуть обмежуватись лише одним видом покриття. Це знову ж таки підтверджує необхідність вміти правильно аналізувати свої потреби в захисті, аналізувати запропоновані вам страхові продукти, мати розуміння об’єктів ризику та вміти зіставити запропоновані варіанти. Це дозволить максимально ефективно використати ваші інвестиції в страховий кібер-захист.

Таблиця. 2.1

Види страхового покриття кібер-ризиків

Типи покриття	**Що покриває?**	**Пряме покриття або покриття кібер-відповдальності?**
Переривання бізнес-процесу	Втрата доходу від бізнесу через кібератаки	Пряме покриття
Комп'ютерне шахрайство	Покриває крадіжку грошей, цінних паперів та інших форм матеріального майна за допомогою комп'ютерного шахрайства і схем соціальної інженерії	Пряме покриття

Продовження табл. 2.1

Типи покриття	Що покриває?	Пряме покриття або покриття кібер-відповдальності?
Страхування від витоку даних	Заяви про нездатність захистити особисту інформацію (PII) і захищену медичну інформацію (PHI) клієнтів	Обидві
Матеріальна шкода	Вартість заміни комп'ютерів, пошкоджених кібератакою	Пряме покриття
Крадіжка особистих даних	Витрати, пов'язані з власником бізнесу або його співробітниками після крадіжки особистих даних	Пряме покриття
Реклама та шкода завдана репутації третьої особи	Збиток, спричинений дифамацією на веб-сайті або в соціальних мережах	ПКВПТО
Передача вірусу або шкідливого контенту	Нездатність зупинити передачу комп'ютерного вірусу або шкідливого контенту	ПКВПТО
Помилки та пропуски	Втрата, викликана нездатністю забезпечити належну безпеку мережі	ПКВПТО

Аналізуючи інформацію про існуючі страхові продукти в сфері кібер-ризиків, на основі порталу Insurance statistics [18], стало зрозуміло, що станом на жовтень 2019 року витрати на кібер-страхування варіюються в широких межах. Звісно, в основному на дельту коливань впливає залежність від ступеня ризику, з яким стикається ваш бізнес. Аналізуючи доступну інформацію, можна зробити висновок, що невеликий бізнес, який працює з зберіганням даних, але має відносно невелику кількість клієнтів, може розраховувати на вартість страхового захисту від кібер-ризиків в межах від 800 до 2000 доларів на рік. Для великого бізнесу, який отримує великі доходи, працює з великою кількістю клієнтів, обробляє масивні об’єми даних може розраховувати на плату від 2000 доларів до 8000 доларів на рік.

Розглядаючи дані Американського ринку страхування кібер-ризику , який зараз є найбільш відкритим у в плані доступу до інформації в даній галузі страхування, сформована таблиця 2.2 «витрати на страхування кібер-відповідальності за галузями»

Таблиця 2.2

Витрати на страхування кібер-відповідальності за галузями

Галузь бізнесу	Річний дохід	Страхова сума	Типова щорічна страхова премія
IT-провайдер в сфері охорони здоров'я	500 000$	1 мільйон доларів	1000-2500$
Медична клініка	400 000$	1 мільйон доларів	1200-3000$
Бухгалтерія/податкова підтримка	100 000$	1 мільйон доларів	1200-3000$
Невеликий роздрібний магазин	250 000$	1 мільйон доларів	1000-2500$

Побудовано автором на основі [19]

Витрати на страхування кібернетичної відповідальності малого бізнесу, як правило, починаються з 1000 доларів США за ліміт покриття в 1 мільйон доларів. Однак ряд факторів, в тому числі дохід і кількість, об’єми масивів особистих даних, можуть підняти щорічну плату страхових премій до більш високого рівня ціни, близько 7500 доларів США для підприємств усіх розмірів. Малі підприємства, основною діяльністю яких є обробка даних більших фірм, компаній, можуть зіткнутися зі значно більш високими ризиками, а відповідно і витратами - іноді до 40 000 доларів на рік.

Страхування відповідальності по кібер-ризикам є відносно новим продуктом. Саме тому страховики, які пропонують його, самостійно розраховують тарифи, пропонують покриття, зазвичай використовують свої

власні формули, використовують специфічні андеррайтерські підходи, які не мають аналогів. Як результат таких специфічних умов творення нового продукту - премії можуть сильно відрізнятися в різних страхових компаніях. Брокерська компанія HardFort рекомендує при укладанні договорів з страхування кібер-ризків, спочатку отримати передстрахову оцінку, оцінити варіант покриття, об'єми страхових премій, як мінімум, від трьох страховиків, щоб переконатися, що ви знайдете покриття кібер-страхування, яке буде оптимальним для ваших операцій і ведення бізнесу в цілому, а також не змусить вас переплатити.

Також для вибору оптимального розміру стразових премій по страховим договорам в цій сфері, слід звернути свою увагу на розмір франшизи. Вибір більш високих франшиз означає більш низькі преміальні витрати. Після того, як ви і ваш агент або брокер визначили ступінь свого найбільшого ризику, ви вирішите подумати про те, яку фінансову відповідальність може собі дозволити ваш бізнес. Слід відрегулювати свої франшизи до максимально можливого рівня, який ви зможете заплатити в разі злому даних. [19]

Кібер-страхування - це хороша інвестиція для зниження вартості кібер-атак після того, як вона вже сталася. Проте, в першу чергу прийняття активних заходів може значно знизити шанси стати жертвою. А по-друге, страховики часто винагороджують компанії з хорошим управлінням ризиками і ті компанії, які мали в своїй історії лише декілька випадків кібер-інцидентів більш низькою премією.

Проводячи аналіз ринку страхування кібер-ризику, було проаналізовано обсяги страхових премій. Однією з найперших компаній, яка презентувала страхування кібер-ризиків серед своїх продуктів і зараз займає одну з лідируючих позицій в цій сфері за своїми преміями є компанія AIG. Дивлячись на звіти компанії, наочно стає зрозуміло якої швидкості і темпів набирає страхування кібер-ризиків в наші дні. Зростання обсягів страхових премій в цій сфері сягає неймовірних показників. Лише за один 2017 рік

обсяг попиту в сфері кібер-страхування став більшим в 2 рази ніж за 2013-2016 роки разом. А 2016 рік показав зростання в більш ніж половину в порівняно з 2013-20015 р. сумарно.

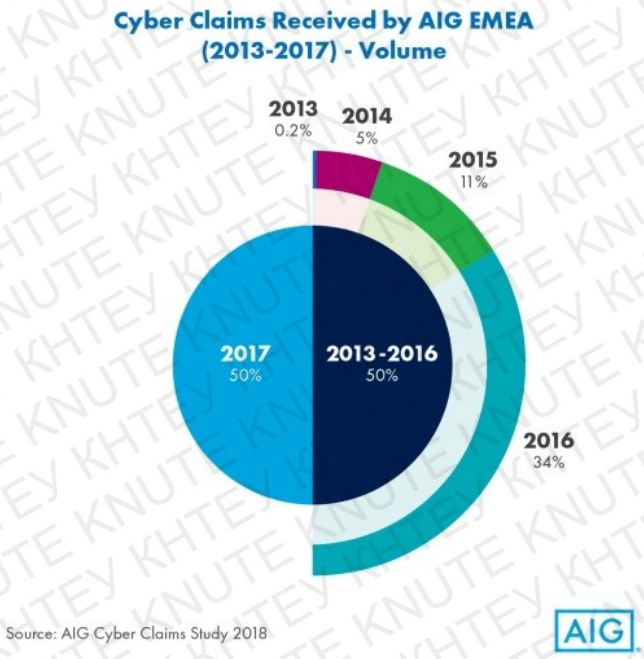


Рис. 2.3 Отримані запити щодо кібер-страхування [20]

Аналізуючи звіти компанії видно, що потреби в розвитку галузі страхування кібер-ризиків, кібер-відповідальності збільшує свої темпи в геомертричній прогресії. 2018 рік став знову рекордним і показав збільшення стосовно 2017 року майже в 2 рази. (рис. 2.4)

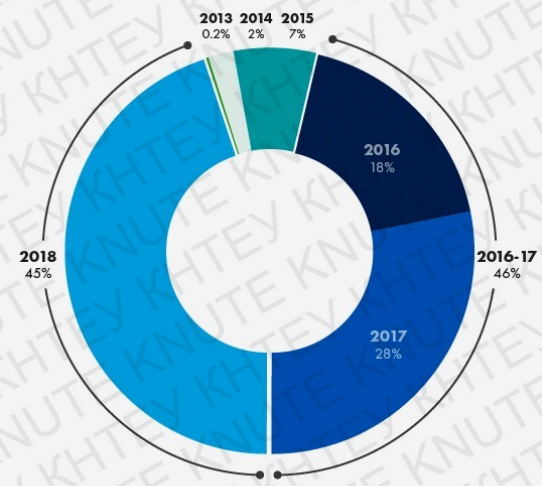


Рис. 2.4 Попит на страхування кібер-відповідальності за звітами AIG 2013-2018 р.

Порівнюючи статистичну інформацію, яку надала компанія AIG, можна відслідкувати пряму відповідність до зростання світових страхових премій у сфері кібер-страхування.

Опитування у 2016 р. показало, як швидко зростають обсяги премій кібер-страхування. Інвестиції склали 2,5 млрд $ у 2015 р. Страхові премії сягнули 4,3 млрд $ у 2017 р. Експерти очікують, що до 2020 р. об'єми сягнуть 7,5 млрд $. До опитування було включено понад 10000 керівників компаній з 127 країн. [21] Очікується, що премії по кібер-страхуванню в глобальному масштабі до 2025 р. досягне 20 млрд $. [22] У 2018 р. премії по кібер-страхуванню в США зросли приблизно на 10% у річному обчисленні до 2,03 млрд $. Загалом 184 страховика повідомили про отримання деяких премій по страхуванню кібер-ризиків у 2018 р. Цей показник збільшився на 14 страховиків за 2017 р, у т. ч. 21 новий страховик, який мав програму з кібер-страхування і отримував премії, став частково компенсований через злиття та поглинання. [23]

Вищенаведене свідчить, що кіберстрахування швидко стає стандартним компонентом стратегії кібербезпеки. Як показують попередні статистичні дані, майже кожна компанія є вразливою до атак, і навіть компанії, що мають надійну кібербезпеку, не є цілком захищеними. Кіберстрахування забезпечує останню лінію захисту, покриваючи витрати, пов'язані з порушеннями та іншими інцидентами.

На основі наведених даних побудовано таблицю зі значеннями сум страхових премій за кожен рік, починаючи з 2013 (табл. 2.3). Використовуючи дану таблицю, спрогнозовано об'єми страхових премій для 2020-2025 років (табл.2.5) .

Таблиця 2.3

Страхові премії за 2013-2019 роки

X	**Сума страхових премій**	1,3	1,84	2,5	3,1	4,3	5,5	6,7
Y	**Рік**	2013	2014	2015	2016	2017	2018	2019

На основі величини достовірності апроксимації (R^2), яка характеризує наскільки добре лінія тренда описує початкові дані, було виявлено, що даний прогноз має поліноміальний тренд (рис. 2.5). Оскільки за поліноміальним трендом показник R^2 був найбільшим для зміни показників страхових премій за 2013-2019 роки. (табл. 2.4)

Таблиця 2.4

Найбільший показник величини достовірності апроксимації (R^2)

Тип тренду:	Формула:	Величина достовірності апроксимації (R^2):
Лінійний	$y = 0{,}9043x - 1819{,}4$	$R^2 = 0{,}9719$
Експоненсіальний	$y = 2E\text{-}239e^{0{,}2733x}$	$R^2 = 0{,}9944$
Логарифмічний	$y = 1822{,}9\ln(x) - 13867$	$R^2 = 0{,}9718$
Поліноміальний	$y = 0{,}0857x^2 - 344{,}7x + 346545$	$R^2 = 0{,}9981$

Рис. 2.5 Поліноміальна лінія тренду

Використовуючи поліноміальне рівняння лінії тренду $y = 0{,}0857x^2 - 344{,}7x + +346545$, знайдемо прогнозовані значення для 2020-2025 років.

Таблиця 2.5

Прогнозні обсяги страхових премій кібер-ризику 2020-2025 роки

X	**Сума страхових премій**	8,2	9,9	11,6	13,7	16	18,4
Y	**Рік**	2020	2021	2022	2023	2024	2025

РОЗДІЛ 3 Проблеми та перспективи розвитку страхування кібер-ризиків

3.1 Страхування кібер-ризиків в Україні

Кіберзлочинність давно стала поза межами кордонів, втратила національність і зламала мовні бар'єри. На американські енергетичні підприємства здійснюють атаки громадяни Нідерландів, Канади та Великобританії, а в останніх атаках на стратегічні об'єкти України фахівці відзначають російський слід. Можна отримати віддалений доступ до інфраструктури обленерго і відключити електропостачання в регіоні на період до 8 годин, використовуючи методи соціальної інженерії, як це сталося з «Прикарпаттяобленерго» 23 грудня 2015 р.

З кібер-злочинністю борються спеціалізовані державні органи, об'єднуючись у цій боротьбі з іншими організаціями та навіть цілими державами. Наочний приклад такої співпраці - затримання організатора кіберзлочинністі угруповання Avalanche в Полтаві. В операції брали участь правоохоронці з 41 країни і представники Європолу. [24]

В останні кілька років суттєво збільшилася кількість кібератак на українські організації. Метою хакерів стають не тільки державні інститути і підприємства, а й приватний сектор, вдаривши по якому, зловмисники розраховують підірвати фінансову систему країни або отримати грошову вигоду. Прикладом такого інциденту була атака на український банк (назва якого не розголошується з міркувань конфіденційності) через систему SWIFT, про що повідомляється в телеграмі НБУ №56-0031/37708, в результаті якої банк втратив $ 10 млн. [25]

Крім того, у звіті з інформаційної безпеки в 2016 році компанія Cisco повідомляє, що більше половини опитаних українських компаній піддавалися кібератакам.

У світлі зростання кількості і серйозності кібер-злочинів ризик-менеджмент організацій змушений внести до свого списку ще одну небезпеку для бізнесу і держави, на яку раніше закривали очі. Хакерські атаки стали реальністю сьогоднішнього дня. З даними ризиками необхідно працювати і шукати шляхи їх оптимізації.

Для таких цілей існує три основних напрямки: технологічні рішення безпеки, просвітницька робота в сфері протидії та профілактики кібер-злочинів, а також кібер-страхування.

В останні роки інструмент кібер-страхування набув значного поширення на міжнародному ринку. І зараз його пропонує понад 60 страхових компаній по всьому світу. Однак для українського ринку це все ще необізнаний сектор.

Завданням кібер-страхування є захист від великомасштабної хакерської атаки. Цей вид страхування забезпечує фінансовий механізм відновлення після великих збитків, допомагаючи підприємствам повернутися до нормального функціонування, збереження стабільності, платоспроможності і зниження втрат в результаті перерви у виробництві.

Свою популярність в розвинених країнах кібер-страхування отримало завдяки розумінню того, що, впроваджуючи новітні рішення в сфері кібер-безпеки і проводячи постійну роботу з персоналом, завжди залишається той 1% ризику компрометації системи, який неможливо передбачити і оцінити. Власне, на цьому етапі і вступає в справу кібер-страхування, яке характеризується широким спектром покриттів і захищає компанії від фінансових втрат в результаті DDoS атак, фішингу, зараження шкідливим програмним забезпеченням, відповідальності за зберігання конфіденційної інформації і персональних даних.

Результати настання кібер-ризиків можуть розглядатися з позиції видів завданих збитків (фінансовий і майновий) та суб’єктів наслідків їх реалізації (1-ша особа, 3-тя особа), наведені на рисунку 3.1.

	Першої особи	*Третьої особи (3-ті особи можуть вимагати):*
Фінансові збитки	✓ Витрати на реагування (IT-розслідування, повідомлення клієнтів) ✓ Юридична допомога: консультації і захист від вимог третіх осіб ✓ PR: мінімізація репутаційного збитку ✓ Втрата прибутку через падіння системи/хмари ✓ Витрати на відновлення даних ✓ Кібер-шантаж (зняття загрози) ✓ Інтелектуальна власність	✓ Втрачену внаслідок кібер-інциденту вигоду; ✓ Витрати на відновлення ✓ Витрати на юридичну допомогу ✓ Збитки від втрати даних (персональні та інші) та інші фінансові втрати ✓ На них можуть бути накладені штрафи та санкції
Майнові збитки	✓ Крадіжка активів ✓ Поломка машин внаслідок кібер-інциденту ✓ Знищення або збиток будівлям/спорудам або іншому майну ✓ Перерва у діяльності (зупинка виробництва через фізичний збиток майну внаслідок кібер-інциденту) ✓ Збиток здоров'ю працівників	✓ Крадіжка активів третіх осіб ✓ Поломка машин третіх осіб внаслідок кібер-інциденту ✓ Знищення або збиток будівлям/спорудам або іншому майну 3-х осіб ✓ Шкода навколишньому середовищу ✓ Збиток здоров'ю третіх осіб

Рис. 3.1 Класифікація наслідків кібер-ризиків [26]

Важливо те, що під покриття потрапляє перерва у виробництві і втрата прибутку в результаті згаданих інцидентів. Крім того, страхові компанії пропонують такі додаткові умови:

- відшкодування витрат на розслідування кібер-злочинів;
- антикризовий піар з метою відновлення репутації;
- витрати на захист в суді;
- відновлення роботи IT-систем.

На даному етапі український страховий ринок істотно відстає від своїх західних колег у питанні розробки і впровадження продукту кібер-страхування. Цікаво й те, що міжнародні гравці, як брокери, так і страхові компанії, представлені в Україні, маючи готові варіанти програм захисту від кібер-ризиків, не поспішають пропонувати його українському бізнесу.

Досліджуючи ринок кібер-страхування в Україні, стало зрозуміло, що абсолютна більшість страховиків говорить про запровадження програм з кібер-страхування лише з метою піару страхової компанії, для створення враження інноваційності, стабільності і готовності до розвитку компанії. Реальне існування договорів з кібер-страхування можуть підтвердити лише кілька страхових компаній, кількість яких, нажаль, не буде перевищувати 5.

В основному це масштабні світові компанії, які вже мають чіткі алгоритми роботи з оцінкою, визначенням ризику і мають напрацьовану процедуру визнання страхової події та шляхи її врегулювання.

З цього приводу існує дві точки зору.

1. На тлі загальної економічної стагнації акціонери не бачать перспективи і обсягу ринку, який міг би їх зацікавити.

2. Акціонери вважають український портфель занадто високо-ризиковим.

У будь-якому випадку, керівники і власники міжнародних страхових компаній досить обережні і консервативні, до того ж часто страждають від високого рівня бюрократії в ухваленні рішень, тому вони не скоро вийдуть на наш ринок з продуктом кібер-страхування.

У такій ситуації виходом може стати схема фронтінг, згідно з якою мінімальна частка ризику (1-2%) утримується локальним страховиком, а інша, найбільша частина передається закордонному партнеру. У свою чергу, такий партнер здійснює оцінку ризику і надає умови страхування і бере участь у врегулюванні збитків. Перевага цієї схеми - той факт, що клієнт отримує вже перевірений і відпрацьований на практиці страховий продукт, а також гарантії стабільності закордонного учасника, підтверджені, як правило, міжнародними рейтингами. Цей метод дає шанс українським компаніям отримати професійний якісний захист в разі найгіршого з можливих і неможливих сценаріїв.[27]

За словами фахівців в сфері кібер-безпеки, всі компанії діляться на дві частини: ті, які знають, що їх зламали, і ті, які ще не знають, що їх зламали.

Нажаль, навіть з урахуванням зростаючого інтересу до напрямку страхування кібер-ризику, страховики нерідко підміняють клієнтам мету і можливості такого виду страхування. В реаліях українського страхування, нерідко клієнти страхової компанії, часто не без допомоги консультантів страховика, вважають, що IT-страхування захищає від загроз інформаційної безпеки або від втрати даних. Проте, це хибна думка. Збереження цінної для компанії або для клієнта інформації — це або їхня власна турбота, або

проблеми тих, кому вони цю інформацію передали та довірили. На превеликий жаль, ризики того, що ці дані буде втрачено, збільшуються з кожним роком.

В сучасних умовах слід реально оцінювати наслідки ймовірної втрати даних. Існує ризик втратити репутацію на ринку через розголошення комерційної, банківської або адвокатської таємниці. Можна постійно платити зламникам, які будуть відновлювати ваш ресурс на якийсь час, а потім знову вимагати гроші. Наприклад, так робила вже відома дівчина-хакер із Черкас, яка тричі одержувала "викуп" від одного з найбільших міжнародних сервісів онлайн-знайомств, щоб відновити його працездатність. Нарешті, можна втратити частину електронних документів або ключів, а разом з ними можливість вести операційну діяльність компанії.

Сьогодні попит на страхування кібер-ризиків створюють не потенційні жертви хакерських атак, а самі страхові компанії. Часто фірми, навіть усвідомлюючи необхідність і користь такого сервісу, поки що не впевнені, що саме хочуть страхувати, і чи справді потім хочуть одержати те саме відшкодування. [28]

Аналізуючи сучасні можливості послуг з страхування кібер-ризиків можна провести чітку порівняльну паралель з програмами страхування автомобільної сфери. Програми кібер-страхування пропонують у вигляді 2 основних об’єктів страхування.

Першим об’єктом страхування виступає відповідальність страхувальника перед третьою особою, як, наприклад, це відбувається при обов’язковому страхуванні цивільної відповідальності перед третьою особою. Даний вид страхування покриває витрати страхувальника понесені у зв’язку з претензією

третіх осіб, через матеріальну або моральну шкоду понесену в зв'язку з настанням кібер-ризику, наприклад, через виток даних клієнтів, корпоративної інформації компанії партнера.

Другим об'єктом програми страхування від кібер-ризиків, яка є найбільш розповсюдженою в Україні, це страхування від збитку, який понесе страхувальник у зв'язку з власними витратами, які він понесе через переривання робочого процесу. Цей напрямок страхування можна порівнювати з страхуванням по КАСКО. Коли клієнту відшкодовуються матеріальні збитки, які він поніс внаслідок завдання йому шкоди від третіх осіб, стихійних лих, непередбачених ситуацій тощо. Більша поширеність цього напряму страхування пов'язана з більшою прозорістю розрахунків можливих втрат та визнання події, такою що відповідає ознакам кібер-інцидента.

Загалом розвиток кібер-страхування в Україні має повільний темп. Це спровоковано наступними причинами:

По-перше, недостатня обізнаність клієнтів. Це, у свою чергу, створює ефект штучного заниження потреб населення, коли страхові компанії проводять аналіз попиту на продукти кібер-страхування. Процес оцінки ризик-менеджменту інформаційної безпеки страхувльника описаний в додатку В.

По-друге, недосконаліть розрахунків експертів. У страхових компаній поки немає розуміння технічної специфіки страхування інформаційних ризиків. Для проведення даного технічного аудиту інформаційної безпеки в компанії, страховику треба зробити дуже серйозне дослідження.

По-третє, навіть якщо страхова компанія залучає сторонню організацію для андеррайтингу, то, скоріше за все, перевірити рівень якості оцінки теж не завжди представляється можливим.

На думку Н. Приказюк, основними проблемами, що стримують розвиток кіберстрахування, є (рис 3.2):

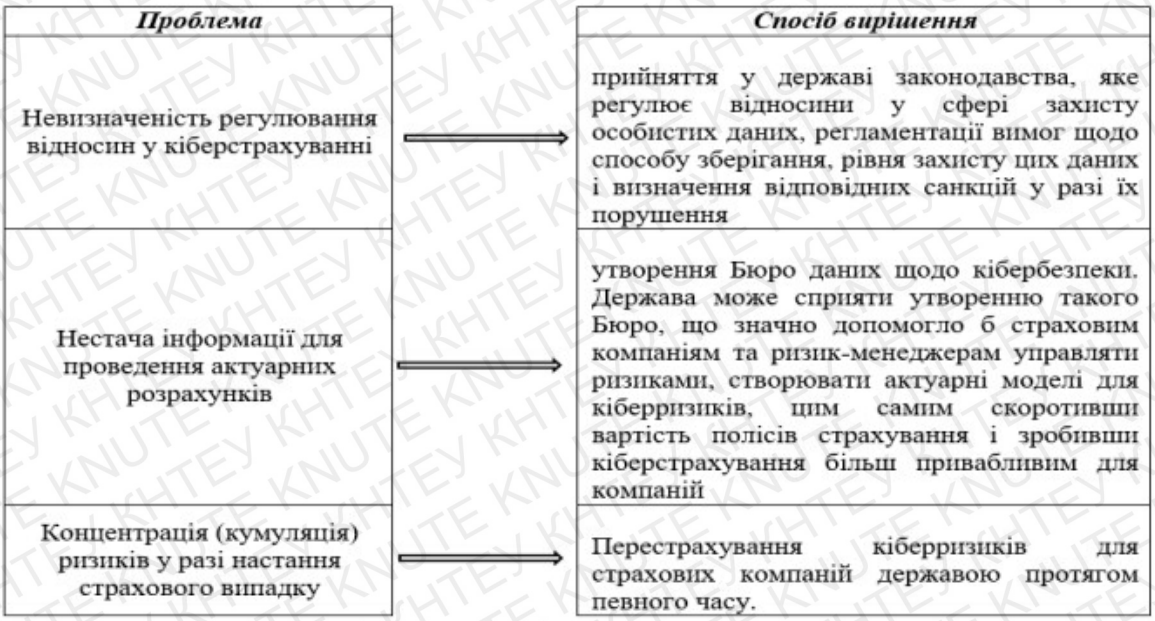


Рис. 3.2 Проблеми, що стримують розвиток кібер-страхування та способи їх розв’язання [29]

На даний момент страхові компанії в нашій країні, готуючи пропозицію для клієнта, оцінюють ризики компанії за допомогою непрямих ознак і характеристик. Фахівці вивчають, як в компанії вирішуються питання з управління ризиками в цілому; яка філософія управління в організації; як зберігаються дані; проводить компанія тестування систем інформаційної безпеки і аудити; які існують в компанії звітності та профілактичні дії, а також оцінюють розмір штату в IT.

Цей підхід має право на життя і дає прийнятний результат. Але очевидно, що найближчим часом почнуть формуватися більш детальні методики, які все-таки будуть відповідати на пряме запитання щодо оцінки ризиків кібер-страхування. В ідеалі договір страхування повинен містити в собі додатки, які прописують зобов'язання страхувальника щодо проведення ряду робіт на регулярній основі.[30]

На відміну від автострахування, де об'єктом є автомобіль і де збиток, пов'язаний з ним, можна прорахувати заздалегідь залежно від його моделі, року випуску та марки, об'єктом кібер-страхування, по суті, є сам бізнес. А

після витоку інформації або зламу інформаційної системи не кожна компанія захоче розголошувати навіть сам факт того, що сталося. Причин кілька. З одного боку, бувають випадки, коли реалізована атака завдасть мільйонного збитку, а розголошення факту зламу — зруйнує мільярдний бізнес. З іншого — для багатьох компаній, наприклад комерційних банків або держустанов, втрата даних клієнтів — це порушення закону.

Наступним питанням, що поставить собі потенційний клієнт страхової, буде оцінка втрат, як прямих, так і непрямих. А для того, щоб застрахувати себе від цих втрат якісно, потрібно цю оцінку здійснювати не постфактум, а перед укладанням договору про страхування. Особливо це складно для представників бізнес-підрозділів і власників підприємств, які багато років сприймали інформаційну безпеку як видаткову та не завжди потрібну складову. Тепер же їм доводиться визнати вже не тільки якісну, а й кількісну ефективність і важливість інформаційної безпеки у своїй компанії.

Найбільш зрозумілими з погляду підрахунку збитків і витрат є, звичайно, штрафи, якими погрожують міжнародні регулятори у разі втрати персональних даних клієнтів відповідно до вимог міжнародних та європейських стандартів на кшталт PCI DSS (Payment Card Industry Data Security Standard) або GDPR (General Data Protection Regulation), що набирає популярності. Це торкнеться перш за все великих фінансових організацій, ритейлерів, сервісних компаній.

Ще одна причина, яка зупиняє вітчизняні страхові компанії в розвитку кібер-страхування – це не зрілість законодавчої бази в сфері інформаційної безпеки та розслідування інцидентів, пов'язаних із нею. Саме тому досвід у сфері зосереджений у глобальних гравців в США, які вже продумали страхові продукти, набили перші гулі, а дехто вже навіть сформував власні групи ризик-інженерів, як аналоги аварійних комісарів у автострахуванні.

В Україні, як, власне, і в усій Східній Європі, кіберстрахування для страховиків і брокерів — сфера нова та незрозуміла. Тому основна частина компаній, які намагаються розпочати діяльність у цьому напрямі, не

розробляють універсальних продуктів, а працюють індивідуально для кожного клієнта. Таких клієнтів поки що небагато. Складність такого підходу не тільки в оцінці ризиків і формуванні тарифу, а й у перестрахуванні таких ризиків у зарубіжних партнерів. Зарубіжні компанії, вже маючи певний досвід, висувають свої конкретні вимоги щодо заходів оцінки захищеності клієнта.

Таку оцінку можна отримати миттєво, онлайн, на сайті глобальних страхових груп, відповівши на ряд простих запитань (більш детально буде розкрито в розділі 3.2).

З огляду на незрілість нашого законодавства при розслідуванні інцидентів виникає чимало запитань. Логічно, що страховики потребують документального підтвердження, підтвердження настання "випадку".

Поки що цей процес виглядає для страховиків виглядає «розмито». Якщо провести паралель с автострахуванням, то процес страхування кібер-ризику набував би такого вигляду: страхувальник дає автовласнику заповнити анкету, клієнт пише, що в нього машина в ідеальному стані. Через якийсь час він потрапляє в ДТП і заявляє збиток. Тут виникає запитання: а чи так усе добре було до аварії? Такі міркування підштовхують страховиків як мінімум на даному етапі займатися найпростішими питаннями. Тобто страхувати на певну суму грошей у разі певної події. Або страхувати від конкретних штрафів, які застосовуються будь-якими міжнародними регуляторами (наприклад, від витоку даних власників банківських карт).

Страховий тариф, відповідно, теж застосовується не оптимізований, а той, який враховує й дороге перестрахування, і локальні ризики.

Як вже зазначалося раніше, більшість потенційних вітчизняних страхувальників задовольняють свої потреби в кібер-страхуванні через інші програми. Наприклад для банківської сфери популярним договором страхування є включення так званого BBB страхування.

Українські страхові компанії намагаються не розкривати дані про свої продукти кібер-страхування. По-перше це пояснюється небажанням ділитися

з конкурентами малодослідженою інформацією, а по-друге, як пояснюють експерти з кібер-захисту, така інформація може стимулювати додатковий інтерес зловмисників на протиправні дії проти страхувальників. Через це в відкритому доступі бракує статистичної інформації.

Дякуючи за надану інформацію провідними експертами, які працюють над розробкою нових страхових договорів, проаналізовано нову розробку відчизняної страхової компанії «Альфа-страхування», в якому зазначені умови страхування кібер-ризику, та види можливих покриттів для базового та повного пакету (додаток Г). Базовий пакет включає втрату даних та перебої роботи мережі.

Передстраховий аналіз для базового пакету включає:

- Стрес-тест (від 3 робочих днів).
- Мережева розвідка афілійованих мережевих ресурсів.
- Автоматизоване сканування вразливостей.
- Ручна експлуатація виявлених вразливостей.
- Тестування навантаження критичних ресурсів.
- Підготовка короткого звіту про ступінь захищеності інформаційних активів компанії, доступних ззовні.
- Експрес-тест (1 повний робочий день).
- Автоматизоване сканування вразливостей Підготовка довідки про захищеність компанії.

Передстраховий аналіз для повного пакету включає:

- Визначення можливих загроз.
- Розробка сценаріїв найбільш вірогідних збитків.
- Рекомендації по підвищенню рівня захищеності і відвертанню можливих збитків.
- Розробка інструкцій по діях у разі надзвичайних ситуацій.
- Визначення можливого впливу кибер-рисков на виробничу діяльність Розрахунок фінансових показників і можливих збитків.
- Підготовка звіту.

Етапи роботи по врегулюванню збитків виділяють такі:

1. Термінове реагування на виникаючі загрози (припинення дій, рекомендації по мінімізації збитку).
2. Розслідування обставин і причин збитку, пошук винуватця.
3. Юридичний аналіз, визначення факту настання страхового випадку Залучення авторитетних юристів у разі потреби. Розрахунок розміру збитків, яких зазнали.
4. Оцінка перспектив суброгування і сприяння в реалізації вимоги.
5. Підготовка звіту з рекомендацією по врегулюванню і узгодження результатів із страховим ринком.

Як асистуючу компанію, вирішили залучити міжнародну компанію LABB. LABB - міжнародна компанія, що спеціалізується в області незалежного розслідування і врегулювання збитків. Має можливість надання сюрвеерских і аджастинговых послуг у більш ніж 140 країнах світу.

Проводячи аналіз українських страхових компаній, нажаль виявилось, що багато страхових компаній проводило роботу в напрямку створення договорів з страхування кібер-ризику, проте, дані розробки не були затверджені керівництвом.

Доволі рано розглядати кібер-страхування в українських реаліях, оскільки його впровадження на даному етапі розвитку страхового ринку України є неможливим, що, в першу чергу, зумовлено відсутністю потужно капіталізованих страховиків, здатних прийняти такі ризики на страхування. По друге, відсутня нормативна база, що визначає природу кібер-ризиків, можливість та умови їх страхування, зокрема, жодна компанія не має ліцензії на такий вид страхування. По третє, вітчизняні страховики ще не мають у своєму розпорядженні методик оцінки даного ризику, що унеможливлює встановлення ціни страхового захисту. І

четверта, мабуть основна причина – відсутність платоспроможних страхувальників, які можуть дозволити собі придбати доволі недешеву програму страхування від кібер-ризиків. [26]

На сучасному етапі функціонування вітчизняного страхового ринку лише деякі страхові компанії можуть запропонувати якісний страховий захист від кіберзлочинності (кібер-ризиків). Відсутня необхідна статистика, законодавча база, судова практика. Недостатньо і кваліфікованих фахівців, що мають уявлення про даний вид ризику та його структуру [31].

3.2 Зарубіжна практика страхування від кібер-атак

На відміну від мало розвинутого Українського ринку кібер-страхування, який тільки робить свої перші кроки, закордоном кібер-страхування бере свій початок наприкінці 1990-х років в США.

Деякі програми страхували засоби масової інформації, або якісь інші помилки в обробці даних. На початку 2000-х договори щодо засобів масової інформації в інтернеті почали покривати: несанкціонований доступ, захист мережі, втрату даних та проблеми, які завдані комп'ютерними хробаками чи комп'ютерними вірусами. Проте, такі договори мали багато винятків. Наприклад вони не покривали збитки спричинені в наслідок халатності або необережності працівників, не відшкодовували штрафи.

У той же час деякі договори, які були пов'язані з звхистом програмного забезпечення, почали розвиватися, додавши до своїх умов субліміти при помилках програмного забезпечення.

Крім того, договір страхування кібер-ризиків зазвичай не передбачав знайомі нам сьогодні покриття. У середині 2000-х умови страхування розвивались у відповідь на кіберзагрози, які були на той момент. З’являються договори, які починають охоплювати такі ризики, як: переривання бізнес процесу, вимагання (фішингові атаки), пошкодження даних в мережі.

Протягом цього періоду, в історії кібер-безпеки слід відмітити, що в 2003 р. вступив в силу закон Каліфорнії про порушення безпеки данних. Це справило значний вплив на розвиток кібер-страхування. Компанії, які працювали на території країни, тепер повинні були надсилати повідомлення про порушення безпеки персональних даних сторонніми особами, всім постраждалим мешканцям.

Перші договори страхування кібер-ризиків були укладені ще у 2010–2011 роках. Цю тему обговорювали на щорічному форумі в Давосі у 2012 році. Але активне зростання цього виду страхування почалося декілька років

по тому, після масових зламів корпоративних і урядових ресурсів у США. Тому 90% ринку страхування кібер-ризиків припадає саме на США. [11]

У 2010-х роках кількість страховиків зі своїми власними продуктами страхування кібер-ризиків виросла до більш ніж 50. Сьогодні це більше 60, а великі збиткі та кількість порушення стали більш поширеними.

Галузь кібер-страхування постійно змінюється, і ціновий діапазон широкий, оскільки договори страхування кібер-ризиків повинні швидко адаптуватися до потреб ринку. Один страховик може запропонувати широкий асортимент покриттів, а інший формує більш обмежену пропозицію послуг, як і вартість страхових премій в 2- 3 рази меншу. [32]

Оскільки ринок кіберстрахування протягом багатьох років постійно зростає, кількість страховиків та різноманітність доступних покритів значно розширилися. Наявність більшої кількості варіантів для вибору забезпечує поліпшення конкурентних цін та їх налаштування під різні потреби страхувальників. Серед зарубіжних страховиків можна виділити топ-10 найкращих та найнадійніших.

Allied world insurance. Протягом 2016 р. ця компанія уклала договори на $32, 533,000 в преміях, який складає 2.4 % в галузі в світі. Компанія обіцяє забезпечити комплексні рішення для клієнтів в сфері віртуальних страхових послуг SRVS.

Liberty mutual insurance. Впродовж 2016 ця компанія підписала договори на $34, 343,000 в преміях, зайняв 2.6 % частки ринку. Liberty Mutual запропонувала договор, який розроблений для потреб малих і середніх підприємств.

AXIS Capital Holdings Ltd. Ця компанія підписала договори на $50, 273,000 в преміях протягом 2016 і має 3.7% ринку. Компанія обслуговує широку різноманітність клієнтів, але значною мірою договори спрямовані на IT компанії.

Blue Cross Shield company. Ця компанія володіє 4.1% премій на ринку, що складає $55, 411,000. Компанія пропонує захист проти ризиків,

починаючи від загубленого девайсу до кибер-атак, з покритям відповідальності та покриттям особових втрат.

CNA Financial corp. У 2016 Фінансова корпорація CNA підписала договори на $68, 476,000 в преміях і володіла 5.1% ринку кібер-страхування. Має широкий ряд доступних покриттів від специфічних загроз і уразливостей.

Beazly insurance corp. Впродовж 2016 р. головний страховик кібер страхування уклав договори на $83, 908,000 в преміях і займав 6.3% ринку. Beazley Co. пропонує всебічне покриття, від найбільш популярних ризиків та витікаючих, нових відів ризику з них.

Trevelers companies inc. Ця компанія знаходиться в топ п'ять страховиків з $92, 198,000 в преміях і займає 6.9 % ринку. Компанія одна з тих, хто пропонує найбілше і найрізноматінніші покриття, діапазони можливості яких охоплюють покрита від найменших до найбільших бізнесів.

Chubb Ltd. Chubb уклав 10% всіх кібер-страхових премій в 2016, сумарно на $133, 599,000. Страховик пропонує ряд унікальних покриттів, як для найменших так і для великих підприємств.

XL Groupe Ltd. Після укладання договорів на $160, 809,000 в преміях в 2016 р. і займає до 12% кібер-страхового ринку.

American international grope (AIG). Безумовно найбільший постачальник віртуального страхування - AIG з $228, 325,000 в преміях, і 17% ринку. Компанія запропонована продукт під назвою CyberEdge, який обіцяє забезпечити комплексне рішення з управління кібер-ризиком.[33]

Дивлячись на проблеми кібер-страхування в нашій країні, а саме аналіз ризиків та розрахунки тарифів, слід перейняти закордонний досвід компаній.

Лідери галузі кібер-страхування розробили онлайн додаток для швидкого прорахунку ризиків та їхніх обсягів. Програма, на основі заповненої анкети, відповідно до потреб клієнта, надасть найбільш оптимальний варіант покриття. Анкета міститься у додатку Д. Проте, не дивлячись на те, що програма користується великим попитом та добре себе

зарекомендувала в експрес оцінці, вона також не враховує всі фактори ризиків.

Іншуртех-стартап «Coalition» запустив безкоштовний загальнодоступний інструмент оцінки кібербезпеки і ризиків для малого і середнього бізнесу Cyber Risk Assessment Tools, який оцінює очікувану вірогідність і серйозність інциденту безпеки для компанії. Сьогодні Coalition Cyber Risk Assessment об'єднує інструменти страхування і кібербезпеки, щоб допомогти компаніям управляти і знижувати кіберриски. За підтримки страхових компаній з рейтингом A+/A таких, як Swiss Re, Lloyd's of London і Argo Group, стартап надає страхове покриття від кіберрисков до $15 млн. Використовуючи запатентовану платформу і дані про претензії, Cyber Risk Assessment оцінює положення організації у сфері кібербезпеки відносно інших учасників платформи і надає компаніям рекомендації по зниженню їх ризик. Оцінка попереджає компанії про критичні уразливості програмного забезпечення, уразливих базах даних і інфраструктурі, зараженнях шкідливим програмним заберзпеченням і схожих реєстраціях доменів, а також надає адаптовані рекомендації з безпеки для відвертання вимагачів, злому даних і атак на соціальні служби.

Оцінка кіберризиків також включає рейтинг, який вимірює вірогідність кіберінцидента на основі її подібності з компанією, що раніше подали позов про відшкодування збитку, а також рекомендації щодо зниження вірогідності кримінальних справ і збоїв кібербезпеки. Щоб отримати оцінку кіберризиків, що персоналізується, компанія надає свою робочу адресу електронної пошти, назву компанії і галузь, а оцінка генерується автоматично і вирушає на робочу адресу електронної пошти. Компанії не зобов'язані реєструвати або створювати обліковий запис, але зобов'язані надати адресу електронної пошти з ім'ям домена, яке скануватиметься в якості заходу безпеки, щоб користувачі могли сканувати тільки ті домени, з якими вони пов'язані. Як тільки необхідна інформація вводиться в платформу Cyber Risk Assessment,

оцінка ризику, як правило, вирушає на електронну пошту людини впродовж однієї хвилини. [35]

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Кібер-ризик – специфічний вид ризику, поява якого зумовлена розвитком людства, появою та використанням ІТ-технологій. Особливістю кібер-ризиків є те, що він має прояв в нових, нематеріальних формах, які за своєю природою не залежать від людини, настання яких майже неможливо передбачити. В сучасних реаліях людина, як фізична особа або компанія, як юридична особа – всі однаково схильні до ризику. Кібер-ризики не мають територіальних меж. Швідкість розвитку і винекнення нових ризиків прямозалежна до розвитку людини та технологій.

Поняття «кібер-страхування» - наразі немає єдиного визначення. Аналізуючи праці вітчизняних і закоронних науковців, більшість класифікує явище кібер-ризику, як частину ризик менеджменту. Кібер-страхування розглядається як спосіб додаткового захисту, коли превентивні заходи захисту не будуть ефективними, як засіб мінімізування фінансових збитків та швиткого відновлення після настання страхової події.

Наразі вітчизняні страхові компанії ще не здатні сформувати і запропонувати на ринку свої власні рішення з страхування кібер-ризиків. Одним з факторів, що стримує розвиток цієї послуги в Україні - це специфіка кибер-ризиків, які потребують індивідуального підходу для розрахунків ризиків. Другим фактором гальмування розвитку виступає висока ціна страхувих премій, що суттєво знижує попит на даний страховий продукт. Вітчизняні страхові компанії, готуючи пропозицію для клієнта, оцінюють ризики компанії за допомогою непрямих ознак і характеристик, таких як: методи управління ризиком в компанії; способи зберігання даних; проведення чи тестування систем інформаційної безпеки та аудиту, а також оцінюють кількість співробітників зайнятих в ІТ. Слід очікувати, що найближчим часом почнуть формуватися більш детальні методики, які все-таки будуть відповідати на пряме запитання щодо оцінки ризиків кібер-страхування.

Підсумовуючи можна роботу можна сформувати такі пропозиції.

- Слід використовувати закордонний досвід. Запрошувати та наймати кваліфіковані досвідчені кадри.
- Для прискорення розвитку вітчизняного кібер-страхування обов'яково слід створити законодавче підгруття для даної галузі страхування.
- Потрібно законодавчо визначити ознаки настання кібер-інцидента, сформувати загально-обов'язкові превентивні заходи захисту від кібер-загроз. Наприклад, це може бути хочаб встановлений антивірус, який буде працювати за чітко визначиним протоколом, на всіх організаціях, учасниках фінансових взаємовідносин, або в організація, в яких річний обіг коштів перевищує певну, зазначену законодавчо, суму. Це значно полегшить процедуру визнання інцеденту страховим або не страховим випадком.
- Затвердити необхідну мінімальну базу захисту.

Все це, на мою думку, суттєво покращить стан кібер-страхування і дозволить вітчизняним страховим компаніям піднятись на новий рівень надання послуг в сфері кібер-ризиків.

Список використаних джерел:

1. Trend Micro: Число бесфайловых атак в первом полугодии выросло URL: http://www.tadviser.ru/index.php
2. Чайковська М. П., Стратегії розвитку ІТ-ринку України в умовах фінансової кризи: збірник наук праць. № 35, 2009, Вісник соціально-економічних досліджень.
3. Ротова Т. А., Шевченко Ю., Страхування як фінансовий інструмент захисту від кібер-ризиків.
4. Кібер-атаки URL: http://zdrav.expert/index.phpB8
5. Віннікова І.І., Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними: монографія. Придніпровська державна академія будівництва та архітектури.
6. Кібербезпека-2018: чого чекати бізнесу URL: https://pershyj.com/p-kiberbezpeka-2018-chogo-chekati-biznesu-12919
7. Как компании страхуют кибер-риски в Украине URL: https://delo.ua/special/kak-kompanii-strahujut-kiber-riski-v-ukraine-346724/
8. Потери организаций от кибер-преступности URL:http://www.tadviser.ru/index.php_Juniper_Research
9. Актуальные киберугрозы., I квартал 2019 года URL:https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1-2019/
10. Д. Нікулеско, Ера нових видів злочинів: Юридична газета URL: http://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html .h

11. Пігулка від хакерів: як бізнес захищає себе від кібератак URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak
12. Волосович С., Клапків Л., Детермінанти виникнення та реалізації кібер-ризиків: Київський національний торговельно-економічний університет.
13. Ponemon Institute LLC. Global Cyber Risk TransferComparison Report. 2017 URL: http://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfercomparison-report.jsp.
14. Allianz Global Corporate and Speciality. A Guide to Cyber Risks. URL:https://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf
15. Passeri P. Cyber Attacks Statistics. January 2018. Nextgen Network Monitor. URL:https://www.hackmageddon.com/2018/02/22/january-2018-cyber-attacks-statistics.
16. Cyber Insurance Cost URL: **Ошибка! Недопустимый объект гиперссылки.**
17. R. Harvig, «White book: Cyber Risks.Threat and Opportunity»
18. Institute of Insurance statistics URL: https://www.iii.org/press-release/us-cyber-insurance-market-demonstrates-growth-innovation-in-wake-of-high-profile-data-breaches-102015
19. Tips on Getting Affordable Cyber Insurance Coverage URL: https://fitsmallbusiness.com/cyber-liability-insurance/
20. Cyber insurance claims: Ransomware disrupts business. URL: https://www.aig.co.uk/insights/cyber-ransomeware-disrupts-business
21. Cyber insurance market growing from $2.5 billion in 2015 to $7.5 billion by 2020. URL: https://cyberinsureone.com/stats/
22. A Guide to Cyber Risk, Alianz URL: https://www.agcs.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.html

23. US Cyber Market Update 2018, US Cyber Insurance Profits and Performance, June 2019 URL: http://thoughtleadership.aon.com/Documents/201906-us-cyber-market-update.pdf
24. Кто такие украинские хакеры из Avalanche, которых ловили спецслужбы 41 страны мира URL: https://www.depo.ua/rus/politics/hto-taki-hakeri-z-avalanche-foto-video--07122016113000
25. BBC Ukraine: «Есть те, кого "взломали", и те, кто об этом еще не знает - эксперт по кибербезопасности» Анастасия Зануда URL: https://www.bbc.com/ukrainian/features-russian-38596911
26. Пострелко Ю. М., Кібер-захист за M.E.DOC –результати ваємодії з бізнесом, державою і міжнародними експертами.
27. Кібер-страхування: новий інструмент ризик-менеджменту. URL:http://sk-ridna.com.ua/home/1019-2017-01-24-14-57-52.html
28. Реальне страхування від "віртуальних" ризиків. URL: https://dt.ua/finances/realne-strahuvannya-vid-virtualnih-rizikiv-262800_.html
29. Приказюк Н. В., Необхідність та можливість впровадження нових страхових продуктів у страховій системі: Економіка і фінанси 2016
30. Новости страхового рынка Украины от компании УКРФИНСТРАХ URL: https://ufi.net.ua/novosti-rynka/308-rynok-strakhovaniya-ot-kiber-ugroz-v-blizhajshie-10-let-mozhet-stat-odnim-iz-naibyuolee-perspektivnykh
31. Иващенко А.Н., Шарко И.А., Мировой рынок страхования кибер-рисков: перспективы и препятствия для развития в Республике Беларусь, материалы IX Международной научно-практической конференции студентов.
32. The Evolution of Cyber Insurance. URL: https://prowritersins.com/cyber-insurance-blog/top-cyber-insurance-companies/
33. Cyber insurance companies. URL: https://cyberinsureone.com/cyber-insurance-companies/

34. Calco commercial insurance. URL: https://www.calcoinsurance.com/cyber-insurance?gclid=CjwKCAiAh5_uBRA5EiwASW3IarPyCraJujUUskfSYhZcjmfdPJlsiRzEzUAyB6roe5qiHGyNvhJF7xoChZUQAvD_BwE
35. Иншуртех-стартап Coalition запустил бесплатный инструмент оценки киберрисков для малых и средних компаний URL: доступу https://forinsurer.com/news/19/11/08/37382?fbclid=IwAR0WJvcDk68ypgpLiXxG1ohCO7MfGf0vCMNvElpiRI0cn-2y8i-tmDZP2Go
36. Страхова компанія «Альфа страхування» URL: https://alfaic.ua/ru

ДОДАТКИ

Додаток А

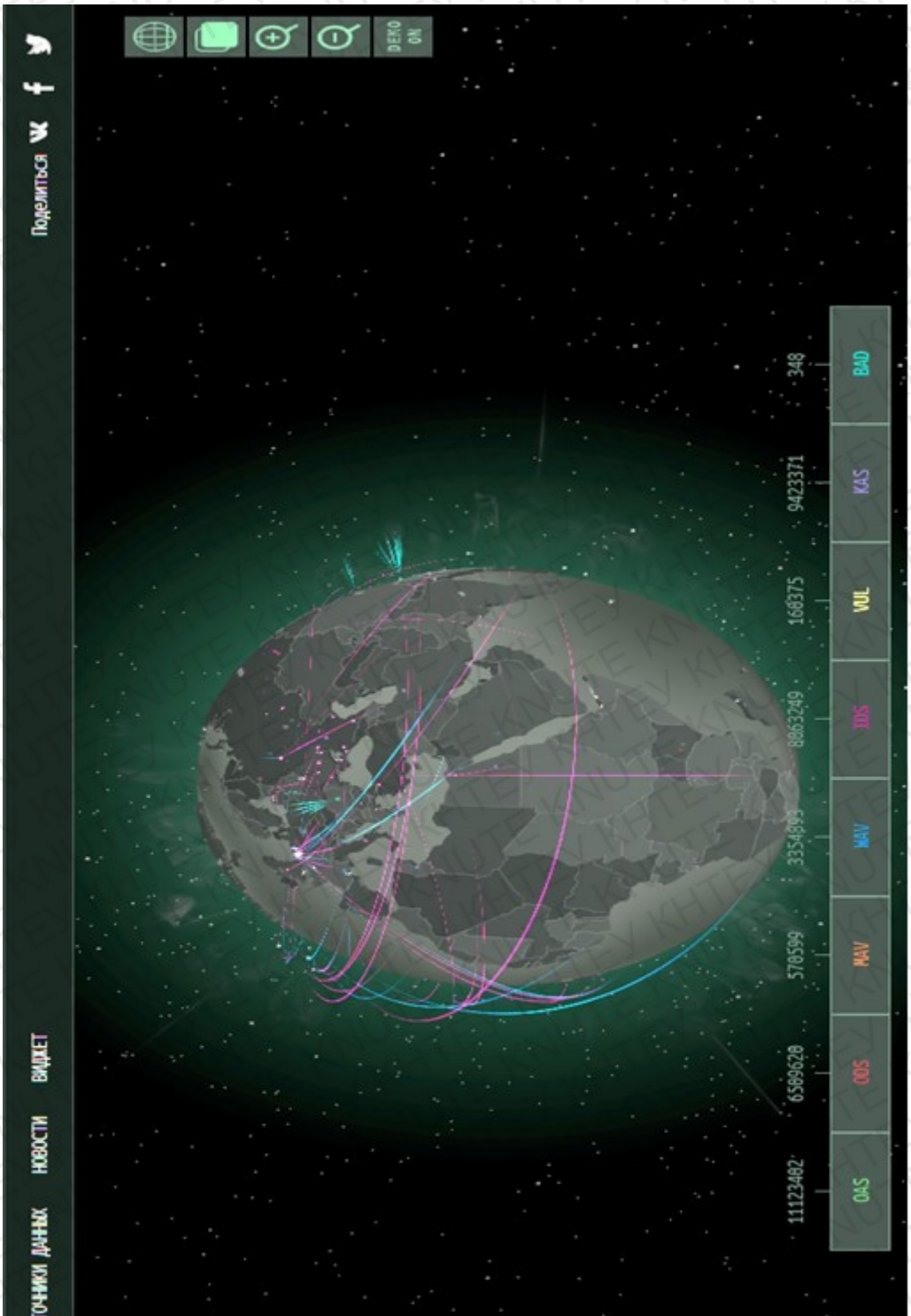
«Топ-10 кібер-ризиків у 2017 році» [6]

№	Назва	Опис
1	Petya	програма-вимагач, яка шифрує дані
2	Blueborne	вразливість – у протоколі Bluetooth
3	NotPetya	програма, яка знищує дані на ПК
4	Wannacry	програма-шифрувальник, що вимагає викуп за дешифрування
5	KRACK	критична уразливість мереж Wi-Fi
6	EternalBlue	програма для одержання віддаленого доступу до системи
7	Bad rabbit	вірус-шифрувальник, розроблений для ОС сімейства Windows
8	Loki / Locky	Android-шкідливий / шифрувальник Windows
9	Reaper	вірус, спрямований на IoT-пристрої

1 0	Критична вразливість у доступі під root користувачем в MacOS

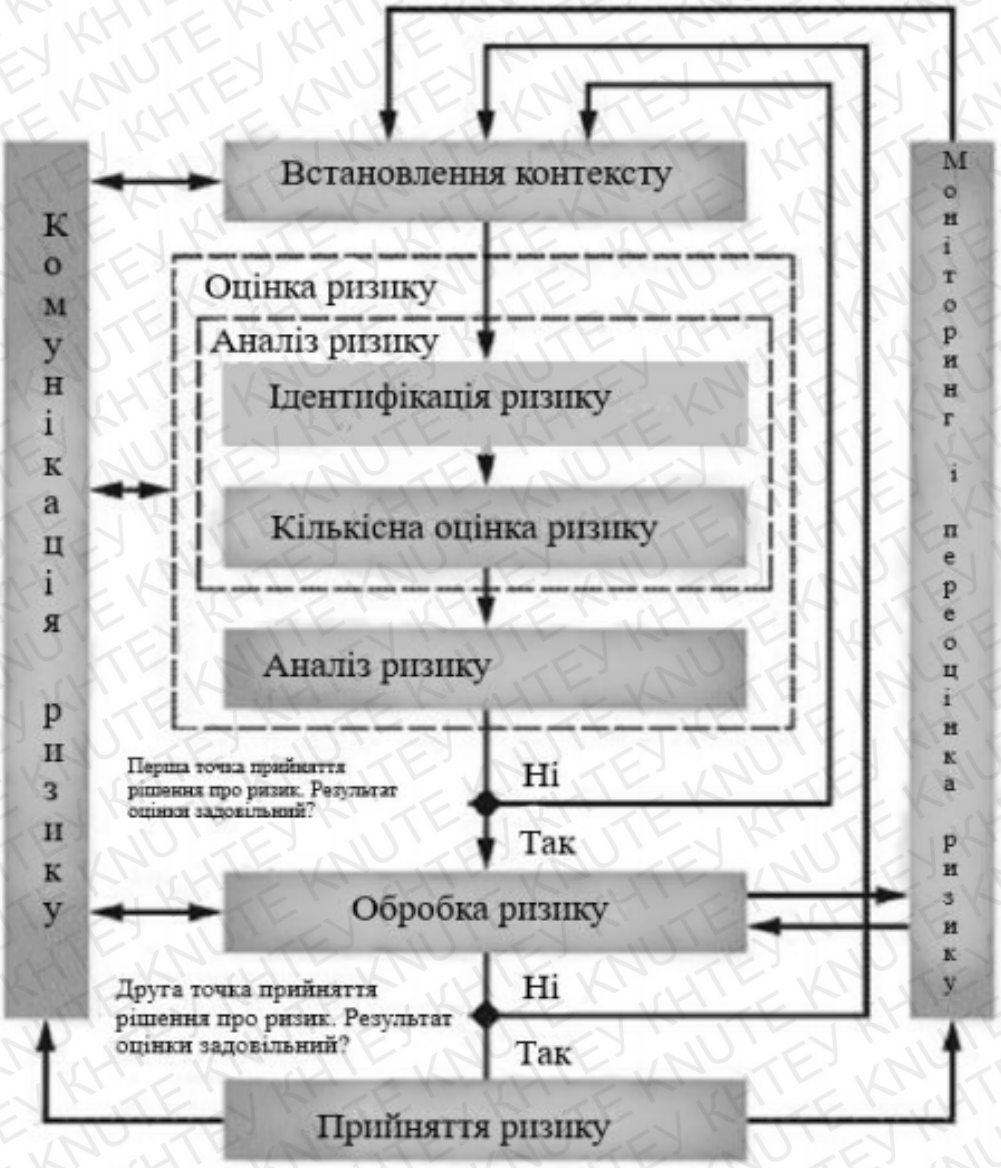
Додаток Б

Онлайн-карта кібер-атак KASPERSKY



Додаток В

Процес менеджменту ризику інформаційної безпеки



Додаток Г

Покриття «повного» пакету послуг за договором кібер-страхування від СК «Альфа Страхування» [36]

Покриття А (кібер-ризик)	**Покриття В (відповідальність)**
Втрата даних - що виникла в результаті збою даних в або у зв'язку з бізнесом страхувальника, вперше виявленого страхувальником в період страхування. "Збій даних" - втрата, незаконна або несанкціонована зміна, неналежна публікація або крадіжка даних тих, що знаходяться на комп'ютерах страхувальника або втрата, незаконна або несанкціонована зміна, неналежна публікація або крадіжка електронних даних.	Відповідальність за порушення персональних даних і корпоративної інформації (комерційні таємниці, професійна інформація, бюджети, переліки клієнтів і ін.) унаслідок несанкціонованого розкриття або передачі, у тому числі зараження вірусами, знищення, модифікації або видалення інформації.
Покриття С (перерва виробництва)	**Покриття D (додаткове покриття)**
Переривання роботи мережі (перерва у виробництві) страховик відшкодує збитки страхувальникові, понесені впродовж періоду відшкодування, пов'язаного з комп'ютерами страхувальника, в результаті кібер-атаки, уперше виявленою в період страхування	Компенсація за присутність в суді "Кризове PR - управління" Регуляторні розслідування / штрафи

Загальна страхова сума:

- За кібер-ризикам - 5 млн $,
- За перервою у виробництві - 1 млн $

Страхова премія від 60 тис доларів.

Додаток Д

Анкета розрахунку покриття страхування від кібер-ризиків [34]