МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Києво-Могилянська академія»

Факультет економічних наук
Кафедра фінансів

Кваліфікаційна робота
освітній ступінь - бакалавр

на тему: Розвиток страхування кібер ризиків в Україні

Виконала: студентка 4-го року навчання,
напряму підготовки
07 «Управління та адміністрування»
спеціальність 072 «Фінанси, банківська справа та страхування»

Сивоконь Єлизавета Андріївна

Керівник: Бридун Є.В., кандидат економічних наук, доцент

Кваліфікаційна робота захищена
з оцінкою «_____»

Секретар ЕК _____

«____» _____ 2020 р.

Київ – 2020

ЗМІСТ

ВСТУП

Цифрова трансформація економічної діяльності створює значні можливості для впровадження інновацій. Однак, останні великі випадки втрати та шифрування даних підкреслили необхідність цифрової безпеки та захисту конфіденційності у всіх галузях. Наразі, ринок кіберстрахування в Україні існує в теорії і перебуває на першому етапі розвитку.

Для ефективного функціонування він потребує законодавчої бази, яка була б підставою для видачі ліцензій страховим компаніям на проведення страхування від існуючих кібер ризиків та інших загроз. Поняття кібер ризик є досить новим на сьогоднішній день і потребує досконального вивчення та розробки методології його страхування.

Вагомий внесок у дослідження нового виду страхування в Україні зробили такі автори, як В.П. Братюк, О.М. Парубець, В.П. Ільчук та Д.О. Сугонянко, але зважаючи на стрімкий розвиток технологій проблема страхування кібер ризиків залишається недослідженим у повному обсязі та актуальним на сьогоднішній день.

Актуальність теми. Щодня стається тисячі кібер-нападів на організації державного та комерційного характеру по всьому світу. Основними наслідками є втрата корпоративних даних, інтелектуальної власності та репутації, що може призвести до численних штрафів та банкрутства фірми, тому питання страхування від кібер-атак є надзвичайно актуальним, оскільки конфіденційна інформація має такою і залишатися.

Метою цієї кваліфікайної роботи є вивчення особливостей функціонування та класифікації кібер ризиків та виявлення проблем здійснення їх страхування в Україні на прикладі іноземного досвіду.

Досягнення цієї мети забезпечене вирішенням таких **завдань**:

- дослідити страховий портфель майнового ринку та принципи страхування;
- описати види страхування в Україні;
- проаналізувати іноземний страховий ринок та виявити особливості страхування
- зробити кластерний аналіз та виявити галузі, які найбільше потребують кібер захисту
- розробити алгоритм оцінки ризиків

Об'єктом дослідження виступає ринок майнового страхування в Україні, іноземний ринок кібер-страхування і проблема відсутності виду кібер-страхування, як окремого виду страхування серед страховиків.

Предметом дослідження розглядається досвід іноземних страхових компаній при страхуванні інформаційної безпеки фірми та методи впровадження цього виду страхування на український ринок шляхом потужної законодавчої бази, алгоритмами перевірки фірми на готовність до кібер-атак та розробки превентивних заходів.

Методи дослідження. Основним методом дослідження є системний, використання якого призвело до аналізу поняття «майнове страхування» у всіх проявах його елементів, а також у кооперації з розвитком ринку страхових послуг за 2016-2019 роки. Особливості різних видів страхування ризиків та дослідження тенденцій розвитку кібер-злочинів у світі.

Інформаційну базу дослідження становлять Закони України про страхування та Закон про основні засади забезпечення кібербезпеки, інформація зі

звітів огляду ринку страхування України та консолідованих даних по ньому, а також різні джерела інформаційного характеру про страхування України та світу.

У **першому розділі «**Теоретичні основи страхування кібер-ризиків» визначені поняття страхування, його форми та класифікація. Показані предмети та об'єкти страхування. Виокремлені ризики, які можуть виникнути в наслідок кібератак та інших видів інтернет злочинів. Наведена класифікація та опис кібер злочинів. Названі необхідні дії, щоб покращити захист компанії від зовнішніх загроз. Перераховані методи оцінки наскільки компанії готові до кібер-нападів.

У **другому розділі** «Аналіз розвитку майнового страхування» наведено загальний аналіз показників за 2016-2019 роки, проведено характеристику страхового поля України та чітко визначено проблеми і подальші перспективи розвитку страхування кібер ризиків.

У **третьому розділі** «Проблеми та рекомендації здійснення страхової діяльності» проведені різноманітні аналізи: загальний аналіз кібер ризиків та способи їх страхування на світовому рівні, кластерний аналіз та дискримінантний аналіз найбільших випадків витоку даних та виокремлення груп галузей, які найчастіше зазнають кібер-нападів. Розроблено два чек-листи для підготовки компаній до страхування від кібер ризиків та виявлення їх слабких зон. Надано рекомендації до правил страхування. Розроблено алгоритм оцінки активів компаній для подальшого страхування.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СТРАХУВАННЯ КІБЕР-РИЗИКІВ

1.1. Теоретичні основи майнового страхування

Майнове страхування одне з найдавніших видів страхування, яке існує. Починаючи з 1750 р. до нашої ери вавилоняни запровадили систему кредитів для купівлі товару, при якій клієнту за додаткову суму давалася гарантія на скасування кредиту, якщо вантаж буде викрадений або втрачений в морі. Наступним був крок створення окремих контрактів страхування, які були забезпечені не кредитами, а земельними заставами. Наслідки Лондонської пожежі у 1666 році слугували, щоб створити необхідний «Офіс для страхування будинків», який застрахував від пожежі близько 5000 домівок у 1681 р.

Один з найрозповсюдженіших видів страхування, яке охоплює практично всі види власності юридичних осіб та фізичних осіб: будівлі, споруди, машини, обладнання, сировина, матеріали, робоче і продуктивне тваринництво, сільськогосподарські культури і предмети побуту.

Страхування - це найдавніша категорія суспільно-економічних відносин між людьми, яка є невід'ємною частиною виробничих відносин. Зокрема, вираз "страхування" іноді вживається в значенні підтримки в якій-небудь справі, гарантії в різних галузях. В даний час даний термін все частіше вживається в значенні інструмента захисту майнових інтересів фізичних і юридичних осіб. Найточніше поняття описує Закон України «Про страхування» -

«Страхування - це вид цивільно-правових відносин щодо захисту майнових інтересів фізичних осіб та юридичних осіб у разі настання певних подій (страхових випадків), визначених договором страхування або чинним законодавством, за рахунок грошових фондів, що формуються шляхом сплати фізичними особами та юридичними

особами страхових платежів (страхових внесків, страхових премій) та доходів від розміщення коштів цих фондів» [1].

«Економічний зміст страхування полягає в тому, що цей різновид людської діяльності спрямований на захист майнових інтересів юридичних та фізичних осіб, що потерпіли у зв'язку з настанням страхових випадків, визначених договором чи страховим законодавством, за рахунок страхових фондів, які формуються учасниками страхування» [2].

Економічна природа страхування виявляється в грошовому відшкодуванні збитків в результаті випадкових подій.

«Страхування майна фізичних осіб здійснюється в основному в добровільній формі, тоді як значна частина майна юридичних осіб страхується в обов'язковій формі. Насамперед, це стосується тих об'єктів, які мають високу вартість та зачіпають майнові інтереси не тільки окремих суб'єктів господарювання, але й національні інтереси.

Предмет майнового страхування є інтереси, пов'язані з:

1. Володінням.
2. Користуванням.
3. Розпорядженням майна.

Суб’єктами страхових відносин є: юридичні особи, фізичні особи, фізичні особи, що займаються підприємницькою діяльністю, тощо.

Система ставок страхових тарифів, їх диференціація, застосування знижок, націнок, пільг - найбільш тонкий елемент страхових відносин. Тарифні ставки в майновому страхуванні диференційовані за галузевою належністю, за видами підприємств та організацій, за категоріями страхувальників, за ступенем ризику окремих видів транспорту, за групами тварин тощо. Знижки застосовуються, якщо страхується цілісний майновий комплекс, якщо страхувальник за даними об'єктами є постійним клієнтом страхової компанії та не отримував страхового відшкодування. Націнки призначені для страхування транспортних засобів та

майна при проведенні випробувань та експериментів. Пільгами користуються підприємства сільської місцевості та громадяни певних категорій (інваліди, постійні клієнти). Використання франшизи також впливає на зменшення розміру тарифної ставки» [4, с. 43].

«Страхове відшкодування виплачується залежно від розміру страхового збитку та системи (методу) страхування.

Збитком при страхуванні майна вважається:

1.1 У разі його знищення чи крадіжки — його дійсна вартість з урахуванням зносу на момент настання страхового випадку або дійсна вартість, виходячи із ринкових цін.

2.1 У разі пошкодження — різниця між заявленою (вказаною, визначеною) дійсною вартістю і вартістю цього майна з урахуванням знецінення в результаті страхового випадку.

Страховий збиток при страхуванні основних і оборотних активів включає:

1. вартість знищеного майна за страховою оцінкою; вартість пошкодженого майна з урахуванням його знецінення.

2. витрати, пов'язані з рятуванням майна, запобіганням та зменшенням збитків (переміщення майна в безпечне місце, відкачка води тощо).

3. вартість робіт з приведення застрахованого майна в належний вигляд (прибирання, сушіння, сортування тощо).

Із розміру страхового збитку вираховуються:

1. вартість придатних для використання частин майна;

2. вартість придатних для використання, але знецінених частин майна (дошки, цегла, запчастини, інструменти тощо)

Страховий збиток при страхуванні транспортних, засобів визначається:

1. При крадіжці — за його вартістю з урахуванням зносу на момент настання страхового випадку;

2. При знищенні — за його вартістю з урахуванням зносу за вирахуванням вартості залишків (можливо і знецінених), придатних для подальшого використання;

3. При пошкодженні — за вартістю ремонту у такому порядку: до вартості нових деталей, зменшеної відповідно відсотку зносу, який вказується в договорі страхування, додається вартість ремонтних робіт, далі віднімається вартість залишків, придатних для подальшого використання та переоцінених відповідно до відсотку зносу і ступеня їх знецінення, що викликані страховим випадком; включаються також витрати й на рятування транспортного засобу (у тому числі й додатковий збиток, викликаний рятуванням людей) під час страхового випадку, на приведення в належний вигляд та транспортування до найближчого ремонтного пункту чи постійного місця проживання (але не дальше найближчого ремонтного пункту); окремо страховик оплачує вартість робіт зі складання кошторису витрат на ремонт, але оплачує збиток втрати товарного виду автотранспортного засобу» [4, с.45].

Отже, майнове страхування є видом страхування, в якому об'єктом страхових відносин виступає майно. Воно забезпечує страховий захист та відшкодування, насамперед, прямих збитків, хоча за певних умов в обсяг страхової відповідальності можуть включатися й непрямі збитки.

1.2. Класифікація майнового страхування та кібер-ризиків

Страхування кібер-активів відноситься до страхування майна, класифікацію якого наведено нижче. Класифікацію визначають, як поділ загальної інформації, визначень, галузей, різноманітних ознак на специфіковані розділи. Це процес групування на класи, розділи та інші види класифікації та систематизації, що

допомагає глибше зрозуміти предмет класифікації та застосовувати більш вузькі значення.

Оскільки страхування є обширною, широкоспеціалізованою галуззю для якої було запроваджено класифікацію (Рис. 1.1), яка визначає економічне призначення та поділяє його за видами, формами, ознаками, об’єктами, статусом страхувальника та страховика та за родом небезпеки чи ризику.

Існує наступна класифікація майнового страхування:

- за ризиками
- за формою

Добровільне страхування - це страхування, яке здійснюється на основі договору між страхувальником і страховиком. Загальні умови і порядок здійснення добровільного страхування визначаються правилами страхування, що встановлюються страховиком самостійно відповідно до Закону України "Про страхування". Конкретні умови страхування визначаються при укладенні договору страхування відповідно до цього закону [1]. Обов’язкове страхування, яке передбачене Законом України про страхування.

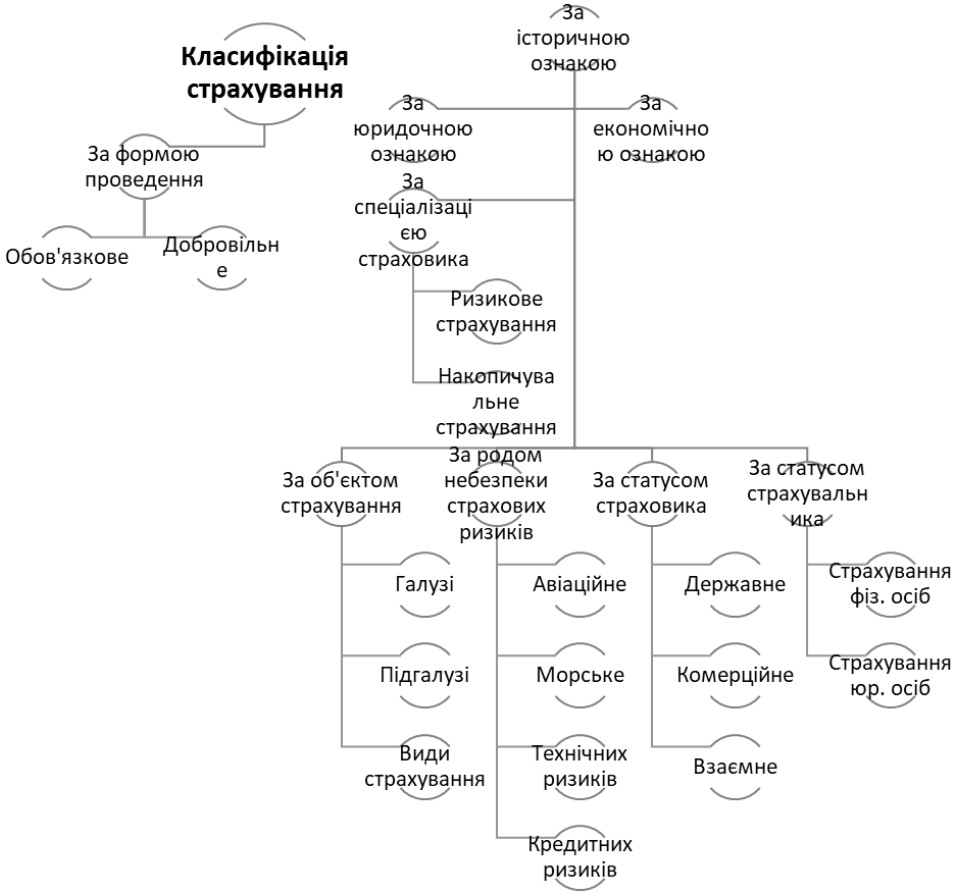


Рис. 1.1. Класифікація страхування

Джерело: Побудовано автором на основі данних [14]

Існує наступна класифікація майнового страхування:

- за ризиками
- за формою

Добровільне страхування - це страхування, яке здійснюється на основі договору між страхувальником і страховиком. Загальні умови і порядок здійснення добровільного страхування визначаються правилами страхування, що встановлюються страховиком самостійно відповідно до Закону України "Про страхування". Конкретні умови страхування визначаються при укладенні договору страхування відповідно до цього закону [1]. Обов’язкове страхування, яке передбачене Законом України про страхування.

- за видами

Видами добровільного страхування можуть бути:

1. страхування життя;
2. страхування від нещасних випадків;
3. медичне страхування (безперервне страхування здоров'я);
4. страхування здоров'я на випадок хвороби;
5. страхування залізничного транспорту;
6. страхування наземного транспорту (крім залізничного);
7. страхування повітряного транспорту;
8. страхування водного транспорту (морського внутрішнього та інших видів водного транспорту);
9. страхування вантажів та багажу (вантажобагажу);
10. страхування від вогневих ризиків та ризиків стихійних явищ та інші;

Види обов'язкового страхування:

В Україні здійснюються такі види обов'язкового страхування:

1. медичне страхування;
2. особисте страхування медичних і фармацевтичних працівників (крім тих, які працюють в установах і організаціях, що фінансуються з Державного бюджету України) на випадок інфікування вірусом імунодефіциту людини при виконанні ними службових обов'язків;
3. особисте страхування працівників відомчої (крім тих, які працюють в установах і організаціях, що фінансуються з Державного бюджету України) та сільської пожежної охорони і членів добровільних пожежних дружин (команд);
4. страхування спортсменів вищих категорій;
5. страхування життя і здоров'я спеціалістів ветеринарної медицини;
6. особисте страхування від нещасних випадків на транспорті;

7. авіаційне страхування цивільної авіації та інші [1].

Майнове страхування є обов'язковим елементом кожної соціально-економічної системи і в страховій літературі трактується як галузь страхової діяльності, де предметом страхового захисту виступають майнові інтереси фізичних та юридичних осіб, що не суперечать чинному законодавству і пов'язані з правом володіння, користування та розпорядження майном.

Економічне призначення майнового страхування полягає у відшкодуванні збитків, заподіяних страхувальникові внаслідок знищення, пошкодження майна при настанні страхового випадку.

Усі види страхових послуг у галузі майнового страхування за статусом страхувальника поділяються на дві групи:

1. Послуги, що обслуговують майнові інтереси фізичних осіб;
2. Послуги, що обслуговують майнові інтереси юридичних осіб.

Такий розподіл пояснюється різним змістом правил страхування. З урахуванням цієї обставини структуру галузі майнового страхування формує дві підгалузі:

1. Страхування майна юридичних осіб;
2. Страхування майна фізичних осіб. [3, с.119].

Далі потрібно навести наглядно що таке ризик та які види кібер-ризиків існують та зазначені на законодавчому рівні. Щодо ризику виділено наступні визначення:

- Ризик – це конкретне явище, або сукупність явищ (подія чи декілька подій) на випадок якого проводиться страхування, явище повинно бути випадковим, незапланованим і мати усі ознаки ймовірності [5].
- Ризик – це нестабільність невпевненість у майбутньому або рівень невпевненості, пов'язаний з проектами або іншими економічними видами діяльності [5].

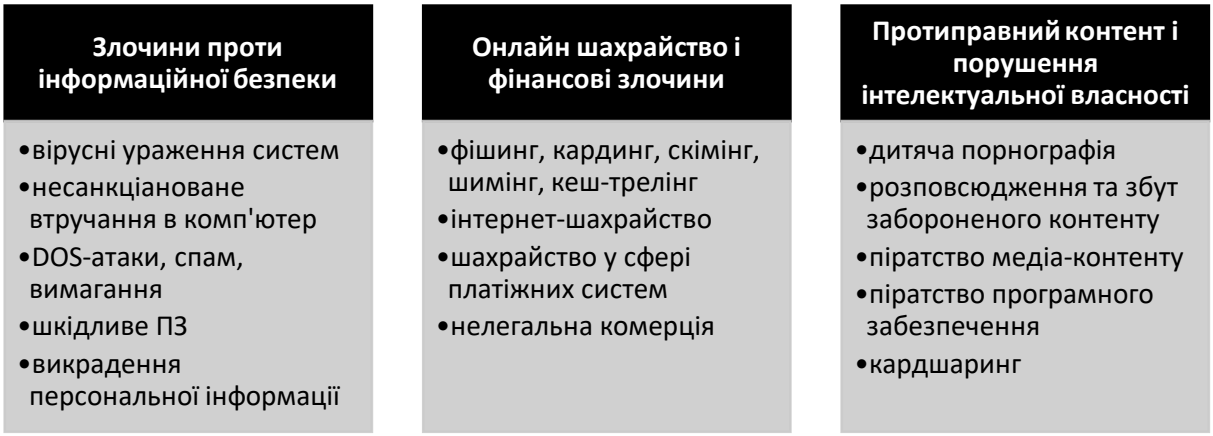
Можливості, які приносять нам цифрові технології, пристрої та засоби масової інформації також приносять ризики, які не дуже швидко виявляються. Кібер-ризик ніколи не є проблемою виключно для IT-команди, а для всієї компанії цілком. Функція управління ризиками потребує глибокого розуміння постійно зростаючих ризиків, а також практичних інструментів і методів, доступних для їх вирішення, та страхування відповідного майна.

На сьогоднішній день не існує класифікації окремо виділеного кібер-ризику в Україні, але іноземні видання виокремлюють його як:

Кібер-ризик означає будь-який ризик фінансових втрат, зривів або пошкодження репутації організації від певного невдачі своїх систем інформаційних технологій [6].

Кіберполіція України визначає незаконну діяльність як кіберзлочин такі дії у трьох категоріях: злочини проти інформаційної безпеки, онлайн шахрайство і і фінансові злочини та протиправний контент і порушення інтелектуальної власності (ІВ). Класифікація наведена на Рис. 1.2. нижче.

Рис. 1.2. Класифікація незаконної діяльності в інтернеті



Джерело: Побудовано автором на основі данних [7]

«Законом України про основні засади забезпечення кібербезпеки виділено наступні терміни:

- індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;
- інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;
- інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;
- кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або

технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

- кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;
- кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;
- кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;
- кіберзлочин (комп’ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;
- кіберзлочинність - сукупність кіберзлочинів;
- кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

- кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;
- кіберрозвідка - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;
- кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;
- кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням;
- критична інформаційна інфраструктура - сукупність об'єктів критичної інформаційної інфраструктури» [10];

«Всі типи та розміри організацій знаходяться під загрозою, а не тільки фірми фінансових послуг, оборонні організації та широковідомі компанії.

Договір про кібер-ризик може гарантувати страхувальникам відшкодування таких збитків:

1. Прямий збиток – перерва діяльності, витрати на відновлення даних, втрати доходу в результати виходу з ладу IT – мереж або веб-сайтів.
2. Збиток завданий третім особам – відповідальність за збереження даних, позовні витрати у зв'язку з відповідальністю щодо злому бази даних конфіденційної інформації;
3. Додаткові витрати – витрати на юридичний супровід, покриття суми штрафів і стягнень у зв'язку з порушеннями конфіденційної інформації;
4. Додаткові послуги – пов'язані з врегулюванням наслідків інциденту (повідомлення клієнтів, судова експертиза, експертна підтримка)» [8].

Отже, класифікація кіберзагроз та ризиків досить обширна та потребує більшого аналізу, щоб визначити як оцінювати та як страхувати їх у подальшому.

1.3. Основи страхування кібер ризиків

Важливою частиною теорії страхування є розуміння, які є складові ризику та на що впливають можливі загрози. Нижче наведено ілюстрацію (Рис.1.3.), як ризик впливає на активи компанії. Загрози викривають чутливість компанії, що є результатом витоку даних, який провокує ризик. Ризик у свою чергу пом'якшується захисним контролем, який зберігає активи, що можуть бути під загрозою. Цей цикл доступно пояснює взаємозв'язок, як найменший ризик є реальною загрозою для цілісності бізнесу.

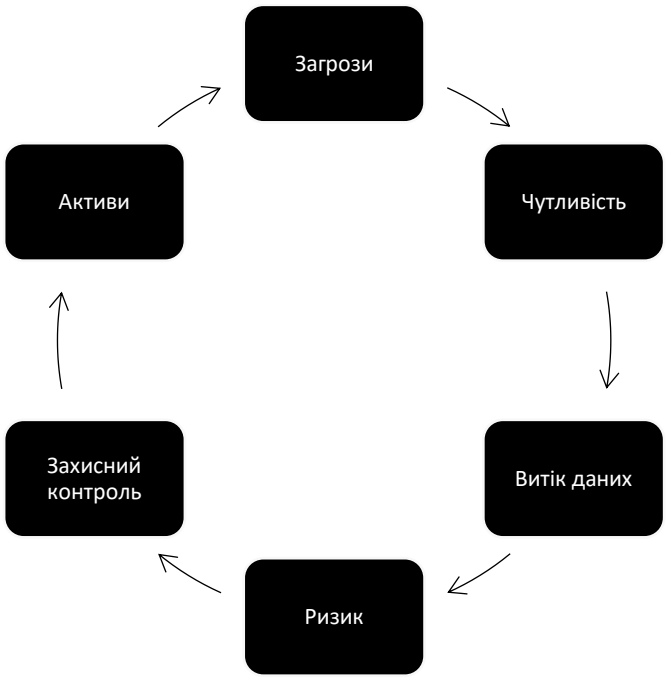


Рис. 1.3 Цикл загроз та складові ризику

Джерело: Побудовано автором на основі данних [11]

Насамперед при страхуванні від кіберзлочинів потрібно переконатися, чи страхувальник дотримувався або не дотримувався заходів безпеки при користуванні будь-яким пристроєм підключеним до мережі інтернет адже це прямо

впливає на страхову суму та саму оцінку страхування. Підприємствам слід застосовувати різні заходи з кібербезпеки, щоб зберегти свої бізнес-дані, їх грошовий потік та клієнтів в Інтернеті. Загальноприйнятими заходами безпеки вважаються наступні перелічені дії.

1. Надійний пароль;

Сильний пароль життєво важливий для безпеки в Інтернеті, він повинен бути складним, щоб мінімізувати ризик вгадування. Зробити його складним можуть наступні складові:

- комбінація великих і малих букв, цифр та символів
- використовувати від 8 до 12 символів
- уникати використання персональних даних
- регулярно оновлювати пароль
- ніколи не використовуючи його для кількох облікових записів
- при можливості використання двофакторної аутентифікації

2. Контроль доступу;

Обмежений доступ до секретної інформації тільки для тих людей, які мають дозвіл на це. Наприклад:

- контролювати фізичний доступ до приміщень та комп’ютерної мережі
- обмежити доступ стороннім користувачам
- обмежити доступ до даних або послуг через управління додатками
- обмежте те, що можна скопіювати з системи та зберегти на пристрої зберігання даних
- обмежити надсилання та отримання певних типів вкладень електронної пошти

3. Встановлення брандмауера;

Брандмауери - це ефективний засіб для захисту між вашим комп’ютером та Інтернетом і є одним із головних бар'єрів для запобігання поширенню кіберзагроз.

4. Використання надійного програмного забезпечення;

Обов’язкове встановлення ПЗ для виявлення та захисту від анти-шпигунського, анти-шкідливих та антивірусних програм, щоб допомогти видалити шкідливий код, якщо він прослизає у вашу мережу.

5. Регулярно оновлюйте програми та системи;

Оновлення допомагають захистити від відомих помилок та вразливих місць у мережі. Оновлене програмне забезпечення та пристрої є обов’язковим заходом, щоб не стати жертвою злочинців. [12]

Щоб оцінити готовність компанії до можливих кібератак та інших видів кіберзагроз на заході використовують огляд Cyber Resilience Review.

Cyber Resilience Review (CRR) - це оцінка на основі інтерв'ю, яка визначає практичну стійкість організації та практику кібербезпеки. Ця оцінка виходить з моделі управління стійкістю CERT (CERT-RMM), моделі вдосконалення процесів, розробленої Інститутом програмного забезпечення Інженерії програмного забезпечення Карнегі Меллона для управління операційною стійкістю. Огляд Cyber Resilience Review оцінює зрілість можливостей та можливостей організації у виконанні, плануванні, управлінні, вимірюванні та визначенні можливостей кібербезпеки у наступних 10 областях:

- Управління активами
- Конфігурація та управління змінами
- Управління вразливістю
- Управління інцидентами
- Управління безперервністю послуг

- Управління ризиками
- Управління зовнішньою залежністю
- Навчання та обізнаність
- Поінформованість про ситуацію

Огляд на кібер-стійкість забезпечить організацію більш надійною поінформованістю про її позицію в кібербезпеці, забезпечуючи та сприяючи наступному:

- Поліпшення обізнаності з усіма підприємствами про необхідність ефективного управління кібербезпекою
- Перевірка можливостей, необхідних для безперервної роботи критичних служб під час операційних викликів та криз [13].

РОЗДІЛ 2. АНАЛІЗ РОЗВИТКУ МАЙНОВОГО СТРАХУВАННЯ

2.1. Загальний аналіз показників

«Ринок страхових послуг є другим за рівнем капіталізації серед інших небанківських фінансових ринків. Загальна кількість страхових компаній станом на 31.12.2019 становила 233, у тому числі СК "life"1 – 23 компанії, СК "non-life" – 210 компаній, (станом на 31.12.2018 – 281 компанія, у тому числі СК "life" – 30 компаній, СК "non- life" – 251 компанія). Кількість страхових компаній значно скоротилася, так за 2019 рік порівняно з 2018 роком, кількість компаній зменшилася на 48 СК, порівняно з 2017 роком зменшилася на 61 СК» [16].

За 2019 рік частка валових страхових премій у відношенні до ВВП становила 1,3%, що на 0,1 в.п. менше в порівнянні з 2018 роком; частка чистих страхових премій у відношенні до ВВП залишилась на рівні 2018 року та становила 1,0%.

У порівнянні з 2018 роком на 3 633,7 млн грн (7,4%) збільшився обсяг надходжень валових страхових премій, обсяг чистих страхових премій2 збільшився на 5 161,7 млн грн (15,0%). [16].

Представлені макропоказники, такі як чисті страхові премії, чисті страхові виплати, частки страхових платежів та валові надходження від страхових платежів на діаграмі (Рис. 2.1.) показують, що страхування майна займає більшу частку серед інших видів діяльності. Наступним видом діяльності за обсягом є страхування фінансових ризиків.

«Питома вага чистих страхових премій у валових страхових преміях за 2018 рік становила 69,7%, що на 4,1 в.п. більше в порівнянні з 2017 роком. Протягом аналізованого періоду збільшилась кількість укладених договорів страхування на 15 594,6 тис. одиниць (або на 8,4%), при цьому на 4 909,5 тис. одиниць (або на 8,1%) зросла кількість договорів з добровільного страхування, в тому числі збільшилась кількість укладених договорів. Кількість укладених договорів з обов'язкового страхування збільшилась на 9 222,3 тис. одиниць (або на 7,5%) за рахунок збільшення кількості договорів страхування від нещасних випадків на транспорті на 8 757,9 тис. одиниць (7,6%)» [16].

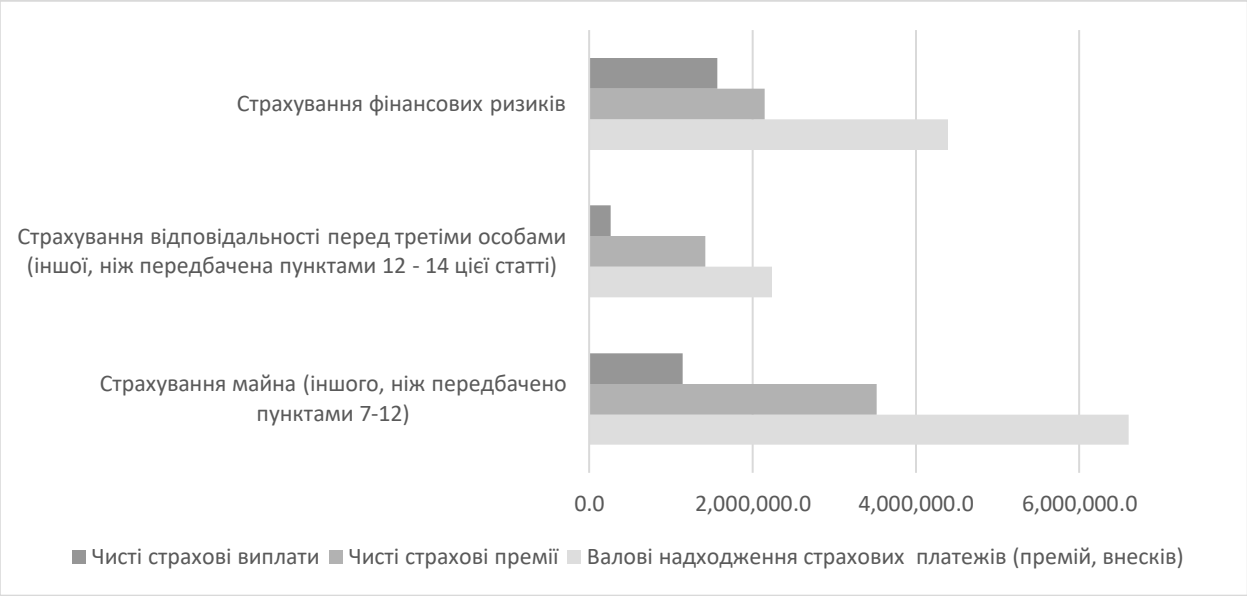


Рис. 2.1. Показники діяльності страхування, крім страхування життя за 2019 р.

Джерело: складено автором на основі консолідованих даних [15]

Загалом, на ринку страхування майна за 2016-2019 р. зберігається тенденція росту розміру серед валових надходжень від страховиків таких, як чисті страхові премііїї за весь період та чисті страхові виплати до 2018 року, а у 2019 вони почали знижатися (Рис. 2.2.). Схожа ситуація є на ринку страхування відповідальності перед третіми особами, там теж є наглядне збільшення премій (Рис. 2.3.), але на

ринку страхування фінансових ризиків ситуація інакша, хоч є значний ріст валових надходжень, чисті страхові премії повернулися на рівень 2017 року. Чисті страхові виплати не мають конкретної тенденції (Рис. 2.4.).

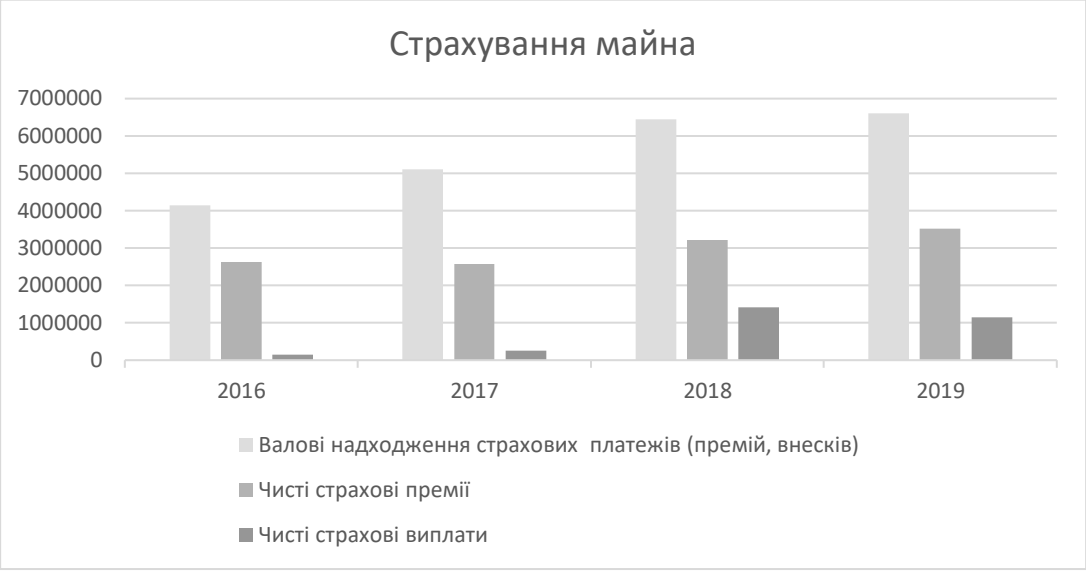


Рис. 2.2. Платежі за страхуванням майна за 2016-2019 р.

Джерело: складено автором на основі консолідованих даних [15]

Рис. 2.3. Платежі за страхування відповідальності перед третіми особами за 2016-2019 р.

Джерело: складено автором на основі консолідованих даних [15]

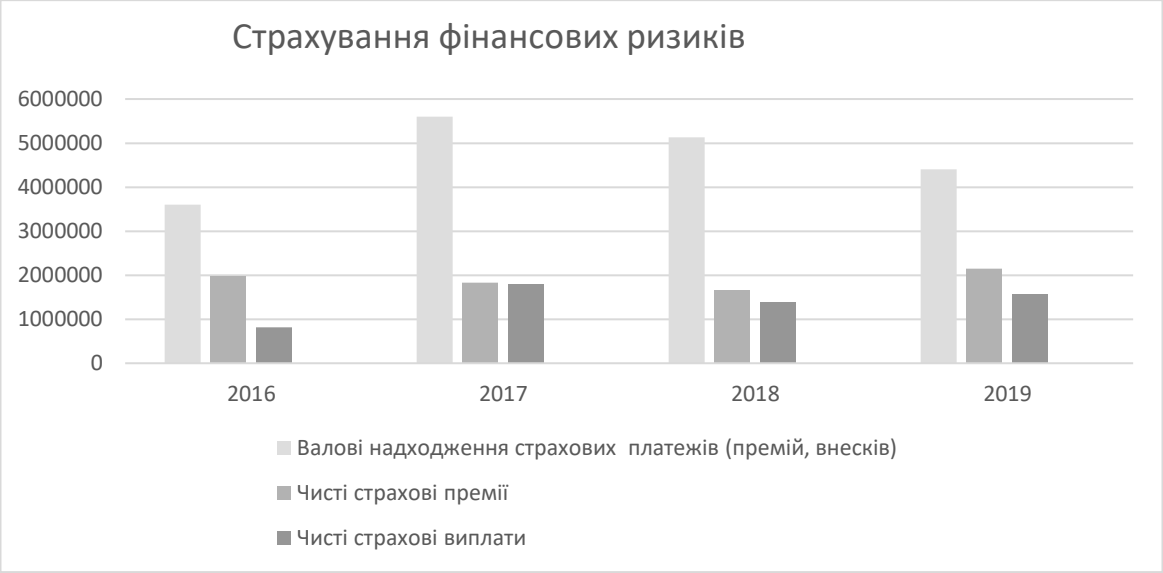


Рис. 2.4. Платежі за страхування фінансових ризиків за 2016-2019 р.

Джерело: складено автором на основі консолідованих даних [15]

«Рівень валових виплат у порівнянні з аналогічним періодом 2018 року збільшився на 1,0 в.п. та становив 27,1%. Рівень чистих страхових виплат станом на 31.12.2019 становив 35,5%, що менше на 0,6 в.п. у порівнянні з аналогічним періодом минулого року» [16].

2.2. Аналіз страхового поля страхування кібер-ризиків

На сьогоднішній день поле страхування кібер-атак в Україні вузьке і таку послугу надають лише декілька страхових компаній, не більше ніж 5. Все частіше компанії та державні організації беруть до уваги масивні кібер-атаки, які були в 2017 році (WannaCry, Petya) та шукають методи, які дозволять запобігти майбутнім втратам

Підприємства діляться на три типи:

- ті, що вже постраждали та мали значні збитки та зниження репутації компанії
- ті, що вважають, що вони обережні в своїх вчинках та достатньо захищені власними ресурсами
- ті, що бачили наслідки інших компаній від атак та вже захистили свій бізнес від кібер-нападів

В Україні більшість компаній першого та другого типу і лише одиниці, які обрали страхування кібер-ризиків для свого бізнесу. За 2017 рік від вірусів WannaCry та Petya постраждали близько 2000 компаній, а в 2018 році кіберполіцією було зафіксовано 11131 злочин з яких: 1139 у сфері протиправного контенту, 3697 у сфері платіжних систем, 3607 у сфері е-комерції та 2688 у сфері кібербезпеки (Рис. 2.6.). Протягом року найбільша кількість злочинів була зосереджена у місті Києві (2207), а також на території Одеської (1084), Миколаївської (903) та Львівської (729) областей [8].

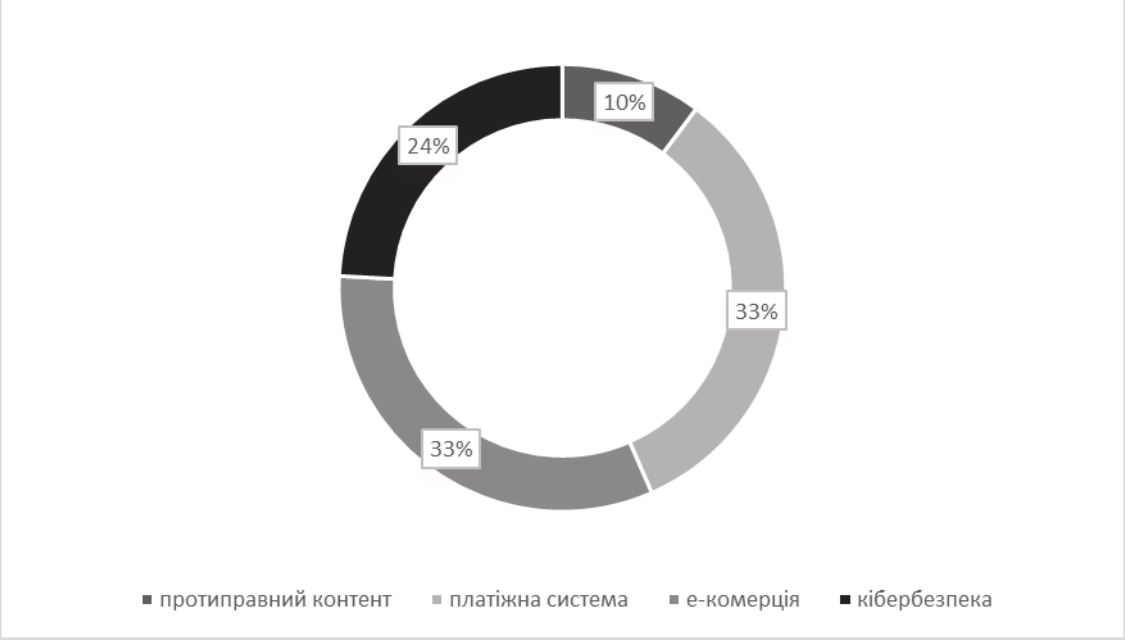


Рис. 2.5. Зафіксовані кібер-злочини у 2018 р.

Джерело: складено автором на основі консолідованих даних [9]

Зокрема, виділяють наступні дії, як кібер-злочин та від яких можна страхувати компанії:

У сфері використання платіжних систем:

- скімінг (шимінг) – незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток;
- кеш-трепінг - викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;
- кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем;
- несанкціоноване списанням коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

У сфері електронної комерції та господарської діяльності:

- фішинг - виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо;
- онлайн-шахрайство – заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

У сфері інтелектуальної власності:

- піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті;
- кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного TV;

У сфері інформаційної безпеки:

- соціальна інженерія – технологія управління людьми в Інтернет просторі;

- мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;
- протиправний контент - контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;
- рефайлінг – незаконна підміна телефонного трафіку [11].

Є лище 5 СК, які страхують від кібер-ризиків і лише одна, яка включає в свій поліс не тільки страхування від атак, ризиків та втраченого прибутку, а й страхування відповідальності перед партнерами в наслідок витікання даних та антикризисну PR компанію наслідків атаки. Ця галузь страхування надзвичайно слабко представлена в Україні і потребує вагомих зусиль, зважаючи на кількість кібер-злочинів за 2018 рік. Черговою проблемою є те, що такий вид страхування є конфіденційним і компанії можуть не здогадуватися про існування послуг.

2.3. Проблеми та перспективи розвитку

На сьогоднішньому страховому ринку, інформаційні технології є рушійною силою, яка дозволяє страховим компаніям успішно взаємодіяти з більш вимогливими і нетерплячими клієнтами. Клієнти прекрасно розбираються в технологічних інноваціях і активно використовують їх у повсякденному житті, очікують відповідний технологічний рівень сервісу і від СК.

Найголовнішою проблемою страхування кібер-ризиків є відсутність такого виду страхування у більшості СК України. Незважаючи на існування кіберполіції та загальновідомих рекомендацій задля запобігання кібер-атакам та іншим ризикам вони трапляються щомісяця та несуть значущі збитки для компаній. Наступною проблемою є відсутність алгоритмів оцінювання ризиків в Україні, оскільки для кожного виду кібер-злочину потрібно виокремити рівні заподіяної шкоди, оцінити їх та розробити заходи, щоб запобігти наступним атакам.

Потенційні фактори ризику на які слід звернути увагу у 2020 році

1. Технології – активи, що підключені до Інтернету, робить їх легкодоступними для професійних хакерів. Онлайн газети, бази даних і автономні транспортні засоби є одними з прикладів потенційних цілей для кібер-атак. Ланцюг поставок - у 2018 році, 59% компаній Великобританії і США заявили, що вони стикаються з витіком даних через треті особи і тільки 35% з них оцінили свої програми безпеки, як ефективні.
2. Internet of Things — (Інтернет речей) може включати величезну кількість різних пристроїв, від принтерів і відео-проекторів до вбудованих датчиків і камер спостереження. Кожен пристрій може стати потенційною загрозою безпеки для компаній, якщо він не управляється належним чином.
3. Ділові операції - діяльність компанії може бути легко зупинена за допомогою шкідливих програм або вірусів. Хоча, широке підключення може підвищити експлуатаційну ефективність, вони також можуть опосередковано збільшити вплив кібер-атак. У 2017, вірус WannaCry вразив понад 230 000 комп'ютерів. Вірус шифрував дані з вимогою платити біткоіни від користувачів, щоб розблокувати файли.
4. Злиття та поглинання - у 2018 загальний обсяг злиттів і поглинань досяг майже 4 000 млрд. доларів США, це найбільша цифра за останні 4 роки. Якщо велика компанія купує меншу, вона може автоматично взяти на себе її вразливість.
5. Правове регулювання - уряди країн прийняли заходи щодо запровадження вимог кібер-безпеки для підприємств. Це хороша ініціатива, але вважається, що занадто багато нормативних змін в той же час, для підвищення кібер-безпеки, можуть змусити компанії вибирати не ефективні рішення безпеки для свого бізнесу, щоб

уникнути штрафів. Компанії повинні бути пильними не тільки проти кібер-загроз, а й дотримуватися вимог кібер-безпеки.

Також можлива поява окремих тенденцій кібер-злочинів:

- Перша тенденція: поява нових вірусів і розширення Арсеналу кіберзлочинців за рахунок використання нових технологій.

Кібер-злочинці будуть атакувати розробників законного програмного забезпечення частіше, ніж кінцеві цілі. Є великі компанії з надійним і багатошаровим кібер-захистом в зоні ризику. У таких випадках набагато простіше використовувати посередника, який може бути виробником популярних програм, що використовуються в корпоративному сегменті.

Злочинці будуть продовжувати активно поширювати вірус шифрування. Багато нападів з їхньою допомогою можуть бути спрямовані на промислові системи. Ще одна приваблива мішень для хакерів – це персональні дані. Вони характеризуються як "нова олія". У цьому випадку, великі дані будуть використовуватися в самих атаках за додатковою адресою для користувача.

Це також підвищить складність виявлення та видалення шкідливого програного забезпечення за допомогою використання DNS, шифрування, інвалідності та інших технологій.

- Друга тенденція: інфраструктура кіберзагроз

В рамках цієї тенденції, напади на програмні інтерфейси, масове хакерство маршрутизаторів і модемів, злом банкоматів і POS-терміналів, посилення контролю за інфраструктурою інтернету, створення централізованої системи управління комунікаційними мережами, а також напади на хмарні бази даних.

- Третя тенденція: напади на криптовалюту

Для цієї мети кіберзлочинці активно використовують ботнет-мережі для видобутку, а також здійснюють напади на обміни валюти і користувачів [17].

РОЗДІЛ 3. ПРОБЛЕМИ ТА РЕКОМЕНДАЦІЇ ЗДІЙСНЕННЯ СТРАХОВОЇ ДІЯЛЬНОСТІ

3.1. Аналіз світового ринку кібер-страхування

Фактично, українська економіка не є винятковою: 1 900 експертів з управління ризиками від 80 країн, опитаних під час щорічного дослідження глобальних ризиків від компанії Allianz, ставлять кібер-ризики на друге місце серед глобальних загроз. Щорічні втрати світової економіки від кіберзлочинності в 2017 перевищили $600 млрд. і склали 0,8% світового ВВП, зросли на 35% в порівнянні з 2015. Звичайно, безпека вимагає інвестицій: за оцінками аналітичної компанії Gartner, для 2017 світові компанії витратили близько $86 млрд. на профілактичні системи і заходи кібербезпеки. За прогнозами на 2018, вартість зросте на 8-12%, але неможливо гарантувати, що інвестиції будуть ефективними і дозволять уникнути зростаючої загрози.

На відміну від превентивних заходів, страховий поліс може компенсувати збитки від реалізованого кіберзагрози, якщо компанія не була попереджена.

Сьогодні рівень охоплення цих послуг в 37 країнах з розвиненою економікою досягає 50-60% серед компаній-представників великого бізнесу. Глобальний ринок страхування від кібер-ризиків оцінюється приблизно $2,5 млрд. в 2017 і продовжує зростати: очікується, що до 2021 року він досягне $10 млрд.

Можливості та вигоди для страхування кібер-ризику не однакові для компаній з різних галузей промисловості. За даними всесвітньої статистики, близько 35% всіх платежів страхування кібер-ризиків генеруються клієнтами з

фінансового сектору - банків, інших фінансових установ і фінансово-технологічних стартапів, на другому місці представники енергетики [18].

У минулому році, портал Cybersecurity Ventures передбачив, що кіберзлочинність обійдеться світу в $6 млрд. щорічно впродовж до 2021, це вдвічі більше ніж $3 млрд. в 2015. Передбачені збитки будуть найбільшими в історії і їх можна порівняти з прибутковістю глобальної торгівлі всіма незаконними речами разом. Прогнози заподіяної шкоди, які базуються на цифрах кіберзлочинності, включаючи останні роки активного зростання будуть на порядок більше в 2021, ніж це є сьогодні, оскільки кібернапади є найбільш швидкозростаючим злочином в світі.

Від Yahoo Hack постраждали 3 млрд облікових записів користувачів, а від Equifax в 2017 145 млн. клієнтів. Це основні кібератаки, які порівнюють з WannaCry і NotPetya, що теж сталися в 2017 [18]. У грудні 2017, AIG оголосила про запуск системи, яка оцінює кіберризики клієнтів і забезпечує більш просунутий аналіз страхування від хакерських атак.

З листопада 2017, андеррайтери компанії AIG використовують метод комп'ютерного аналізу, який об'єднує дані про поточні кіберзагрози для отримання оцінок. Система оцінює те, наскільки кібернапади можуть впливати на бізнес компанії та вираховує потенційні збитки від різних кіберінцидентів, а також повідомляє про кібер-ризики клієнтам.

Питання кіберстрахування стає все більш гострим у всьому світі завдяки зростаючому числу хакерських атак. Страхові компанії намагаються оцінити їх потенційні ризики, як інтерес до страхування і кібер-ризики зростає, Reuters Notes.

У жовтні 2017, AIG заявила, що було розглянуто всі види страхового покриття, щоб краще оцінити недоліки в оцінці кіберризиків. У грудні, вони оголосили про партнерство з Darktrace IT компанією для запуску CyberMatics програми, яка перевіряє інформацію, отриману AIG з клієнтських інструментів

кібер-безпеки. Пакет використовує штучний інтелект для вивчення застрахованої компанії на наявність сильних і слабких точок [22].

Для наглядного аналізу світового ринку був проведений кластерний аналіз найбільших та найгучніших витоків даних з 2009 по 2020 роки в програмі Orange (Рис. 3.1.) і дискримінантний аналіз у програмі Statistica (Рис. 3.2.).

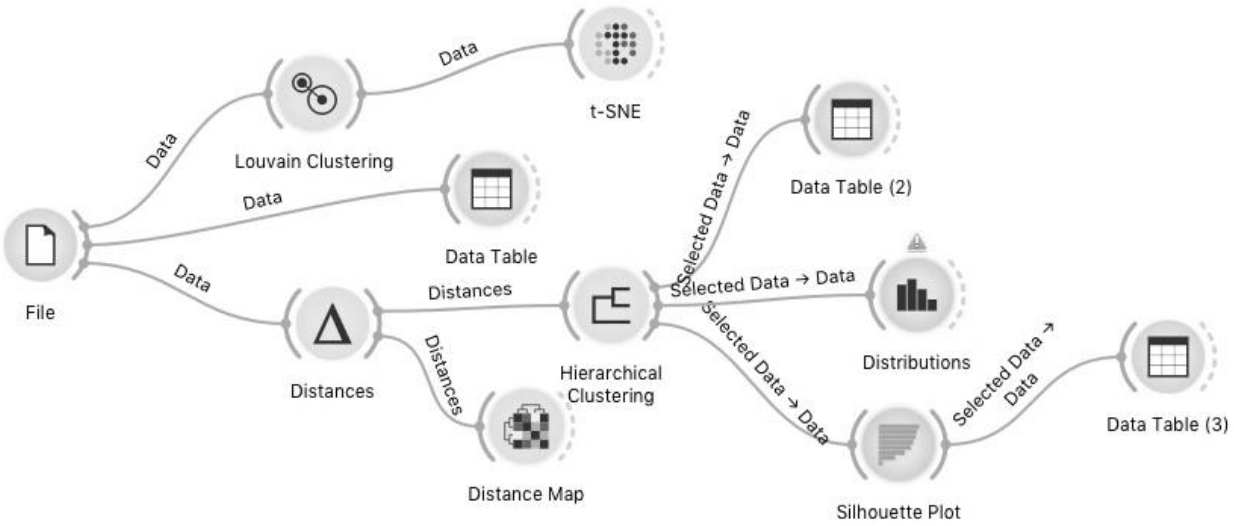


Рис. 3.1. Кластерний аналіз

Джерело: Побудовано автором

All Groups
Discriminant Function Analysis Summary (Spreadsheet1)
No. of vars in model: 2; Grouping: Method (5 grps)
Wilks' Lambda: ,92129 approx. F (8,702)=3,6717 p< ,0003

N=357	**Wilks' Lambda**	Partial Lambda	F-remove (4,351)	p-value	Toler.	1-Toler. (R-Sqr.)
Records lost	0,963489	0,956200	4,019554	0,003351	0,990854	0,009146
Sector	0,956869	0,962815	3,389009	0,009735	0,990854	0,009146

Рис. 3.2. Дискримінантний аналіз

Джерело: Побудовано автором на основі даних [24].

На Рис. 3.2. можна побачити, що значення лямбди Уїлкса наближається до 1, що свідчить про те, що модель не є дискримінантною. Значення статистики F-критерію 3, 67 при рівні p-value 0,0003, отже аналіз є значущим.

1. **Аналіз датасету**

Датасет складається з 358 випадків протягом 2004-2020 років у 14 різних галузях та з 5 методів викрадення даних. Серед цього датасету є, як державні сайти та консульства окремих країн, масштабні ТНК та соціальні мережі, так і лікарні, заклади академічної сфери, звичайні додатки та ігри.

Сфери: web, healthcare, app, retail, gaming, transports, financial, tech, government, telecoms, legal, media, academic, energy, military.

Методи: poor security, hacked, oops! (employee mistake), lost device, inside job.

2. **Louvaine clustering**

Віджет Louvaine clustering перетворює вхідні дані в графік k-найближчих сусідів. До графіку застосовується алгоритм виявлення спільних оптимізацій модульності для отримання кластерів взаємопов'язаних вузлів. За результатом пропонується 8 кластерів.

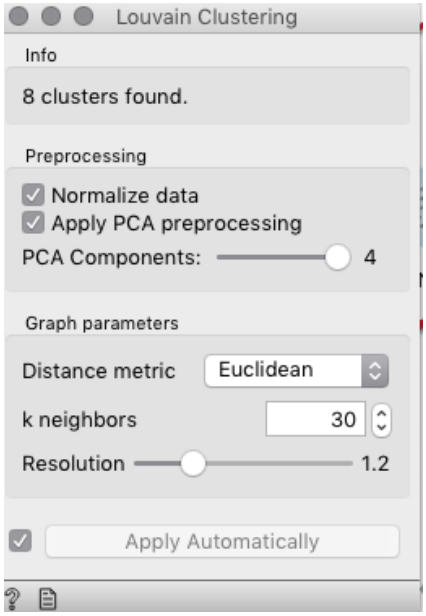


Рис. 3.3. Louvaine clustering

Джерело: Побудовано автором на основі данних [24]

3. Ієрархічна кластеризація

На дендрограмі можна побачити, що дані краще всього діляться на 8 кластерів, що підтверджує результат Louvaine clustering.

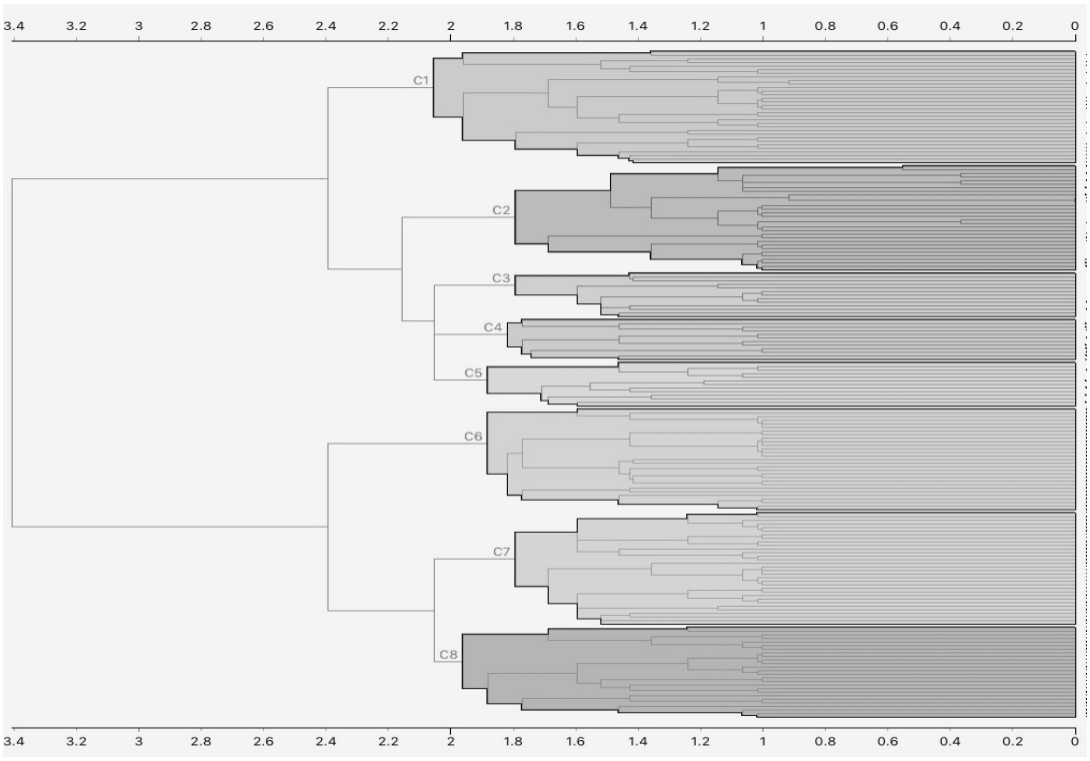


Рис. 3.4. Дендрограма

Джерело: Побудовано автором на основі данних [24]

4. Опис кластерів

В першому кластері згруповані випадки, які сталися в період 2011-2017 років в фінансовій сфері, в сфері продажу товарів (retail) та на державному рівні. Більшість було зламано хакерською атакою та декілька випадків сталися у наслідок помилки співробітників компанії.

В другому кластері згруповані випадки, які сталися в період 2013-2019 років тільки в мережі виключно після хакерської атаки.

В третьому кластері згруповані випадки, які сталися в період 2014-2020 років серед додатків та технічних компаній через скрутну внутрішню безпеку від кібер нападів.

В четвертому кластері згруповані випадки, які сталися в період 2017-2020 років в фінансовій сфері, в сфері продажу товарів (retail) за рахунок хакерської атаки та скрутної внутрішньої безпеки.

В п’ятому кластері згруповані випадки, які сталися в період 2014-2020 років в сфері здоров’я, додатків, на державному рівні, серед операторів мобільного зв’язку та в сфері продажу товарів (retail) у рівних частинах кластеру шляхом хакерської атаки.

В шостому кластері згруповані випадки, які сталися в період 2004-2008 років в академічній та фінансовій сферах і на державному рівні у наслідок загублених або вкрадених гаджетів та через внутрішній витік даних.

В сьомому кластері згруповані випадки, які сталися в період 2007-2013 років в мережі та на державному рівні шляхом хакерської атаки.

В восьмому кластері згруповані випадки, які сталися в період 2008-2013 в сфері здоров’я, на державному та військовому рівнях через внутрішній витік даних та загублені чи вкрадені гаджети.

5. Розподіл за методами витоку даних

На гістограмі можна побачити, що найрозповсюдженішим методом викрадення даних є кібер атаки, які стрімко набрали популярність з 2004 року та їх

кількість збільшується на 10% щороку. Другим за розвитком методом є викрадення чи втрата гаджетів. Наразі маючи доступ до телефона співробітника майже будь-якої компанії можна заволодіти конфіденційними даними. Третім методом є недоліки компанії у внутрішній безпеці. За рахунок того, що компанія не приділяє достатньої уваги своїй кібербезпеці вона полегшує хакерам скористатися їх даними. З 2014 року ця проблема набуває все більших масштабів.

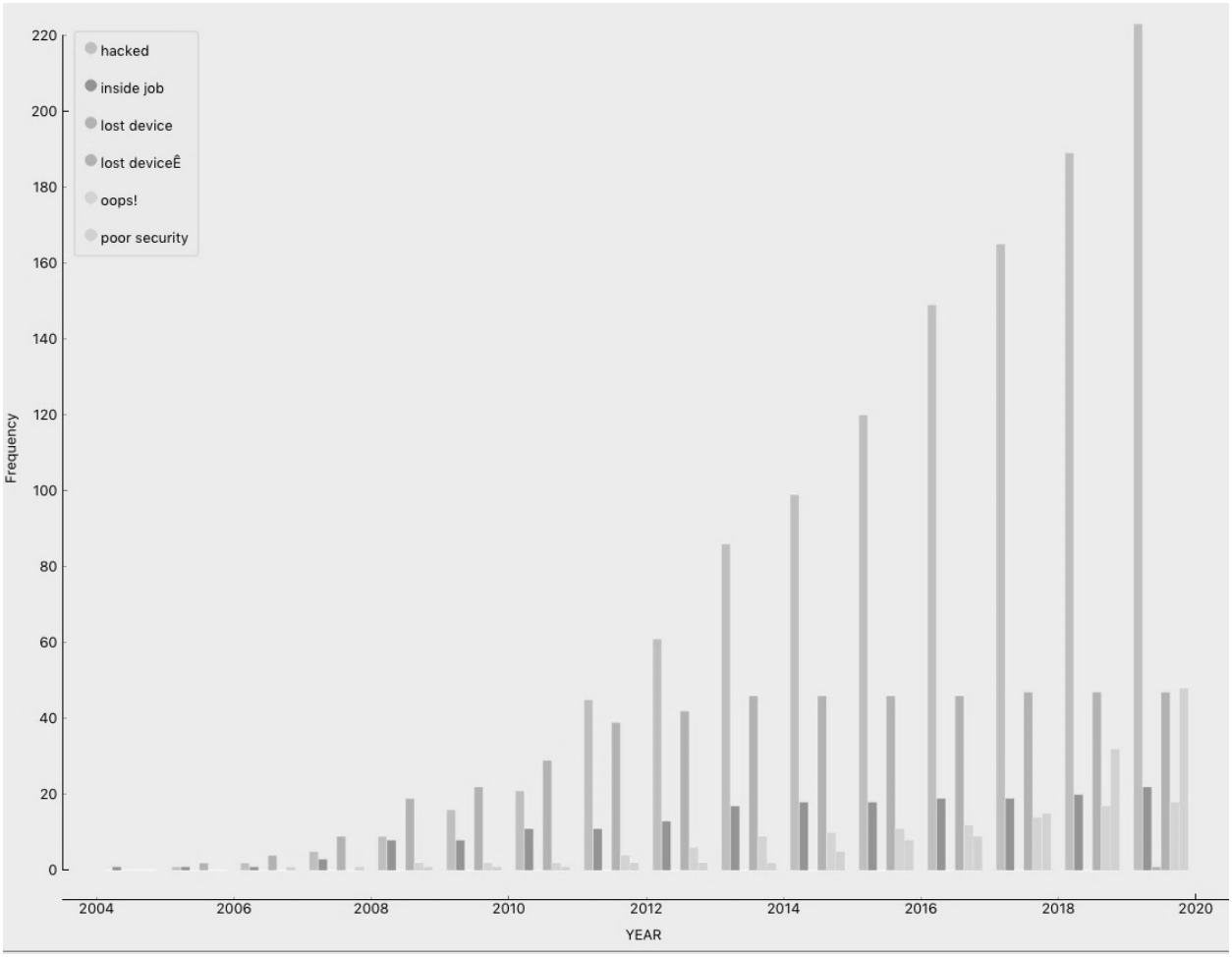


Рис. 3.5. Розподіл за методами витоку даних

Джерело: Побудовано автором на основі данних [24].

Отже, після проведеного аналізу можна сказати, що найбільше схильні стати цілями кібер-атак державні органи та компанії, які діють у фінансовій сфері і сфері продажу товарів. Окремо можна виділити, як відносно легко було отримати конфіденційну інформацію в період 2004-2008 років в таких серйозних сферах, як

державні органи та військові підрозділи, де дані повинні бути якнайкраще захищенні завжди. Четвертий кластер найбільше відповідає рокам дослідження наукової роботи і репрезентує актуальні сфери, які під загрозою можливих кібер злочинів і яким необхідно приділити максимальну увагу внутрішній безпеці.

3.2. Рекомендації щодо вдосконалення страхування кібер-ризиків

Укладення контракту на страхування кібер-ризиків передбачає комплексну оцінку клієнта та її систем інформаційної безпеки. В першу чергу оцінюється економічний стан підприємства та країни збуту. При цьому оцінюється безпека комп'ютерних мереж та ступінь захисту персональних даних клієнтів. Чим більше страхувальник має доступ до конфіденційної інформації користувачів, тим дорожче буде коштувати поліс.

В окремому порядку оцінюється вплив субпідрядників, яким страхувальник видає частину робіт для аутсорсингу, до того ж перевіряється їх досвід і надійність [18]. З точки зору кібер-безпеки фірми перевіряється:

- Наявність анти-вірусів,
- Наявність брандмауерів,
- Наявність систем контролю за нелегальним вторгненням,
- Як працюють з рахунками,
- Процедури контролю доступу та методи захисту даних.

Для визначення рівня ризику потрібно провести кількісний аналіз, який складається з 4 кроків (Рис.3.5.).

1. Інвентаризація всіх активів і призначення їм цінності.

2. Створення листу з можливими вразливостями компанії для кожного окремого активу, визначення фактору незахищеності та розрахунок суми одноразової втрати активу.
3. Проведення аналізу загроз та розрахунок ймовірності настання подій в межах одного року, які призведуть до втрати активів.
4. Визначення точної суми втрати коштів від втрати активу.

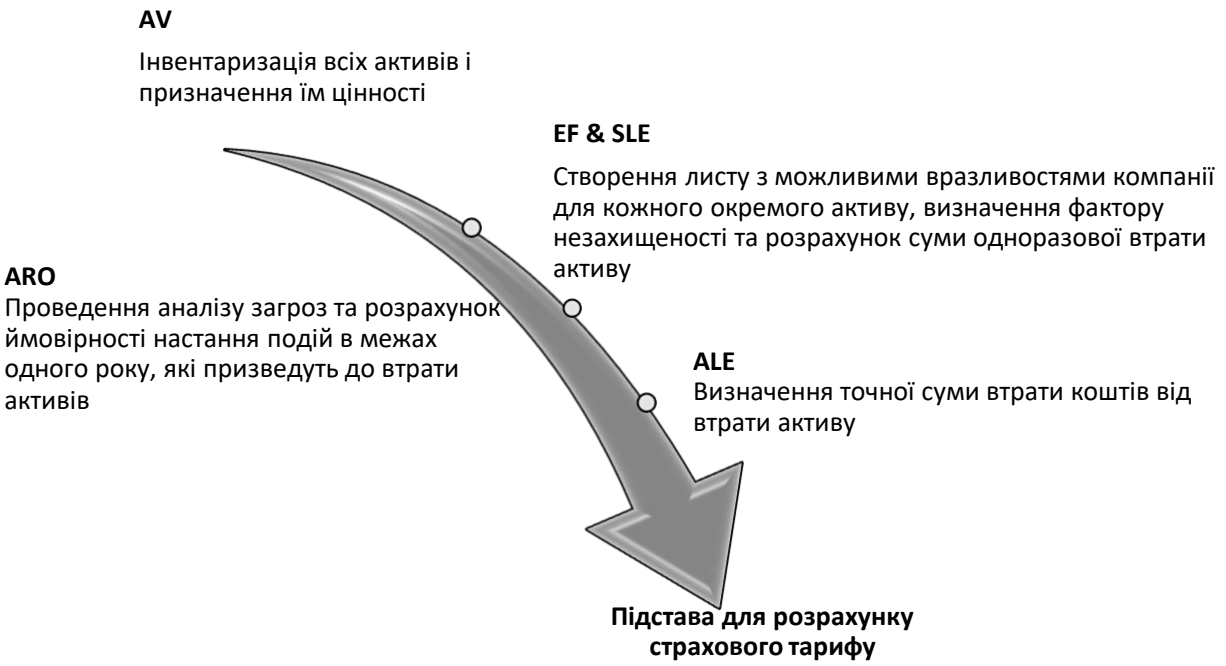


Рис. 3.6. Алгоритм дій для страховика та страхувальника при заключені поліса кібер-страхування

Джерело: складено автором.

При виконанні першого кроку, компаніям необхідно дотримуватися списку чинників, які прямо впливають на точну оцінку активу. Призначення грошового еквіваленту є складним процесом, але він є невід'ємною частиною аналізу і підставою для розрахунку страхового тарифу. Компаніям, які хочуть застрахувати свої активи правильно необхідно звернути увагу на наступні чинники:

- Вартість активу

- Вартість додаткової розробки активу
- Обслуговування
- Витрати на процес придбання активу
- Витрати на захист
- Цінність для власників та користувачів активу
- Цінність активу, якщо ним скористаються конкуренти
- Цінність інтелектуальної власності
- Ринкова ціна активу
- Ціна заміни активу
- Операційні витрати пов’язані з активом та його втратою
- Зобов’язання при втраті активу
- Корисність активу

Базою для визначення рівня ризику є допущення появи різноманітних подій. Щоб краще оцінити появу інформаційного ризику потрібно розробити комбінацію, яка б включала збір та обробку інформації щодо чутливості фірми до можливих загроз. Ця комбінація повинна змінюватися залежно від вихідних результатів таких як, кількість працівників з доступом до інформації, кількості обладнання, що використовується та яка система захисту наявна.

Нижче наведено чек-лист для визначення чутливості активів до різноманітних ризиків, проблем та явищ в тому числі і стихійних, які можуть не мати до сфери IT ніякого відношення. Потрібно пам’ятати, що ризик та загрози з’являються неочікувано. Чек-лист (Табл. 3.1.) заповнюється на основі припущення, що подія сталася і компанії тепер потрібно визначити скільки часу потрібно для налагодження попереднього рівня роботи компанії та наскільки складно відновити дані, активи та інші цінні речі. Фактор незахищеності (EF) вимірюється у % залежно від цінності активів. Активи, які можна швидко замінити матимуть

низький %, а такі активи, як бази даних, обладнання без резервів чи сервери матимуть високий %, оскільки замінити чи відновити їх набагато складніше.

Таблиця 3.1.

Чек-лист для компанії на визначення чутливості активів до подій

Ймовірна подія, явище, ризик	**Чутливість наявних активів до події (%)**
Зараження комп'ютерної мережі вірусом	
Кримінальна активність (викрадення IP, розтрата коштів, тощо)	
Втрата всіх даних	
Хакерська атака	
Неправильне використання даних, ресурсів чи сервісів	
Поломка обладнання	
Зловживання персональними привілеями співробітниками	
Помилки співробітників при використанні активів	
Незадоволені співробітники	
Політичні чи воєнні обмеження. Обмеження з боку влади	
Стихійні лиха	
Пожежа	
Зміна напруги	
Зміна температури	
Банкрутство	
Фізична крадіжка активів	

Джерело: Побудовано автором на основі данних [10]

Наступним кроком потрібно розрахувати (3.1) очікування від одноразової втрати (SLE), який показує скільки компанія втратить грошей, якщо актив буде пошкоджено чи викрадено.

Формула для розрахунку:

$$SLE=AV*EF \tag{3.1}$$

де AV – вартість активу

EF – фактор незахищеності

Потім необхідно розрахувати річний показник появи події (ARO), який визначає, як часто перелічені у чек-листу події трапляються на рік. Він оцінюється від 0 до великих чисел. Цей показник розраховується на основі визначення ймовірності, як і історичних подій, статистичного аналізу так і керуючись особливими географічними умовами для регіонів, в яких знаходяться активи компаній (для стихійних явищ).

Фінальним показником для аналізу ризику є річна очікувана сума втрати коштів (ALE), яка розраховується за формулою (3.2):

$$ALE=SLE*ARO \tag{3.2}$$

де SLE – очікування від одноразової втрати

ARO – річний показник появи події

Можливий розгляд дослідження взаємозв’язків на вразливість між конкретними одиницями IT обладнання та матеріальними та нематеріальними активами, як публічна, конфіденційна, фінансова, та службова інформація, репутація, активи та витрати на відновлення, програмне забезпечення, тощо.

Також можливий розгляд окремих загроз між цими же одиницями обладнання та різноманітними загрозами, як спам, внутрішні атаки, шкідливий код, помилки співробітників та відмова або закінчення терміну дії обслуговування.

Якщо успішно запровадити таку комбінацію, можна вдало оцінювати взаємозв'язки та своєчасно захистити і застрахувати вразливі сфери компанії.

Неодмінно, потрібно включити до полісу страхування хмарні технології, Big Data та всі портативні пристрої, які знаходяться на балансі компанії. Більшість офісів вже давно використовує робочі планшети та смартфони, які теж є дуже вразливими до вірусів, як допоміжне обладнання до стаціонарних комп'ютерів.

Необхідною дією є визначення в договорі всіх можливих нюансів пов'язаних з втратою даних та загроз для обладнання та доповнення правил страхування майна:

До розділу «Предмет страхування» віднести всі сервери, комп'ютери, ноутбуки та інші гаджети, які приєднані до мережі.

До розділу «Страхові ризики» віднести існуючі кібер-злочини та події з чек-листа

До розділу «Порядок визначення страхової суми» додати рівні суттєвості кожного з видів ризику до розрахунку страхової суми

До розділу «Термін страхування» зазначити, що шкідливі коди та хробаки можуть «спати» в обладнанні и проявити себе з часом.

До розділу «Підстави для розірвання договору та відмови виплати СС» додати, що працівник може навмисно не дотримуватися правил безпеки наданими СК, або що вид кібер-загрози неможливо точно оцінити у грошовому вигляді.

3.3. Нормативно-методологічні акти та алгоритми

Кількість злочинів та сума збитків від кібер-атак вказує на те, що організації починають вважати за необхідне страхувати свій бізнес, тож детально розглянемо що кібер-страхування зазвичай покриває. Незважаючи на відсутність стандартів для оформлення цих полісів, сучасний поліс страхування від кібер-ризиків повинен містити наступні складові:

- Розслідування: необхідно обов’язково додати розслідування форензік експерта до полісу, щоб визначити, що сталося та як відновити пошкодження і як запобігти виникненню такої ж шкоди в майбутньому.
- Бізнес-збитки: поліс кіберстрахування може включати подібні елементи, які охоплюють грошові втрати внаслідок простою мережі, переривання діяльності, відновлення втрат даних та витрат пов'язаних з уладненням кризи, результатом якої є пошкодження репутації компанії.
- Конфіденційність та сповіщення: включає в себе необхідні повідомлення про крадіжку даних для клієнтів та інших зацікавлених сторін, які мають регулюючий характер, та моніторинг для клієнтів, чия інформація була або може бути порушена.
    - Судові позови та вимагання: судові витрати, пов'язані з витоком конфіденційної інформації та інтелектуальної власності, юридичних розрахунків та нормативних штрафів.

Додатками до цього полісу можуть бути такі чинники:

- Покриття повинне застосовуватися як до першої, так і до третьої сторони. Будь-яка атака, а не тільки цілеспрямована, що впливає на компанію, повинна відшкодовуватися.
- Охоплення не шкідливих дій працівників під час атаки
- Часові рамки, застосування відшкодування

При придбанні полісу надаються детальні запитання про комп'ютерну систему фірми та її політику безпеки. Нижче наведений список ключових пунктів за якими необхідно надати відповідь:

- Безпека мережі
- Відповідальна особа
- Політика безпеки

- Нові працівники
- Віддалений доступ
- Конфіденційні дані
- Резервне копіювання та зберігання даних.
- Аутсорсинг
- План реагування

Таким чином, загальний чек-лист для підприємця, який хоче придбати поліс страхування від кібер-ризиків виглядає у таблиці 3.2.

Таблиця 3.2.

Чек-лист для підприємця

Запитання щодо фірми:	**Відповідь**
Які типи заходів безпеки має ваша фірма?	
Чи є у нього брандмауер, захист від вірусів і шкідливих програм, програмне забезпечення для виявлення вторгнень, безпечна система паролів і т.д.?	
Чи регулярне оновлення програмного забезпечення?	
Хто відповідає за безпеку мережі?	
Чи є у вас політика фізичної та мережевої безпеки?	
Ви проводите перевірку всіх нових працівників?	
Чи регулярно ви готуєте працівників з питань безпеки даних?	
Чи працюють співробітники, клієнти або інші користувачі віддалено?	
Якщо так, то яка система існує для аутентифікації користувачів?	
Які види особистої інформації ви збираєте, передаєте або зберігаєте?	
Ви шифруєте дані?	
Скільки записів, що містять таку інформацію, ви обробляєте щороку? Як контролювати доступ до конфіденційних даних?	
Ви періодично перевіряєте заходи контролю даних?	

Ви щодня виконуєте резервне копіювання даних?	
Де зберігаються резервні копії?	
Чи є у вас письмовий план реагування на порушення даних, який ви б дотримувалися у випадку комп'ютерного інциденту?	

Джерело: складено автором на основі даних [23]

Після аплікаційного чек-листа потрібно визначити на якому рівні захищеності від різноманітних атак знаходиться фірма в конкретний проміжок часу і що можна покращити у найкоротший термін. Стадії визначаються безпосередньо страховиком за рівнем суттєвості наявних превентивних заходів.

Пропонуються наступні стадії захищеності:

Не захищена – у такому разі компанії пропонується виконати мінімальні заходи для поліпшення стану захищеності, які може запропонувати СК.

Помірно захищена – на цій стадії страховик пропонує комплекс превентивних заходів та покращене програмне забезпечення для обладнання.

Середньо захищена – компанія слідкує за своєю інтернет-безпекою на 50% та потребує більш професійного страхового захисту у разі настання інциденту.

Достатньо захищена – компанія готова до кібер-атак, але хоче застрахувати свої активи для профілактики.

Після підписання договору СК повинна розробити план дій для страхувальника у разі кібер-атаки та надати консультацію, як уникнути будь-яких загроз для даних, обладнання та іншого майна в інтернеті.

Алгоритм чітких дій у разі добровільного страхування від кібер-ризиків та інших загроз повинен виглядати наступним чином (Рис. 3.6.). З його допомогою можна розробити певний план дій після укладання поліса.

Рис. 3.7. Алгоритм дій для страховика та страхувальника при заключені поліса кібер-страхування

Джерело: складено автором.

Конкурентну перевагу на ринку страхування отримають СК, які при розробці страхових тарифів будуть керуватися індивідуальним підходом до окремих компаній та якіберуть до уваги на особливості їх роботи та особливості сфери їх діяльності загалом.

ВИСНОВКИ

Страхування кібер ризиків щорічно розвивається і є необхідним елементом розгалуженої інфраструктури ринку страхування. У розвинених країнах страхування забезпечує клієнтам надійний захист їхніх інтересів у разі настання страхових випадків, таких як: природні та техногенні катастрофи, фінансові ризики, крадіжки, пожежі та інші. Наразі новим для України є страхування кібер-зазгроз.

Відсутність належної законодавчої бази призводить до труднощів у страхуванні окремих складових кібер-загроз. Після появи Закону про основні засади забезпечення кібер-безпеки виділено основні терміни, які полегшують ідентифікацію загроз та дають можливість застрахуватися від них. Імплементування законодавчих актів у сфері страхування та забезпечення кібербезпеки на рівні держави стане поштовхом для розвитку ринку страхування в Україні. Західний підхід до оцінювання компаній на готовність до загроз та їх рекомендації є важливим прикладом, як потрібно захищати будь-який бізнес чи державний заклад. Українськими експертами ще не було створено оцінювання кібер-ризиків та взаємозв’язок між загрозами та активами.

У роботі проаналізоване страхове поле внаслідок якого виявлено, що тільки одна з п’яти страхових компаній публічно оголосила свою готовність до страхування від різноманітних кібер-ризиків. Була запропонована класифікація компаній на предмет бажання застрахувати себе від цих атак та чітко виокремлені кібер-злочини. Наявність більше 11 тисяч злочинів в Україні за 2018 рік у сфері інтелектуальної власності та інформаційної безпеки свідчить про нагальну необхідність страхувати компанії від майбутніх випадків.

Найголовнішою проблемою роботи є відсутність алгоритму страхування та методології оцінювання ризиків. Наявність численних щомісячних збитків для компаній державного то комерційного сектору і відсутність розповсюджених страхових рішень, щоб запобігти цьому виділяє страхування від кібер ризиків важливим елементом для продуктивного існування установ. У роботі була звернута увага на можливі тенденції розвитку шахрайства в інтернеті, та які сфери можуть бути пошкоджені в наслідок нього. Був проведений кластерний аналіз найбільших витоків даних з 2004 року, який виявив 8 окремих кластерів та 3 найрозповсюдженіших галузей, котрим необхідно приділити максимальну увагу кібербезпеці, а саме: державний та фінансовий сектор, а також сфера продажів різноманітний товарів (retail).

Після аналізу іноземного досвіду, який є досить інноваційним, було розроблено два чек-лист для фірми, що бажає застрахувати себе, перелічено складові, щоб правильно визначити вартість активу. Перелічені найрозповсюдженіші загрози, на основі яких можна визначити фактор незахищеності. Розроблено алгоритм визначення розміру грошової втрати, якщо актив буде втрачено чи пошкоджено. Запропоновано алгоритм подальших дій для страховика та страхувальника. Виокремлені компоненти, на рівень захищеності яких бажано звернути увагу при страхуванні та стадії захищеності компанії від кібер-атак загалом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України про страхування. – [Електронний ресурс] - URL: https://zakon.rada.gov.ua/laws/show/85/96-%D0%B2%D1%80
2. Базилевич В.Д. Страхова справа. – К.: Знання, 1997. , 1997. – 216 с.
3. Страхування: навч. посіб. / Т.А. Говорушко, В.М. Стецюк; за ред. Т.А. Говорушко. – К.: – Львів: «Магнолія 2006», 2014. – 328 с.
4. Пічугіна Ю. В. Страхування. Конспект лекцій. – [Електронний ресурс] – URL: http://liber.onu.edu.ua/metodichki/epf/konspect_lekc_strahuv_2018.pdf
5. Бридун Є. В. Лекція №2 . – [Електронний ресурс] - URL: https://prestige-ic.com.ua/storage/other/tema_2.pdf
6. Поняття про кібер-ризик . – [Електронний ресурс] - URL: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/
7. Опис кіберзлочинності та покарання за них. – [Електронний ресурс] - URL: https://vseosvita.ua/library/prezentacia-kiberzlocini-ta-pokaranna-99852.html
8. Відшкодування збитків після кібер-атаки. – [Електронний ресурс] - URL: https://www.insa.com.ua/blog/kiberataki-kak-zashhitit-biznes-ot-novogo-oruzhiya/
9. Підсумки 2018 року кіберполіції. – [Електронний ресурс] - URL: https://cyberpolice.gov.ua/results/2018/
10. Закон України про основні засади забезпечення кібербезпеки. – [Електронний ресурс] - URL: https://zakon.rada.gov.ua/laws/show/2163-19
11. Mike Chapple, James Michael Stewart, Darril Gibson. CISSP. – К.: John Willey & sons, 2018.

12. Загальний опис превентивних заходів для кібер безпеки компанії. . – [Електронний ресурс] - URL: https://www.nibusinessinfo.co.uk/content/common-cyber-security-measures
13. Оцінка кібер безпеки. – [Електронний ресурс] - URL: https://www.cisa.gov/cybersecurity-assessments
14. Загальний опис кіберполіції України. – [Електронний ресурс] - URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%96%D1%86%D1%96%D1%8F_(%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B0)
15. Консолідовані дані для аналізу показник. – [Електронний ресурс] - URL: https://www.nfp.gov.ua/ua/Konsolidovani-zvitni-dani.htm
16. Огляд ринку страхування за 2019 рік . – [Електронний ресурс] - URL: https://nfp.gov.ua/files/OgliadRinkiv/SK/sk_2019.pdf
17. Тренди, які передбачаються у кіберзлочинах. – [Електронний ресурс] - URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A2%D1%80%D0%B5%D0%BD%D0%B4%D1%8B_%D1%80%D0%B0%D0%B7%D0%B2%D0%B8%D1%82%D0%B8%D1%8F_%D0%98%D0%A2_%D0%B2_%D1%81%D1%82%D1%80%D0%B0%D1%85%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B8_(%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%81%D1%82%D1%80%D0%B0%D1%85%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B8_%D1%82%D0%B5%D0%BB%D0%B5%D0%BC%D0%B0%D1%82%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5)
18. Страхування: Підручник./ Керівник авт.кол. і наук. ред. Осадець С.С. -К.: КНЕУ, 1998. -528с
19. Звіт від Cyber Ventures за 2018 рік. – [Електронний ресурс] - URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

20. Приклади страхування кібер-ризиків від українських страхових компаній. – [Електронний ресурс] - URL: https://delo.ua/special/kak-kompanii-strahujut-kiber-riski-v-ukraine-346724/

21. Новий продукт від компанії AIG для страхування ризиків. – [Електронний ресурс] - URL: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:AIG_CyberMatics_CyberEdge_%D0%A1%D1%82%D1%80%D0%B0%D1%85%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%80%D0%B8%D1%81%D0%BA%D0%BE%D0%B2

22. Оцінка кібер-ризику. – [Електронний ресурс] - URL: https://insfero.com/business/drugie-vidy-strahovaniya/strahovanie-kiber-riskov/

23. План для підприємця уникнення від кібер-ризику. – [Електронний ресурс] - URL: https://www.thebalancesmb.com/cyber-liability-insurance-coverage-for-data-breaches-462582

24. Найбільші витоки даних у світі в період 2004-2020 років. – [Електронний ресурс] - URL: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/