КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Факультет комп'ютерних наук та кібернетики

Кафедра прикладної статистики

Кваліфікаційна робота

на здобуття ступеня бакалавра

за спеціальністю 124 Системний аналіз

на тему:

Моделі прийняття рішень у сфері кіберстрахування

Виконав студент 4-го курсу

Решетніков Вадим Олексійович

Науковий керівник :

доцент, кандидат фіз.-мат. наук

Розора Ірина Василівна

Засвідчую, що в цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент

Роботу розглянуто й допущено до захисту на засіданні кафедри прикладної статистики

«06» червня 2022р.,

протокол № 11

Завідувач кафедри

Розора Ірина Василівна

Київ - 2022

АНОТАЦІЇ

Дипломна робота складається зі вступу, 3 розділів, висновку, списку використаних джерел, лістингу програми. Загальний обсяг роботи становить 50 сторінок, основний текст роботи викладено на 35 сторінках.

Ключові поняття: КОНТРАКТ, ОЦІНКА РИЗИКІВ, СТРАХУВАННЯ, ПРИЙНЯТТЯ РІШЕНЬ, КІБЕРРИЗИК, СТРАХОВИЙ ВИПАДОК, ПОЛІС, СТРАТЕГІЗОВАНА ФРАНШИЗА, КІБЕРСТРАХУВАЛЬНИК, ОПТИМАЛЬНА ПРОПОЗИЦІЯ.

Об’єктом роботи є розгляд проблеми прийняття рішень в умовах страхування сучасних кіберстрахових компаній. Предметом роботи є моделі оцінки кібер-ризику та визначення умов кіберстрахування.

Метою роботи є демонстрування технології оцінки ризику та визначення умов страхування для кіберстрахової компанії.

Інструменти та методи розробки: огляд методів страхування та їхнє застосування для оцінки кіберризиків. При розробці обчислювального програмного пакету була використана мова програмування C++ та фреймворк QT5 для створення візуального інтерфейсу програми.

ЗМІСТ

АНОТАЦІЇ

ВСТУП **4**

РОЗДІЛ 1. СПЕЦИФІКА РОБОТИ СУЧАСНОЇ КІБЕРСТРАХОВОЇ КОМПАНІЇ **5**

1.1 Моральний ризик **5**

1.2 Управління IT-ризиками **6**

1.3 Аналіз полісів кіберстрахування **7**

РОЗДІЛ 2. ОЦІНКА КІБЕР-РИЗИКУ **11**

2.1 Методи ідентифікації ризиків **11**

2.2 Методи запобігання кіберзагроз **14**

2.3 Методи зменшення кіберризиків **16**

РОЗДІЛ 3. МОДЕЛЬ СТРАХУВАННЯ **19**

3.1 Загальна модель **19**

3.2 Оптимальна франшиза та ціна необізнаності **25**

3.3 Функції корисності та кіберзбитків **28**

ВИСНОВКИ **31**

ЛІСТИНГ ПРОГРАМИ **34**

ВСТУП

Оцінка сучасного стану об’єкта розробки. Нинішній рівень витонченості технологій безпеки не забезпечує повного імунітету від ризику безпеки ІТ. Одним із способів, яким фірми намагаються покрити ризики інформаційної безпеки, є спочатку інвестування в технології безпеки, а потім купівля страховки залишкового ризику. Кіберстрахування відноситься до контрактів, які пом’якшують проблеми відповідальності, втрати майна та крадіжки. Ці контракти також можуть покривати фінансові збитки в результаті пошкодження даних, втрату доходу від збоїв у безпеці мережі, кібер - вимагання, кібертероризм, збори за зв’язки з громадськістю після інциденту та відшкодування коштів у фонд винагород

Актуальність роботи та підстави для її виконання. В останні роки кіберстрахування активно розповсюджується, оскільки Управління підзвітності уряду США (GAO) в нещодавньому аналізі ринку, що розвивається, відзначило, що частка клієнтів страхування, які додають кібер-покриття, зросла з 26 відсотків у 2016 році до 47 відсотків у 2020 році. Ця тенденція, у свою чергу, спричинила постійне зростання кількості кіберстрахувальників, яка досягла 577 клієнтів за останніми підрахунками Національної асоціації страхових комісарів (NAIC) , створивши преміальний пул, оцінений у 3,15 мільярда доларів у 2019 році. Зростання темпів, ймовірно, триватиме й у найближчі роки, оскільки зростаючий профіль широкомасштабних кібератак — і супутній фінансовий ризик, який вони накладають — спонукають директорів компаній і керівників обмежити ризик компромісу своєї компанії з кібербезпеки.

РОЗДІЛ 1. СПЕЦИФІКА РОБОТИ СУЧАСНОЇ КІБЕРСТРАХОВОЇ КОМПАНІЇ

Порушення безпеки негативно впливають на прибуток, ринкову капіталізацію та імідж організації. Глобальні організації вдаються до використання технологічних пристроїв, щоб зменшити частоту порушення безпеки. ***Кібер-ризик*** визначається як ризик, пов’язаний зі зловмисною електронною подією, що спричиняє порушення діяльності та грошові втрати.

Організації інвестують мільйони доларів у програми безпеки, такі як брандмауери, антивірусні системи та системи виявлення вторгнень, щоб мінімізувати порушення безпеки від атак, таких як злом, фішинг та спам. Тим не менш, новий вірус або спритний хакер можуть легко скомпрометувати ці системи виявлення, що призведе до мільйонних збитків щорічно. Організації також використовують цифровий підпис і шифрування для забезпечення конфіденційності і цілісності своїх даних. Проте атаки підслуховування та атаки «людина посередині» (MnM) поширені. Використання суворої технологічної політики забезпечується для аутентифікації та дозволу окремих осіб на доступ до даних.

1.1 Моральний ризик

Зростанню кіберстрахування гальмують дві серйозні проблеми. Пов'язані та взаємозалежні властивості кіберризиків значно підвищують економічний ризик страхових компаній. Ці дві властивості можуть перешкоджати об'єднанню ризиків. Далі ця ситуація може погіршитися, оскільки кіберстрахування негативно впливає на інвестиції для самозахисту. Це явище розглядається як попередній моральний ризик.

Попередній моральний ризик означає, що кіберстрахування негативно впливає на інвестиції в самозахист. Однак і страховики, і застраховані

очікують уникнути високого ризику, пов’язаного з погіршенням безпеки. Тому виник великий попит на спеціальні стратегії, щоб стимулювати користувачів інвестувати в самозахист.

1.2 Управління IT-ризиками

Запропонуємо структуру використання кіберстрахування для пом’якшення інформаційного ризику, який не можна подолати за допомогою технологій. У цих рамках організація повинна оцінити власний інформаційний ризик і профіль організаційного ризику, а потім заповнити технологічний пробіл (залишковий ризик) за допомогою використання відповідних фінансових інструментів (контрактів кіберстрахування). Ця робота розвивається, виходячи з єдиної передумови залишкових інформаційних ризиків, які неможливо зменшити за допомогою наявних на даний момент технологій. Дослідимо спостережувані наслідки впливу порушень на ціни акцій постраждалих фірм за допомогою дослідження подій, узагальнюючи негативний вплив. Модерування результатів дослідження подій, проведене Cavusoglu et al. (2004), Campbell et al. (2003) стверджують, що економічні наслідки порушення, про яке повідомляється, залежать від основних активів, постраждалих від порушення: пояснюючи, що порушення безпеки, які передбачають несанкціонований доступ до конфіденційних даних, приносять більший негативний економічний вплив, ніж інакше. По суті, структура нашої моделі об’єднує інтуїцію, розроблену фундаментальною роботою Borch (1960), і спостережувану вторинну втрату реалізованого порушення (Cavusoglu et al., and Campbell et al.), тоді як наша модель тлі дещо нагадує, що Голльєра (1996). Однак, на відміну від роботи Голльєра, де існує нестрахований фоновий ризик сам по собі, у нашій роботі вторинний збиток (і його ризик) спричиняється актом розкриття інформації про порушення (явним чи неявним) і частково або повністю контролюється застрахованими компаніями. 'кінець. На відміну від робіт Чавушоглу та ін. та Кемпбелл та ін., вторинна втрата від порушення IT є не наслідком, а рушійною силою для подальших стратегій у нашій моделі

1.3 Аналіз полісів кіберстрахування

Кіберстрахування, як і більшість страхових продуктів, зазвичай розрізняє дві широкі категорії збитків: «перша сторона» і «третя сторона». Збитки першої сторони стосуються збитків, яких безпосередньо зазнав страхувальник (тобто «перша» сторона договору страхування), тоді як відповідальність третьої сторони стосується претензій, пред'явлених сторонами, зовнішніми за договором (тобто «третьою» стороною), які зазнають збитків нібито через поведінку страхувальника.

Приведемо статистичний приклад. З 235 полісів, зібраних у Пенсільванії, Нью-Йорку та Каліфорнії, 54 мали повні форми покриття та виключення (2 з яких були дублікати) у період з 2009 по 2016 рік. Крім того, ми зібрали 15 форм покриття та виключення, опублікованих великими страховими компаніями. (з неприйнятого ринку), загалом 67 унікальних полісів.

Було виявлено, що покриття збитків було більш послідовним у всіх політиках, тоді як виключення були більш різноманітними. Наприклад, після перегляду лише 6 полісів 88% покритих збитків було закодовано, а до 37-го поліса ми досягли повного насичення (верхня панель). Тобто знадобилося лише 37 полісів, перш ніж ми визначили всі покриття збитків від політик у нашому наборі даних. Для порівняння, після 16 політик ми досягли 71% насичення для виключень і досягли повного насичення за 60-ю політикою (нижня панель).

Покриття збитків від кіберінцидентів можна класифікувати кількома різними способами, і один спосіб полягає в тому, щоб розрізняти збитки, понесені в результаті інциденту (збитки першої сторони), і збитки, понесені в результаті судового розгляду передбачуваними потерпілих осіб (збитки третіх осіб). Нижче ми обговоримо їх докладніше.

Покриття першої сторони включає збитки, понесені безпосередньо страхувальником. Наприклад, витрати, пов’язані з розслідуванням причин порушення даних або інциденту безпеки, витрати, пов’язані

з відновленням бізнес-послуг, витрати на сповіщення постраждалих осіб, послуги кредитного моніторингу, витрати, пов’язані з зв’язками з громадськістю та засобами масової інформації, щоб повідомити про подію, вимагання та викупу, і збитки, пов'язані з перервою в бізнесі.

Щоб керувати різними ризиками, пов’язаними з такими кіберінцидентами, перевізники часто призначали субліміти (а в деяких випадках і окремі премії) групам втрат першої сторони. Наприклад, деякі політики відрізняються лише за кількома категоріями, такими як компрометація особистих даних та комп’ютерна атака. Компроміс персональних даних стосується «втрати, крадіжки, випадкового оприлюднення або випадкової публікації особистої інформації (PII) або особистої конфіденційної інформації». Комп’ютерна атака пов’язана з несанкціонованим доступом, атакою зловмисного програмного забезпечення або атакою відмови в обслуговуванні (DoS) на будь-який комп’ютер або електронне обладнання, що належить або орендується та керується страхувальником.

Відповідальність перед третіми сторонами покриває витрати на захист від публічних або приватних судових процесів, урегулювання, судові рішення чи інші рішення, а також штрафи, збори та розрахунки, що випливають із цих позовів. Наприклад, покриття відповідальності за безпеку мережі покриває витрати, пов’язані з «цивільним позовом, альтернативним спором, розглядом справи або письмовою вимогою про гроші» в результаті «порушення ділової інформації третьої сторони», ненавмисне розповсюдження або пересилання зловмисного програмного забезпечення, ненавмисне сприяння атаці відмови в обслуговуванні».

Подібно до збитків першої сторони, покриття доступне, а ліміти розподіляються між різними видами претензій.

Наступним компонентом полісів кіберстрахування, який потрібно перевірити, є анкети безпеки. Ці анкети призначені для отримання

всебічного розуміння (або принаймні розумного наближення) загального стану безпеки заявника. Більше того, запитання повинні допомогти «диференціювати» ризики в портфелі претендентів.

З 235 страхових документів, які були проаналізовані, 31 мала ці анкети. У восьми випадках було включено кілька анкет, а у випадках, коли анкети були різними (оскільки вони були написані для різних типів заявників, або використовували різні анкети для подання заявки та поновлення), вони кодувалися окремо, створюючи загальну суму з 45 анкет. Потім виявлено 11 випадків дублювання анкет, які були виключені з аналізу. В результаті було створено 34 унікальні закодовані анкети.

Кожна анкета була детально проаналізована та порівняна з наявними запитаннями та категоріями в кодовій книзі. Хоча більшість запитань були простими для коду (наприклад, «чи дотримується заявник певного технічного стандарту?»), деякі вимагали додаткового вивчення, щоб розрізняти пов’язані питання. Тому, як це є стандартною практикою, кодування виконувалося з використанням ітераційного процесу, який передбачав додавання нових запитань або об’єднання/розділення існуючих питань на основі зростаючого розуміння окремих тем і категорій (наприклад, захоплення нових підкатегорій, таких як політика керування, політика конфіденційності та Технологічна політика). Для достовірності дослідник переглянув кодову книгу, щоб порівняти та відкоригувати кодування, якщо це необхідно. Збірка з 10 політик (22%) була потім перевірена на точність і виявлено 5 розбіжностей.

В анкетах також йшлося про те, як заявник керує своїми відносинами з аутсорсинговими постачальниками та послугами, на які покладається заявник для ведення бізнесу. З огляду на те, що зазвичай передають послуги на аутсорсинг і використовують сторонніх постачальників послуг, ці питання були відносно поширеними. В анкетах застрахованих просили вказати перелік

послуг, які передані стороннім організаціям, та надати назви постачальників, а деякі навіть надали вичерпний список для вибору заявника. Наприклад, «Заявник аутсорсує будь-яку частину мережі, комп’ютерної системи або функції інформаційної безпеки Заявника».

Запитальники також оцінювали, чи була проведена оцінка безпеки, конфіденційності та/або ризику щодо стороннього постачальника. Історія сторонніх постачальників оцінюється з огляду на те, чи були вони об’єктами порушення конфіденційності чи безпеки в минулому. Крім того, перевірялися договори між страхувальником і третьою стороною, наприклад, чи були вони структуровані таким чином, щоб треті сторони брали відповідальність за збитки, спричинені порушенням даних та безпеки, або чи включали вони положення про відшкодування для передачі ризику третій стороні. . У деяких випадках в анкеті запитувалося, чи вимагає страхувальник від постачальника аутсорсингу достатньої кількості кіберстрахування, щоб мінімізувати будь-яку відповідальність, яку клієнт може вимагати в результаті інциденту з постачальником аутсорсингу (наприклад, порушення даних або безпеки на сайті постачальника аутсорсингу).

Резюмуючи, аналіз покритих і виключених втрат висвітлює низку важливих ідей. По-перше, як і у всіх видах страхування, існує чітка різниця між збитками першої та третьої сторони (тобто витратами, які несе фірма безпосередньо, порівняно з тими, що понесені через судовий процес), які стають релевантними для встановлення доларових значень лімітів та сублімітів.

Оскільки споживачі та фірми впроваджують більше технологій та підключених пристроїв, ймовірно, будуть переглянуті збитки, які чітко покриваються або виключаються полісами кіберстрахування. Однак із збільшенням кількості пристроїв, атак на системи (DDoS), що використовують пристрої IoT, повторного використання коду між продуктами та нестандартизованих методів безпеки програмного забезпечення розробників, виключення можуть стати

частішими. І хоча у договорі обговорювались традиційні комп’ютери, мережі та системи, не було прямої згадки про ризики, що виникають через мобільні пристрої, дрони та зростаючу взаємозалежність критичної інфраструктури.

РОЗДІЛ 2. МОДЕЛІ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО КІБЕРРИЗИКІВ

2.1 Методи ідентифікації ризиків

Зазвичай існує величезна кількість даних та інформації доступної з журналів подій, систем виявлення вторгнень та інших інструментів моніторингу, вразливості сканерів, результати тестування на проникнення та інші види оцінок безпеки, вихідний код інспекції тощо. Ми будемо намагатися повністю використовувати таку інформацію під час визначення ризику. Як в результаті ми проводимо ретельний огляд опису цілі, включаючи атаки та активи, щоб знайти будь-які потенційно корисні джерела інформації. Ці джерела зіставляються з відповідними цілями, які будуть корисними пізніше на етапі аналізу ризику. Це взагалі виконується в тісній співпраці з обслуговуючим персоналом, технічними менеджерами, менеджерами з безпеки або тих, хто глибоко знайомий з технічною інфраструктурою. Будь-які результати тесту, що стосуються Інтернет-інтерфейс терміналу вимірювання, наприклад, зіставляються з цим розділом поверхневих атак. Результати цих тестів потім допомагають нам визначити вразливі місця та небезпеки нападів. Важливо визнати, що під час аналізу даних, наприклад журналів подій, важливо уникати припущень, що завтра буде так само, як і вчора. Незважаючи на те, що небезпека там не виникла минулого разу, це не виключає можливості, що вона відбудеться в майбутньому. Відсутність споріднених події в журналах не виключає оцінку загрози чи події. Це особливо важливо розпізнати у разі рідкісних, але серйозних катастроф, таких як масштабна скоординована атака на системи вимірювання.

Аналогічно, те, що вразливість не знайдена за допомогою перевірки безпеки, не означає, що її не існує. Нам не потрібно думати про серйозність вразливостей чи можливість загроз та інциденти під час виявлення ризиків; на даний момент ми просто документуємо все, що може бути актуальним і залишити глибше вивчення на потім. Ми обов'язково ретельно оцінюємо, чи є частини цілі, які потребують додаткового захисту тестування, реєстрація/моніторинг або інше дослідження протягом усього процесу ідентифікації ризику, а також пізніше під час аналізу ризику. Однак є також питання часу та наявних ресурсів. Це також залежить від того, чи можна зібрати відповідні дані з інших джерел. Окрім згаданих вище джерел інформації для конкретних цілей, відкриті джерела, такі як міжнародні стандарти, онлайн-сховища та численні дослідження щодо кібербезпеки, загроз та вразливості можуть надати корисну інформацію для ідентифікації ризику. Наша ключова задача це під час використання таких даних необхідно визначити точні джерела релевантності та вибрати лише ті аспекти, які мають значення для нашої оцінки з цих джерел. Ось простий процес із чотирьох кроків:

1. Встановити критерії релевантності залежно від таких факторів, як тип системи чи домену з якими ми працюємо, активи, з якими ми маємо справу, або тип ризику, з яким ми маємо справу.
2. Використовувати зазначені критерії визначення джерел інформації.
3. Брати з цих джерел лише ті елементи, які є релевантними для нашої оцінки.
4. Перефразувати виділені елементи, які мають бути виражені в зрозумілих термінах, щоб вони стосувалися саме нашої мети оцінки та активів. Навіть коли ви маєте справу з кібер-системами, витягуючи інформацію не тільки з системних журналів, тестів безпеки та інших джерел, а також від людей, які близько знайомі

з об’єктом оцінки з їх унікальної точки зору є критичним для ідентифікації ризику.

Ці особи можуть включати творців центральної системи або вузлів обліку, команду технічного обслуговування центральної системи та операторів, співробітників та керівників з інформаційної безпеки, операторів системи розподілу, а також, можливо, деякі споживачі електроенергії.

Для визначення ризику ми також можемо застосувати мозковий штурм та інші подібні стратегії. На пленарному засіданні зустрічі, ключові зацікавлені сторони та особи, які з перших рук знають конкретні сфери чи компоненти цілі збираються, щоб сприяти процесу ідентифікації. Цей метод має перевагу дозволяючи учасникам обговорювати ідеї один одного та розвивати їх. Якщо одна людина, наприклад, виявляє слабкість, яку ніхто інший не врахував, решта групи може знайти шляхи експлуатації цього. Це може бути дуже ефективним, якщо ми зможемо зібрати відповідних людей. На жаль, мозковий штурм має кілька недоліків, про які ми повинні знати. Першим є те, що особистості учасників важливі, і існує ризик того, що вони будуть більш відвертими і окремі люди будуть домінувати, тоді як інші навряд чи внесуть свій внесок, що призведе до відсутності різноманітності точкок зору. Окремі учасники також можуть використати цей час, щоб досягти власного порядку денного та зосередитися на актуальні для них теми. Інші небезпеки включають можливість того, що дебати відхиляться і що обмежений час не буде розподілено рівномірно між питаннями, які підлягають обговоренню. Як наслідок, для проведення мозкових штурмів потрібен висококваліфікований оцінювач ризиків. Це також вимагає, щоб ми заздалегідь передбачили, як ми будемо структурувати та керувати обговоренням. Активи, типи джерела загроз, типи вразливостей або розділи опису цілі чи поверхні атаки, це все можуть використовувати для побудови конструкції. Як ми організовуватимемо мозковий штурм, залежить від нас, але загалом це залежить від мети оцінки, будь-якої уподобання учасників та етап процесу

визначення ризику, з яким ми працюємо. Це може також ускладнити документацію льготного процесу. У результаті нам потрібно буде найняти спеціального секретаря для вирішення цього завдання. Ми могли б використовувати відео або аудіозаписи, якщо всі учасники згодні, але ми не пропонуємо цього, оскільки це може перешкодити учасникам. На більш практичному рівні, зібрати всіх учасників разом для мозкового штурму може бути важко. Джерела інформації щодо ідентифікації ризику та методології, які слід використовувати, визначаються числом факторів, включаючи наявні ресурси та джерела інформації, а також тип цілі. Наприклад, відповідна ідентифікація ризику для стандартного веб-додатка або служби некритичної системи, швидше за все, може базуватися значною мірою на загальних стандартах і бібліотеках кіберзагроз і вразливості. Ідентифікація ризику, з іншого боку, набагато складніша, якщо мати справу з а високоспеціалізованою критична системою. У результаті ми намагаємося комбінувати методики, щоб отримати більш повну картину та підтвердити результати. Якщо, наприклад, інтерв'ю виявляють побоювання щодо наявності конкретних вразливостей або доцільності напади, сканування вразливостей та тестування безпеки можуть допомогти полегшити побоювання.

2.2 Методи запобігання кіберзагроз

Якщо фінансова операція (фінансове проведення) підприємства через мережу перехоплена, а крадіжка грошей чи інформації – це крадіжка, яка може бути розкрита протягом тривалого часу (якщо взагалі це вдасться). Крім того, повернуті кошти навряд чи вдасться повернути, а злодіїв навряд чи вдасться схопити. Набагато краще уникнути крадіжки, перш за все, і перша лінія захисту — придбати гарний набір засобів безпеки програмне забезпечення від надійного постачальника, яке включає антишпигунське, рекламне програмне забезпечення, зловмисне та антивірусне програмне яке забеспечує захист. Також необхідно мати опцію автоматичного оновлення, а також автоматизовану рутинну перевірку системи, а оновлення програмного

забезпечення слід завантажувати, як тільки вони стають доступними. Отримання допомоги від консультантів, таких як страховики кіберризиків, юристи, бухгалтери та ризик-менеджери, також є хорошою діловою практикою. Коли справа доходить до внутрішньої кіберкрадіжки, існує кілька основних практик, які використовуються підприємствами, щоб зменшити кібер-ризик, пов'язаний з фінансовими рахунками, наприклад, чекові рахунки, що захищені паролем, чеки дебіторської заборгованості, перевірки постачальників і заробітної плати, а також кредитні картки, квитанції. Оскільки багато кіберзламів залишаються невиявленими протягом тривалого періоду часу, додаткові заходи, такі як відокремлення виписування чеків та звірки рахунків, а також оскільки проведення неоголошених періодичних аудитів кредиторської заборгованості та сплачених чеків може допомогти уникнути безперервних кіберкрадіжок. За певний час компанія повинна накласти подвійний підпис для виписування чеків, а також ліміти витрат на кредитні картки персоналу. Якщо перевірки та перекази коштів не можуть здійснюватися таємно на регулярній основі, це запобігає (або пом'якшує) збитки, якщо кіберзлодій приєднається до системи. Подібні заходи слід застосовувати для захисту інтелектуального майна та цінну інформацію, як-от бази даних, наприклад заборонити доступ або вести автоматичний журнал про те, хто отримав доступ до певного запису або набору даних. Оскільки підприємства та некомерційні організації не мають такого ж правового захисту, як фізичні особи, кіберкрадіжка банківських рахунків (банк повинен відшкодовувати витрати фізичній особі, але не компанії), ініціативна ретельність особливо важлива для операцій, пов'язаних із фінансовими переказами через Інтернет. Поки страхування від кібер-крадіжок може забезпечити механізм контролю втрат від таких ризиків, зазвичай воно супроводжується франшизою і тому все ще несе ризик збитків для компанії. Крім того, у багатьох випадках внутрішньої кібер-крадіжки (серед співробітників) можна було б уникнути, якщо працівники, потенційні

працівники (і навіть члени правління) мали перевірку на судимість. Відмова погодитися на такі перевірки слід розцінювати як червоний сигнал.

Співробітники (неважливо термін перебування на посаді) також повинні проходити перевірку на кримінальну історію та перевірку кредитоспроможності кожні п’ять років, особливо якщо вони мають доступ до фінансових рахунків або повноваження для підписання чеків. Незадоволений персонал слід уважніше перевіряти, якщо вони мають доступ до критичної інформації, як зазначено раніше. Шифрування сигналів на обох кінцях каналу зв'язку, а також автентифікація вищого рівня перед тим, як дозволити доступ до потенційно вразливих місць системи, є прикладом подальших методів профілактики. Перш ніж надати доступ до рахунків, певні банки, наприклад, кожен раз застосовувують вторинний метод перевірки. Під час спроби увійти до облікового запису, особа отримує текстове або електронне повідомлення, що містить певний код, який має бути введено разом із паролем. Багато видів небажаного доступу до комп’ютерних систем компанії можуть запобігти за допомогою подібних способів, запобігаючи збиткам до того, як вони виникнуть.

2.3 Методи зменшення кіберризиків

Хоча не всіх ризиків можна уникнути, негативні наслідки можна зменшити за допомогою ретельного планування. Структури та методології управління ризиками, які виявляють вразливості інформаційної безпеки зазвичай використовуються компаніями, які прагнуть пом’якшити свій кіберризик. Організація (або третя сторона) проводить аудит безпеки з метою виявлення ризиків і вразливостей системи компанії як перший етап. Цей крок зазвичай передбачає перегляд комп’ютера для зовнішніх небезпек, а також огляд електронних мереж (включаючи зовнішній доступ працівниками та клієнтами). Компанії також опитують IT-менеджерів, щоб отримати інформацію про їхні поточні профілі ризиків та визначити фінансові наслідки процесу управління ризиками. Раніше консультуючись зі страховиками чи

спеціалістами з безпеки, багато компаній вживали запропонованих заходів організовуючи власну внутрішню відповідь, наприклад, налаштувати контроль доступу та встановити брандмауери. Дані шифрування, яке шифрує кожен документ так, що його неможливо прочитати, навіть якщо його викрадено, є критичним підходом зменшення ризику для бізнесу. Цей підхід майже унеможливлює атаки на бази даних або мобільні пристрої з третьої сторони, якщо документи зашифровані. Шифрування можна використовувати різними способами. Шифрування може виконуватися як для окремих файлів, так і для цілих архівів. Шифрування буває різних форм і масштабів.

Метод криптографії із закритим ключем і метод криптографії з відкритим ключем є найпоширенішими способами шифрування. Алгоритми закритого ключа, як правило, відносно швидкі та легко реалізуються в апаратному забезпеченні. Тому вони часто використовується для масового шифрування даних. Шифрування приватного ключа в основному використовується для шифрування файлів, каталоги та розділи, які відомі лише власнику даних. Алгоритм потокових шифрів і алгоритм блокових шифрів — це два основних типи алгоритмів приватного ключа. Потоковий шифр шифрує кожен байт даних незалежно і часто використовується в бездротовій мережі комунікації. З іншого боку, блочні шифри шифрують один блок даних за раз і в основному таке використовується для шифрування даних. У криптографії з відкритим ключем використовуються два різних, але пов’язаних ключі: відкритий ключ і приватний ключ. Будь-хто може мати доступ до відкритого ключа, і він використовується для шифрування даних призначених для власника приватного ключа. Закритий ключ залишається конфіденційним і використовується для розшифровки даних зашифрованих за допомогою відкритого ключа. Повідомлення електронної пошти, вкладені файли, цифрові підписи та інші операції, пов’язані з транзакціями, вимагають шифрування з відкритим ключем. Часто підприємства не усвідомлюють або недостатньо реагують на потенційне порушення, яке могло б статися.

Показники ефективності постраждалих фірм значно покращилися б, якби вони впровадили сучасні методи моніторингу вторгнення для виявлення атак або загроз у режимі реального часу. Консультанти з безпеки можуть допомогти у визначенні ризику, деталізації заходів щодо зменшення ризику, оцінці фінансових наслідків таких ризиків, завершення та моніторинг аудитів ризиків, а також виявлення кібер вразливості (оскільки середовище постійно змінюється).

Підприємства можуть запобігти ризику втрати даних, шифруючи сигнали на обох кінцях зв'язку. Аутентифікація вищого рівня перед наданням доступу також є запобіжним методом. Деякі банки застосовують вторинний метод підтвердження кожного разу, коли здійснюється доступ до облікового запису. Це тип шифрування, який шифрує кожен байт даних, надісланих провайдером, щоб запобігти перехопленню даних. Компанії можуть зменшити свій кіберризик за допомогою ретельного планування. Шифрування даних, яке шифрує кожен документ, щоб його неможливо було прочитати, навіть якщо його викрали, є важливим підходом до зменшення ризику підприємства. Компанії також можуть налаштувати контроль доступу та встановити брандмауери перед консультацією з професіоналами безпеки.

РОЗДІЛ 3. МОДЕЛЬ СТРАХУВАННЯ

3.1 Загальна модель

Умовні позначення використовувані у роботі:

F_i - страхова компанія, що пропонує кіберстрахування (передбачається нейтральний ризик)

F_d - компанія, що купує кіберстрахування (передбачається уникнення ризику)

W - Початковий капітал застрахованої фірми, константа

q - Ймовірність порушення безпеки IT

δ - Умовна ймовірність спрямованого порушення: A (спрямоване порушення)

γ - Умовна ймовірність приватного порушення: B (приватне порушення / спрямоване порушення)

x - реалізація кібер (первинних) збитків за порушенням для застрахованої фірми, за появи порушення

f(x) - Умовний розподіл кібер-збитків застрахованої фірми (відомий обом сторонам), за появи порушення

P - премія за договором кіберстрахування

Г - Стратегія претензії застрахованої фірми на приватне порушення

I - виплата відшкодування, $I(x) \geq 0$, $I'(x) \geq 0$,

G - Вторинні збитки після здійсненого порушення

U - функція корисності застрахованої фірми (передбачається увігнутою)

λ - коефіцієнт завантаження ринку застрахованої фірми (відомий обом сторонам).

Кіберстраховим договором є пара(P, I), так що коли застрахована фірма F_d виплачує передплату P, страховик F_i обіцяє виплату відшкодування I(x) у разі виникнення події зі кібер-втратою величини x. Попередня премія P залежить від розподілу ймовірності кібер-втрат x ($0 \leq x \leq \infty$) застрахованої фірми F_d та коефіцієнта завантаження ринку λ, який включає (серед інших) збори за оцінку готовності безпеки третіх осіб сторін та написання договору витрати. Оскільки ми припускаємо, що коефіцієнт завантаження ринку пропорційний очікуваній виплаті відшкодування страховиком, і що страховик є нейтральним до ризику, F_i пропонує договір кіберстрахування, оптимальний за Парето, що перебільшує франшизу x_1. Якщо припустити, що позови щодо збитків, що перевищують франшизу, підлягають виплаті в повному обсязі, виплата відшкодування надається:

$$I = 0 \qquad 0 \leq x \leq x_1 \tag{1}$$

$$I = x - x_1 \qquad x_1 < x$$

Страховик вимагає від страхової фірми здійснити авансовий платіж

$$P = q.(1+\lambda)\int_{x1}^{\infty}(x - x_1)\, f\,(x)dx\,, \tag{2}$$

де q - ймовірність порушення, а розподіл збитків f(x) умовно визначено для даного порушення. У страхової фірми є можливість вибору франшизи x_1 (тут передбачається безперервний), що впливає на рівень премії, нарахованої страховиком.

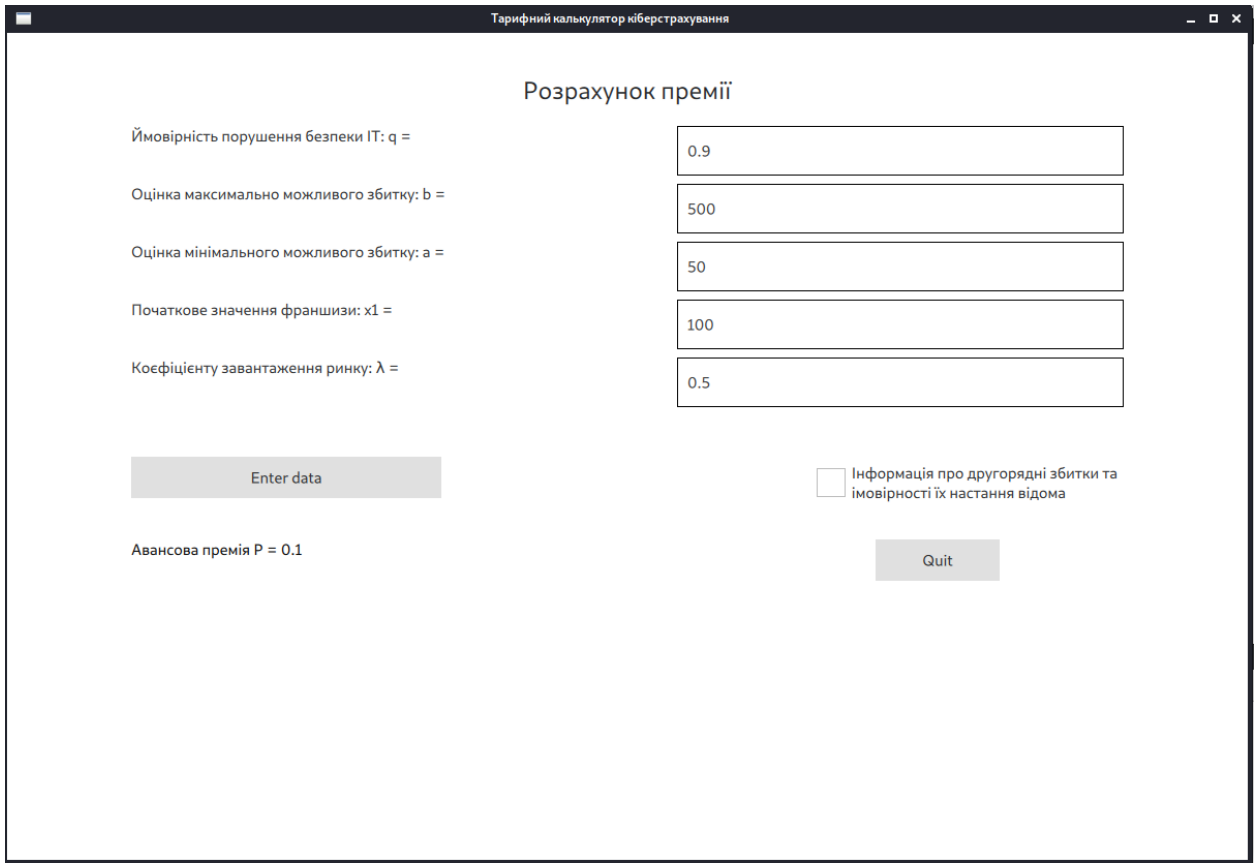

Рисунок 3.1 – Ілюстрація інтерфейсу для розрахунку Авансової премії P

На Рисунку 3.1 зображено інтерфейс програмного засобу, створеного під час виконання даної роботи, ця частина відповідає за введення початкових даних задля розрахунку Авансової премії P використовуючи формулу (2). Для розрахунку знадобиться внести інформацію про умовну імовірність уникнення порушення системи інформаційної безпеки фірми, експертні оцінки максимальних та мінімальних можливих втрат фірми за умови порушення безпеки, початкове приблизне значення франшизи (воно ще буде перераховуватись для отримання оптимальної франшизи) та коефіцієнт навантаження ринку, що за замовченням дорівнює 0.5. Розрахунок проводиться за припущенням про нормальність розподілу кібер-збитків .

На початку періоду контракту (як правило, рік) пишеться договір кіберстрахування. Це вимагає від страхової фірми повідомлення оптимальної франшизи x_1^*. Для кожної франшизи x_1^*, страховик пропонує оптимальний за Парето контракт (P*,I*), форма якого представлена формулами (1) і (2) вище.

Якщо оптимальна франшиза дорівнює 0, застрахована фірма купує повне страхування (100% передача ризику безпеки IT). Якщо оптимальна франшиза нескінченно висока, нарахована премія становить P* = 0, договору немає, і застрахована фірма приймає всі ризики (або «самострахування»). Між цими двома крайніми положеннями франшизи, всі договори мають бути створені, щоб оптимально передати частку IT-ризику страховику. Зауважимо, що функція втрат f(x) та коефіцієнт завантаження λ є загальновідомими в нашій моделі, тому запропонований контракт (P*,I*) у відповідь на повідомлений "оптимальний" обсяг франшизи x_1* завжди прийнятний для страхової фірми (припускаючи відсутність вторинних збитків). Порушення реалізується з ймовірністю q , а ймовірність того, що реалізоване порушення є спрямованим це δ. Направлене порушення стає відкритим з вірогідністю (1-γ) . Розкриття інциденту публічного порушення відбувається автоматично, а вторинні втрати G виникають разом з кібер-втратами x . Потім застрахована фірма претендує на виплату відшкодування. З іншого боку, спрямоване порушення є приватним із ймовірністю γ, а вторинні збитки G виникають лише у випадку, якщо страхувальна фірма подає відповідний позов. В іншому випадку, виникає тільки втрата x.

Життєвий цикл страхового полісу може бути зображений за допомогою ймовірнісної діаграми діяльності:

Страхова фірма спочатку приймає рішення щодо оптимальної франшизи x_1* та повідомляє про це застрахованій компанії. Маючи укладений договір при здійснені приватного порушення, застрахована фірма реалізує свою оптимальну стратегію вимог (при публічному порушенні застрахована фірма завжди вимагає відшкодування збитків відповідно до положень договору). Однак стратегія позову в приватному порушенні впливає на оптимальну

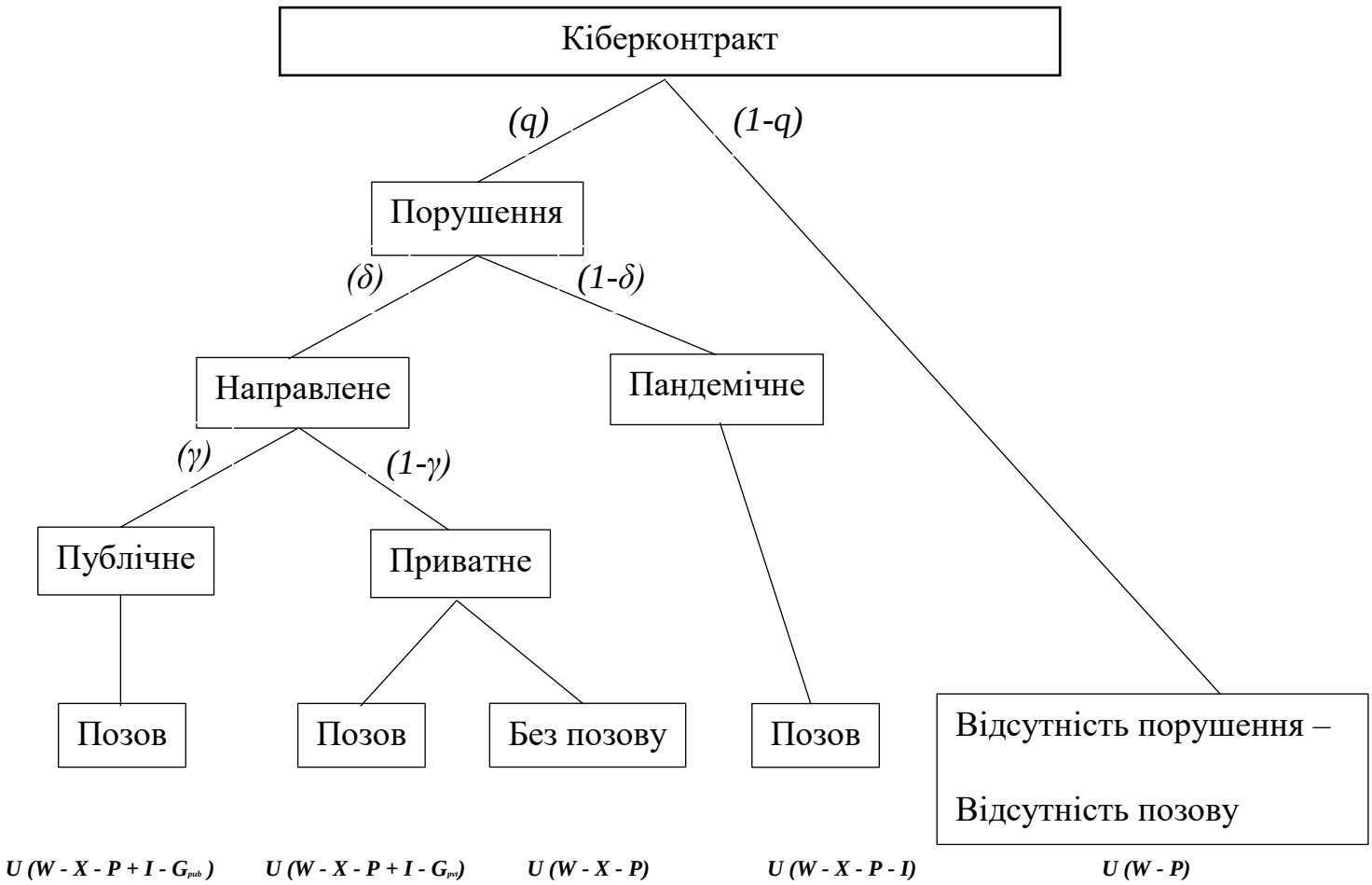

Рисунок 3.2 - Дерево надзвичайних ситуацій для виплат страховій фірмі за договором кіберстрахування

франшизу x_1^* в першу чергу. Тут ми використовуємо стандартний метод зворотної індукції, щоб спочатку з'ясувати оптимальну стратегію претензій у приватному порушенні, а потім – оптимальна франшиза x_1^*, що забезпечує максимальну очікувану корисність для застрахованої фірми. Зауважимо, що стратегія, яка претендує на порушення приватних порушень, неявно включає два рішення: "коли вимагати" та "скільки вимагати".

Визначимо змінну показника: Γ(x) =1, коли застрахована фірма вимагає реалізованих кіберзбитків x через приватне порушення; інакше Γ(x) = 0. Оскільки ми припускаємо, що постійний орієнтований на події вторинний збиток G , Γ(x) =1 може включати лише повне рішення про вимогу. Враховуючи стратегію подання претензії Γ(x), застрахована фірма максимізує наступне, щоб досягти своєї оптимальної франшизи x_1^*. (3)

$$\max_{x1,\Gamma(x)} \left\{ \begin{array}{l} q\delta\left\{\gamma \int_0^\infty U(W\text{-}x\text{-}P+\Gamma(x)I(x)\text{-}\Gamma(x)G)f(x)dx+(1\text{-}\gamma)\int_0^\infty U(W\text{-}x\text{-}P+I(x)\text{-}G)f(X)dx\right\}+ \\ \quad + q(1\text{-}\delta)\int_0^\infty U\big(W\text{-}P\text{-}x+I(x)\big)f(x)dx+(1\text{-}q)\int_0^\infty U(W\text{-}P)f(x)dx \end{array} \right.$$

Перший член в (3) відноситься до приватного порушення (ймовірність qδγ). Заявляти про приватне порушення означатиме явне виявлення порушення: але фірма може тут стратегізувати свою поведінку - таким чином, реалізована претензія дорівнює I = Γ(x)I(x) . Зауважте, що вторинні збитки при приватному порушенні виникають лише у випадку пред'явлення вимоги (тобто Γ(x) =1). Другий член являє собою випадок публічного порушення (ймовірність qδ(1-γ)). Інформація про публічне порушення доходить безпосередньо до зацікавлених сторін - вторинні збитки завжди завдані - і керівники не мають підстав відступати від передбаченої контрактом поведінки. Третій термін стосується ситуації, коли фірма зазнала пандемічного порушення (ймовірність q(1-δ)). Фірма зазнає кіберзбитків x ,

але від вторинних втрат не страждає: фірма заявляє про кіберзбитки та здійснює виплату відшкодування збитків. Четвертий термін стосується ситуації, коли фірма не зазнає порушення, маса ймовірності якої задається (1-q). Це також цілком відповідає представеній раніше у цьому розділі схеми на Рисунку 3.2.

3.2 Оптимальна франшиза та ціна необізнаності

Для постійних вторинних збитків G, пов'язаних з реалізованим приватним порушенням, існує мінімальний збиток r (=x_1+G), до якого застрахована фірма не вимагає своїх збитків, для збитків вищеr , застрахована фірма вимагає своїх фактична втрата.

Локальна задача оптимізації зводиться для пошуку довільної точки r на осі втрат такої, що очікуваний дохід

$$E[R(r)] = \int_r^{\infty} I(x)f(x)dx - (1 - F(r))$$

був максимізованим. Оптимальний розв’язок r: $r = I^{-1}(G)$. Однак точка r повинна лежати справа від точки x^1 (у фірми немає підстав подавати позов нижче франшизи та поглинати тільки вторинні втрати). Таким чином загалом: $r = I^{-1}(r - x_1)$.

Таким чином у разі приватних порушень існування вторинних втрат збільшує ефективність франшизи у договорі кіберстрахування. На відміну від (контрактної) поведінки, в межах $x_1 \leq x \leq r$, застрахована фірма не вимагає своїх збитків внаслідок приватного порушення. Також незатребувані збитки в межах $x_1 \leq x \leq r$ (хоча і піддаються контракту) зменшують загальне очікуване відшкодування від договору кіберстрахування. Важливо, що страховий договір із *фіксованою* франшизою не може змінити стратегію «*без претензій*» застрахованої фірми у діапазоні $x_1 \leq x \leq r$.

Знаючи точну стратегію позову у разі виникнення приватного порушення і супутню виплату компенсацій, ми можемо модифікувати (3) таким чином: (4)

$$\max_{x1}\left\{\begin{array}{l} \mathrm{q\delta\gamma}\left(\int_0^{x1+G} U(W-x-P)f(x)dx + U(W-\mathrm{x_1}-\mathrm{P}-\mathrm{G})(1-F(\mathrm{x_1}+\mathrm{G}))\right)+ \\ \quad +\mathrm{q\delta}(1-\gamma)\left(\int_0^{\mathrm{x1}} \mathrm{U(W\text{-}x\text{-}P\text{-}G)f(x)dx} + U(W-\mathrm{x_1}-\mathrm{P}-\mathrm{G})(1-F(\mathrm{x_1}))\right)+ \\ +\mathrm{q}(1-\delta)\left(\int_0^{\mathrm{x1}} \mathrm{U(W\text{-}x\text{-}P)f(x)dx} + U(W-\mathrm{x_1}-\mathrm{P})\left(1-F(\mathrm{x_1})\right)\right)-(1-\mathrm{q})(\mathrm{W}-\mathrm{P}) \end{array}\right.$$

Рішення (4) дає оптимальне значення франшизи x_1*, яке необхідне страховику задля укладання договору кіберстрахування. Однак, як буде показано в наступному підрозділі, знайдена франшиза x_1* по-різному оцінює договір кіберстрахування в залежності від того, чи усвідомлює страховик наявність вторинних збитків G та розподіл приватних та публічних порушень γ.

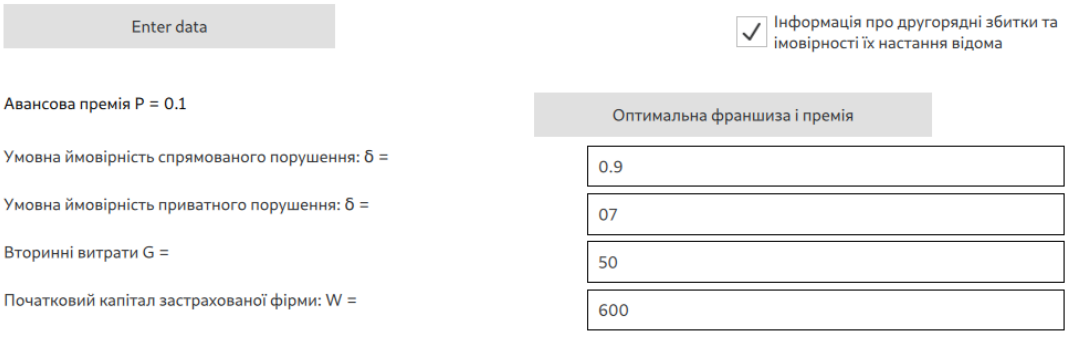

Рисунок 3.3 - Ілюстрація інтерфейсу для розрахунку оптимальної франшизи та остаточної премії

Рисунок 3.3 зображує частину інтерфейсу програмного засобу для введення необхідних даних для розрахунку значення Оптимальної франшизи x_1* за формулою (3) та за його допомогою знаходження фінального значення франшизи P_i за формулою (6). Потрапити у це меню можна лише за умови поставленої галочки у чек-боксі, що підтверджує інформованість страховика. При введенні даних не слід забувати про необхідні обмеження (звичайно у випадку використання справжньою фірмою реальні значення не будуть виходити за ці межі) для коректної роботи програми:

W > Max{ (G + a + P(a)), (G + b), (P(0) + Max{G, a})} та звичайно усі імовірнісні характеристики такі як q, δ, γ, λ повинні лежати у межах [0,1].

Як вже зазначалося у перших розділах цієї роботи напевно найважливішу роль у ціноутворенні кіберстрахування грає обізнаність страховика, саме тому весь ринок зараз прагне все більш персоналізованого підходу до розробки кожного нового поліса. Будемо називати страховика неінформованим, коли він не знає ні вторинних збитків G , ні розподілу порушень γ. Інформований страховик відповідно усвідомлює G і γ. Можливі випадки частково інформованого страховика (який знає лише один із факторів, G або γ) на ринку, але це не має особливого наслідку. Знаючи лише G, страховик не змінює структуру премій (другорядні збитки не враховуються за контрактом), а з іншого боку, знаючи γ, страховик не може помітити зміни у стратегії висування позовів. Як наслідок, рішення щодо ціноутворення необізнаними та частково інформованими страховиками залишаються однаковими. Для того, щоб оцінити відхилену претензійну стратегію компанії, що страхується , страховику обов'язково потрібно знати як G, так і γ. Класифікувавши страховиків, тепер подивимося на їх модель ціноутворення за договором кіберстрахування для франшизи x_1:

Неінформований страховик пропонує договір про премію

$$\mathrm{Pu} = \mathrm{q}(1+\lambda)\int_{x1}^{\infty}(x-x_1)dF(x) \qquad (5)$$

В той час як інформований страховик пропонує контракт на премію

$$P_i = q\delta(1+\lambda)(\gamma\int_{x_1-G}^{\infty}(x-x_1)f(x)dx + (1-\gamma)\int_{x_1}^{\infty}(x-x_1)f(x)dx) + q(1-\delta)(1+\lambda)\int_{x_1}^{\infty}(x-x_1)f(x)dx \quad (6)$$

Для будь-якої даної франшизи інформований страховик пропонує договір страхування кібер-послуг, який ніколи не перевищує ціну, запропоновану неінформованим страховиком, тобто Pu ≥ Pi .

Очікувана корисність застрахованої фірми залежить від структури премії (5) або (6), використаної в (4). Внаслідок цього, оптимальна франшиза x_1* залежність від типу страховика (яка повинна бути передана страховику).

3.3 Функції корисності та кіберзбитків

У розділі 3 ми стверджували, що вторинні збитки (G) від здійсненого порушення та розподіл приватних та публічних порушень (γ) разом змінюють оптимальний обсяг франшизи, а також структуру ціноутворення. Тут ми маємо справу з порівняльною ефективністю страхового інструменту, оскільки G і γ розкриваються договірним сторонам. Для полегшення порівняння ми запроваджуємо конкретні функціональні форми для функції корисності та функції кіберзбитків страхової фірми. Використовується стандартна логарифмічна функція U (.) = Ln(.) корисності страхової фірми. Логарифмічна функція корисності застрахованої фірми зберігає припущення увігнутості в нашій моделі, забезпечуючи тим самим запобігання ризику страхувальника. Для кібервтрати x, ми використовуємо рівномірну функцію розподілу втрат f(x)=1/(b - a), a ≥ x ≥ b. За відсутності емпірично встановленого росподілу кібер-втрат наше припущення про єдину функцію збитків становить загальний інтерес у тому сенсі, що будь-яке зловмисне порушення може бути однаково

вірогідним, і що залежно від цільового активу, понесені збитки можуть впасти у відомому діапазоні.

Відповідно до функцій логарифмічної корисності та рівномірного збитку, застрахована фірма тепер оптимально вибирає свій вирахуваний x_1* ($0 \le x_1 \le b$), що максимально забезпечує наступне: (7)

$$\max_{x_1}\left(\frac{q}{b-a}\begin{cases}\delta\gamma\left(\int_0^{\mathrm{Min}((x_1+G),b)}\mathrm{Ln}(W-x-P)\,dx+\mathrm{Ln}(W-x_1-P-G)\,(b-Min\big((x_1+G),b\big)\right)+\\ \delta(1-\gamma)\left(\int_0^{Min(x_1,b)}Ln\,(W-x-P-G)dx+Ln(W-x_1-P-G)\big(b-Min(x_1,b)\big)\right)+\\ (1-\delta)\left(\int_0^{Min(x_1,b)}Ln(W-x-P)dx+Ln(W-x_1-P)(b-Min(x_1,b))\right)\\ +(1-q)\ln(W-P)\end{cases}\right)$$

Зауважте, що обмеження, введене вище, - це мінімальний початковий капітал, необхідний для застрахованої фірми: це потрібно для збереження цілісності логарифмічної функції корисності нашої моделі.

Ми зручно обмежили межі пошуку оптимальної франшизи в (7). З огляду на нашу рівномірну функцію втрат, верхня межа простору пошуку для x_1 дорівнює b: поза цією точкою f(x) = 0, F(x) =1 скрізь, і ні структура очікуваної корисності E[U] застрахованої фірми (4), ні премія $P(x_1)$ тобто (5) або (6) не зазнає жодних змін. Іншими словами, $\forall b \le x_1$, E[U] є постійним. Діапазон пошуку включає в себе $a \le x_1 \le б$, оскільки місце розташування x_1 безпосередньо впливає на межі інтегрування в структурі премії, яка впливає на E[U]. Хоча межі інтеграції в структурі премій не впливають на $0 \le x_1 < a$; премія $P(x_1)$ дійсно змінюється в цьому діапазоні, оскільки інтеграл $(x\text{-}x_1)$ змінюється, що, в свою чергу, впливає на очікувану корисність E[U] застрахованої фірми. По суті, застрахована фірма могла оптимально вибрати свою франшизу у обмеженому діапазоні $0 \le x_1 \le b$, не приносячи шкоди ефективності рішення.

Зважаючи на те, що ризики безпеки IT є новими, і наше розуміння цієї галузі все ще формується, у першому розділі вже зазначалося, що учасники ринку кіберстрахування можуть стикатися з деякими труднощами

у питаннях визнання та оцінювання вторинних втрат G та імовірності випадків приватного та публічного порушення, γ. Відповідно, визначаємо наступні 2 різних концепції оцінки кіберстрахового ринку:

1. Він знаходиться у «інформаційній асиметрії», коли застрахована фірма розрізняє вторинні збитки від здійсненого порушення та формує позов до відповідного порушення. А страховик не знає G і γ, а тому використовує формулу (5) для підрахунку ціни контракту. Хоча поведінка застрахованої фірми зараз змінюється, ні поведінка, ні причини не є очевидними для страховика (неінформований страховик).

2. Ринок кіберстрахування знаходиться в «інформаційній симетрії», коли обидві сторони кіберстрахового контракту усвідомлюють характеристики, що впливають на вторинні збитки (G і γ) .Страхова компанія може спостерігати за змінами у поведінці застрахованої компанії так інформований страховик може коригувати свою поведінку і користатися формулою (6) для формування остаточного контракту.

Але на практиці реалізується суміш із цих двох положень. Ринок кіберстрахування може починатись із сценарію "наївної симетрії ", коли ні страховик, ні застрахована фірма ще не усвідомили особливість характеристик (G і γ) ризиків безпеки ІТ. З часом застрахована фірма виводить для себе ці показники, і модифікує свою поведінку на позови та угоди. І тоді ринок швидко робить перехід до "інформаційної асиметрії". Нарешті, коли страховик дізнається про зміни формування претензій, а також основні причини, стратегія ціноутворення (премій) змінюється. І ринок переходить до «інформаційної симетрії».

ВИСНОВКИ

Сучасний ІТ-бізнес вимагає сучасних рішень у питанні страхування від потенційних загроз. Кібератаки на ключову інфраструктуру, а також перспектива кібертероризму і навіть кібервійни становлять загрозу для суспільства. Кіберризик стає все більшою проблемою як для громадськості, так і для приватного бізнесу. За останні 30 років сфера кіберстрахування бурхливо розвивалась поєднуючи у собі новітні технології та традиційні математичні моделі.

У роботі були висвітлені основні етапи роботи страхової компанії, методи, види загроз, сучасний стан кібер-страхових компаній, теоретична складова конкретної моделі та програмна реалізація.

З академічної сторони дослідження має більш практичний характер, тому що є практична реалізація у вигляді програмного розрахункового пакету, адже сама модель не є новою у сфері страхування. З точки зору звичайного користувача ця робота досить гарно розкриває всі аспекти сучасного кіберстрахування, що призводить до більшої обізнаності читачів у цих питаннях, та привертання уваги до існуючих проблем, а це важливо насамперед через те, що це дуже перспективний напрямок діяльності, який рухає науково-технічний прогрес.

За приклад взятий стандартний договір страхування (Борч (1960) і Равів (1979) за обставини ринку кіберстрахування, що зароджується, де застраховані фірми передбачають вторинні збитки під час вимагання відшкодування реалізованих кібервтрат.

За допомогою аналізу пояснюється, як цей вторинний ризик збитків:

1. може вплинути на поведінку застрахованої фірми,
2. спричинити інформаційну асиметрію між страховиком та застрахованими фірмами,
3. може перешкодити розвитку цього ринку, що зароджується, за сукупним сценарієм.

Страхові продукти, ймовірно, будуть залишатися дещо дорогими в найближчому майбутньому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

Breuer, Michael, “Optimal Insurance Contracts without the Non-Negativity Constraints on Indemnities Revisited”, University of Zurich Working Paper No. 0406, April 2004.

Cavusoglu, H., Mishra, B., and Raghunathan S., “The Effect of Security Breach Announcement on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers”, UT Dallas Working Paper, 2004.

Doherty, N and Schlesinger, H., “Optimal Insurance in Incomplete markets”, Journal of Political Economy, 91: 1045-1054, 1983

Borch, K., “Economics of Insurance”, North Holland publishing company, 1990
Ermoliev, Yuri M., and Flam, Sjur Didrik, “Finding Pareto Optimal Insurance Contracts”, International Institute for Applied Systems Analysis Interim Report IR-00-033, June 2000.

Gollier, Christian, “Optimal Insurance of Approximate Losses”, The Journal of Risk and Insurance, volume 63, No 3, 369-380, 1996.

Gollier, Christian, and Pratt, John W., “Risk Vulnerability and the Tempering Effect of Background Risk”, Econometrica, Vol. 64, No. 5, 1109-1123, 1996.

USA Today, April 8, 2002, “FBI survey finds computer attacks up” (http://www.usatoday.com/tech/news/2002/04/08/fbi-survey.htm)

Institute for Catastrophic Loss Reduction, “Cyber-Incident Risk in Canada and the Role of Insurance”, Paper Series - No.38, ISBN: 0-9733795-4-5, April 2004.
Institute for Catastrophic Loss Reduction, “Cyber-Incident Risk in Canada and the Role of Insurance”, Paper Series - No.38, ISBN: 0-9733795-4-5, April 2004.

Tridib Bandyopadhyay • Vijay S Mookerjee • Ram C Rao: A Model to Analyze the Unfulfilled Promise of Cyber Insurance: The Impact of Secondary Loss.

Лістинг програми

```
#include <QGuiApplication>
#include <QQmlApplicationEngine>

int main(int argc, char *argv[])
{
    QCoreApplication::setAttribute(Qt::AA_EnableHighDpiScaling);

    QGuiApplication app(argc, argv);

    QQmlApplicationEngine engine;
    const QUrl url(QStringLiteral("qrc:/main.qml"));
    QObject::connect(&engine, &QQmlApplicationEngine::objectCreated,
                     &app, [url](QObject *obj, const QUrl &objUrl) {
        if (!obj && url == objUrl)
            QCoreApplication::exit(-1);
    }, Qt::QueuedConnection);
    engine.load(url);
```

```
    return app.exec();
}
import QtQuick 2.12

Item {
    id: root

    readonly property int modelSize: texts.length

    readonly property real spacing: height * 0.01 * (modelSize / 2)

    property var inputDatas: []

    property var texts: []

    Column {

        spacing: parent.spacing

        Repeater {
            model: root.modelSize
```

```
            delegate: InputField {
                width: root.width
                height: root.height * 0.13
                label: root.texts[model.index]
                onValueChanged: {
                    root.inputDatas[model.index] = value;
                }
            }
        }
    }
}
import QtQuick 2.12
import QtQuick.Controls 2.12

Row {
    id: root

    signal buttonClicked();

    readonly property alias isChecked: _checkBox.checked
```

```
    spacing: width * 0.08


    Button {
        anchors.left: root.left
        anchors.leftMargin: root.width * 0.1
        width: root.width * 0.25
        height: root.height * 0.5
        text: "Enter data"
        onClicked: {
            root.buttonClicked();
        }
    }


    CheckBox {
        id: _checkBox
        anchors.right: root.right
        anchors.rightMargin: root.width * 0.1
        text: "Інформація про другорядні збитки та\nімовірності їх настання відома"
    }
```

```
}

import QtQuick 2.12


Item {
    id: root


    readonly property int modelSize: texts.length


    readonly property real spacing: height * 0.01 * (modelSize / 2)


    property var inputDatas: []


    property var texts: []


    Column {


        spacing: parent.spacing


        Repeater {
            model: root.modelSize
```

```
            delegate: InputField {
                width: root.width
                height: root.height * 0.15
                label: root.texts[model.index]
                onValueChanged: {
                    root.inputDatas[model.index] = value;
                }
            }
        }
    }
}
import QtQuick 2.12
import QtQuick.Controls 2.12
import QtQuick.Controls.Styles 1.4

Item {

    property string label: ""

    property alias value: _txt.text
```

```
    Label {
        anchors.left: parent.left
        width: parent.width * 0.5
        height: parent.height
        text: parent.label
    }

    TextField {
        id: _txt
        anchors.right: parent.right
        width: parent.width * 0.45
        height: parent.height
        background: Rectangle {
            anchors.fill: _txt
            border {
                color: "black"
                width: 1
            }
        }
    }
}
```

```
import QtQuick 2.12
import QtQuick.Window 2.12
import QtQuick.Controls 2.12

Window {
    visible: true
    width: 1200
    height: 800
    title: qsTr("Тарифний калькулятор киберстрахування")

    Label {
        id: _label
        anchors.top: parent.top
        anchors.topMargin: parent.height * 0.05
        anchors.horizontalCenter: parent.horizontalCenter
        text: "Розрахунок премии"
        font.pointSize: 18
    }

    DataInputField {
        id: _inputField
```

```
    anchors.top: _label.bottom
    anchors.topMargin: parent.height * 0.025
    anchors.horizontalCenter: parent.horizontalCenter
    width: parent.width * 0.8
    height: parent.height * 0.4
    texts: ["Ймовірність порушення безпеки IT: q = ",
            "Оцінка максимально можливого збитку: b = ",
            "Оцінка мінімального можливого збитку: a =",
            "Початкове значення франшизи: x1 = ",
            "Коєфіцієнту завантаження ринку: λ = "]
}

ButtonField {
    id: _buttonField
    anchors.top: _inputField.bottom
    anchors.left: parent.left
    anchors.right: parent.right
    width: parent.width * 0.8
    height: parent.height * 0.1
    onButtonClicked: {
        _resultFiled.visible = !_resultFiled.visible;
```

```
            for (var i = 0; i < _input.inputDatas.length; ++i) {
                console.log(_input.inputDatas[i]);
            }
        }
    }

    ResultField {
        id: _resultFiled
        anchors.top: _buttonField.bottom
        anchors.bottomMargin: parent.height * 0.05
        width: parent.width
        height: parent.height * 0.4
        result: 0.1
        isAdditionalMode: _buttonField.isChecked
    }
}
import QtQuick 2.12
import QtQuick.Controls 2.12

Item {
    id: root
```

```
property bool isAdditionalMode: false

property real result: 0

Row {
    id: _row
    width: parent.width
    height: parent.height * 0.05

    spacing: width * 0.1

    Text {
        anchors.left: _row.left
        anchors.leftMargin: _row.width * 0.1
        text: "Авансова премія P = " + root.result.toString()
    }

    Button {
        id: _additionalButton
        anchors.right: _row.right
```

```
        anchors.rightMargin: _row.width * 0.2
        width: parent.width * (root.isAdditionalMode ? 0.3 : 0.1)
        text: root.isAdditionalMode ? "Оптимальна франшиза і премія" : "Quit"
        onClicked: {
            if (!root.isAdditionalMode) {
                Qt.quit();
            }
        }
    }

}

AdditionalResultField {
    anchors.top: _row.bottom
    anchors.topMargin: parent.height * 0.1
    anchors.left: parent.left
    anchors.leftMargin: parent.width * 0.1
    width: parent.width * 0.8
    height: parent.height * 0.9
    visible: root.isAdditionalMode
    texts: ["Умовна ймовірність спрямованого порушення: δ = ",
```

```
            "Умовна ймовірність приватного порушення: δ = ",
            "Вторинні витрати G = ",
            "Початковий капітал застрахованої фірми: W = "]
    }
}
```