Шифр: «Cyber страхування»

НАУКОВА РОБОТА

на тему:

«Страхування кіберризиків підприємств в умовах інтернету речей»

ЗМІСТ

ВСТУП…… 3
РОЗДІЛ І. ТЕОРЕТИЧНІ ОСНОВИ СТРАХУВАННЯ КІБЕР-РИЗИКІВ ЯК УМОВИ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ГРОМАДЯН, БІЗНЕСУ ТА ДЕРЖАВИ…….…….. 5
1.1. Трансформація страхових ризиків в умовах інтернету речей (IoT)…… 5
1.2. Класифікація кібер-ризиків……. 8
РОЗДІЛ 2. ОСОБЛИВОСТІ СТРАХУВАННЯ КІБЕР-РИЗИКІВ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ……. 10
2.1. Наукові підходи до визначення кібер-страхування…….. 10
2.2. Мета, завдання та принципи страхування кібер-ризиків……. 12
РОЗДІЛ 3. НАПРЯМИ АКТИВІЗАЦІЇ РОЛІ СТРАХОВИХ КОМПАНІЙ У ЗАХИСТІ ВІД РИЗИКІВ В УМОВАХ РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ …….... 17
3.1. Алгоритмізація процедур побудови страхового захисту від кібер-ризиків... 17
3.2. Прийняття рішення про доцільність страхування кібер-ризиків підприємством……. 20
ВИСНОВКИ…… 24
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 26
ДОДАТКИ

ВСТУП

Актуальність теми дослідження. Розвиток сучасної економіки, заснованої на використанні новітніх цифрових технологій, створення нових матеріалів, аналізі великих масивів даних, розробці нових систем управління, призводить до зміни принципів конкурентних відносин.

Однак, незважаючи на безумовні переваги цифровізації економіки – поява Dig Data, штучного інтелекту, технології блокчейну, хмарних обчислень з'являються і новітні ризики, генеровані їх використанням, що можуть негативно впливати на економічних суб'єктів та результати їхньої діяльності.

Вагомий внесок у дослідження різних аспектів страхування кібер-ризиків здійснили такі учені, як В.П. Братюк, Е.Д. Семенова, С. Волосович, Ю. Кожедуб, Н.В. Приказюк та інші. Однак, зважаючи на недостатню страхову активність потенційних потерпілих від наслідків кібер-ризиків (споживачів страхових послуг), розгляд сучасного стану та детермінант розвитку страхування кібер-ризиків є актуальним напрямом наукових досліджень.

Мета й завдання дослідження. Метою роботи є виявлення напрямів активізації ролі страхових компаній у забезпеченні страхових інтересів громадян, бізнесу та держави від наслідків кібер-ризиків.

Завдання дослідження відповідно до поставленої мети:

– дослідити трансформацію страхових ризиків в умовах інтернету речей (IoT);

– розглянути класифікацію кібер-ризиків;

– виявити наукові підходи до визначення кібер-страхування;

– розкрити мету, завдання та принципи страхування кібер-ризиків;

– представити алгоритм процедур побудови страхового захисту від кібер-ризиків підприємства;

– сформувати рекомендації щодо прийняття рішення про доцільність страхування кібер-ризиків підприємством.

Об'єктом дослідження є процеси організації страхового захисту від кібер-ризиків.

Предметом дослідження є теоретичні, методичні та практичні аспекти участі

страхових компаній в розробці та реалізації програми страхового захисту підприємств від кібер-ризиків.

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

Наукова новизна отриманих результатів. Основні положення, які формують наукову новизну дослідження, полягають у тому, що *набуло подальшого розвитку:*

– уточнення змісту «кібер-ризик» як ризику, поява якого зумовлена діяльністю на електронному ринку та використанням ІТ-технологій, ідентифікація його специфіки;

– методичний підхід до прийняття рішення про доцільність страхування кібер-ризиків, що ґрунтується на функції корисності для страхувальника і страховика.

Інформаційними джерелами дослідження слугували монографічна література та періодичні видання, дані статистичних Інтернет-сайтів, присвячених кібер-ризикам та кібер-страхуванню, прогнози та експертні оцінки провідних фінансових аналітиків та експертів,

Практичне значення отриманих результатів полягає в тому, що активізація діяльності страхових компаній в сегменті кібер-страхування сприятиме підвищенню інформаційної безпеки та створення умов стабільного функціонування в умовах впливу кібер-ризиків.

Апробація результатів дослідження. Результати наукової роботи впроваджено у діяльність ПрАТ «Страхова компанія «ВУСО» при розробці інструкції з продажу страхових послуг для страхових агентів.

Загальна характеристика наукової роботи. Наукова робота включає вступ, 3 розділи, висновки та пропозиції, список використаних джерел та додатки. Повний обсяг наукової роботи – 30 сторінок, 4 таблиці та 6 рисунків. При написанні наукової роботи було використано 48 наукових джерел.

Ключові слова: кібер-ризик, кібер-загроза, страхування кібер-ризиків, система управління ризиками на основі кібер-страхування, функція корисності.

РОЗДІЛ І
ТЕОРЕТИЧНІ ОСНОВИ СТРАХУВАННЯ КІБЕР-РИЗИКІВ ЯК УМОВИ БЕЗПЕЧНОГО ФУНКЦІОНУВАННЯ ГРОМАДЯН, БІЗНЕСУ ТА ДЕРЖАВИ

1.1. Трансформація страхових ризиків в умовах інтернету речей (IoT)

Світова економічна система знаходиться на постіндустріальній (інформаційній) стадії розвитку. Визначальною характеристикою цифрової економіки є модернізація факторів виробництва, основним із яких стають дані у цифровому форматі. Опрацювання значних обсягів даних та використання результатів їх аналізу дозволяють значно підвищити ефективність різноманітних виробництв, технологій та обладнання, зберігання, продажу і постачання товарів й послуг [7].

Сучасні тренди інтернет-середовища – це рух від об'єднання комп'ютерів і людей до об'єднання (розумних) об'єктів/речей. Дана концепція отримала назву Інтернет речей (Internet of Thing – IoT) і стала невід'ємною частиною IT-інфраструктури та економіки в цілому. Вона пов'язана зі збільшенням кількості і типів пристроїв, підключених до мережі, оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем і розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси , що виключає з частини дій і операцій необхідність участі людини. Інтернетом речей можна назвати об'єднану мережу унікально ідентифікованих кінцевих точок (або «речей»), які можуть спілкуватися без участі людини, використовуючи IP-з'єднання. Екосистема, що підтримує Інтернет речей включає в себе складне поєднання технологій, що не обмежуються тільки модулями/пристроями, пов'язаністю, платформами Інтернету речей, зберіганням, серверами, безпекою, аналітичним програмним забезпеченням та IT-послугами [31, 16, 17].

«Розумні» пристрої та нові послуги можуть бути причиною непередбачених наслідків і вразливостей, що зумовлює появу специфічних ризиків – кібер-ризиків. Розширення підключених до мереж машин і обладнання може привести до появи

надскладних ризиків, таких як крадіжка даних, збої комунікації і навіть відмова цілих виробничих ліній та ланцюгів поставок.

За визначенням В.В. Вітлінського, ризик – це економічна категорія, яка відображає особливості сприйняття заінтересованими суб'єктами економічних відносин об'єктивно існуючих невизначеності та конфліктності, які притаманні процесам цілепокладання, управління, прийняття рішень, оцінювання, що обтяжені можливими загрозами щодо понесення збитків, втрат іміджу та невикористаними можливостями [10]. Дане визначення ризику покладено в основу ідентифікації конкретних видів ризиків в Індустрії 4.0, представленої у роботі [48]:

1) ризики постачання;

2) ризики процесу;

3) ризики управління;

4) ризики попиту;

5) ризики зовнішнього середовища.

Їх зміст деталізовано у роботі [9].

Так, за даними звіту по глобальним ризикам 2015 р Міжнародного економічного форуму (World Economic Forum), віртуальні (кібер) ризики названі одними з найголовніших комерційних ризиків. Підтверджують цей висновок і дослідження підприємницьких ризиків, які представляють небезпеку для ведення бізнесу, проведене компанією Global Corporate & Specialty. Експерти визначили десять найбільш важливих факторів ризику як в світі в цілому, так і в розрізі окремих регіонів. Дані ранжирування факторів ризику, в якому 1 означає найбільш небезпечний ризик, а 10 – найменш небезпечний, представлені в таблиці А.1 (Додаток А).

Згідно представлених даних – кібер-ризики названі одними із найнебезпечніших ризиків для провадження бізнесу, сумарні втрати світової економіки від їх реалізації становили у 2015 році близько 445 мільярдів доларів [35, с. 10], а вже у 2017 році – 600 мільярдів доларів [45]. За даними Страхового брокера «ІНСАРТ» – 25 млн. дол. США – понесений збиток українським бізнесом в результаті кібер-атак, близько 50% вітчизняних компаній мали справу з кібер-

атаками; більш ніж 125000 комп'ютерів було заражене внаслідок кібер-атаки вірусу Petya.A, а розмір збитків склав 466,3 млн. доларів США [45]

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

У сучасній економічній літературі представлено достатню кількість різнопланових підходів до визначення суті поняття кібер-ризику (рис. 1.1).

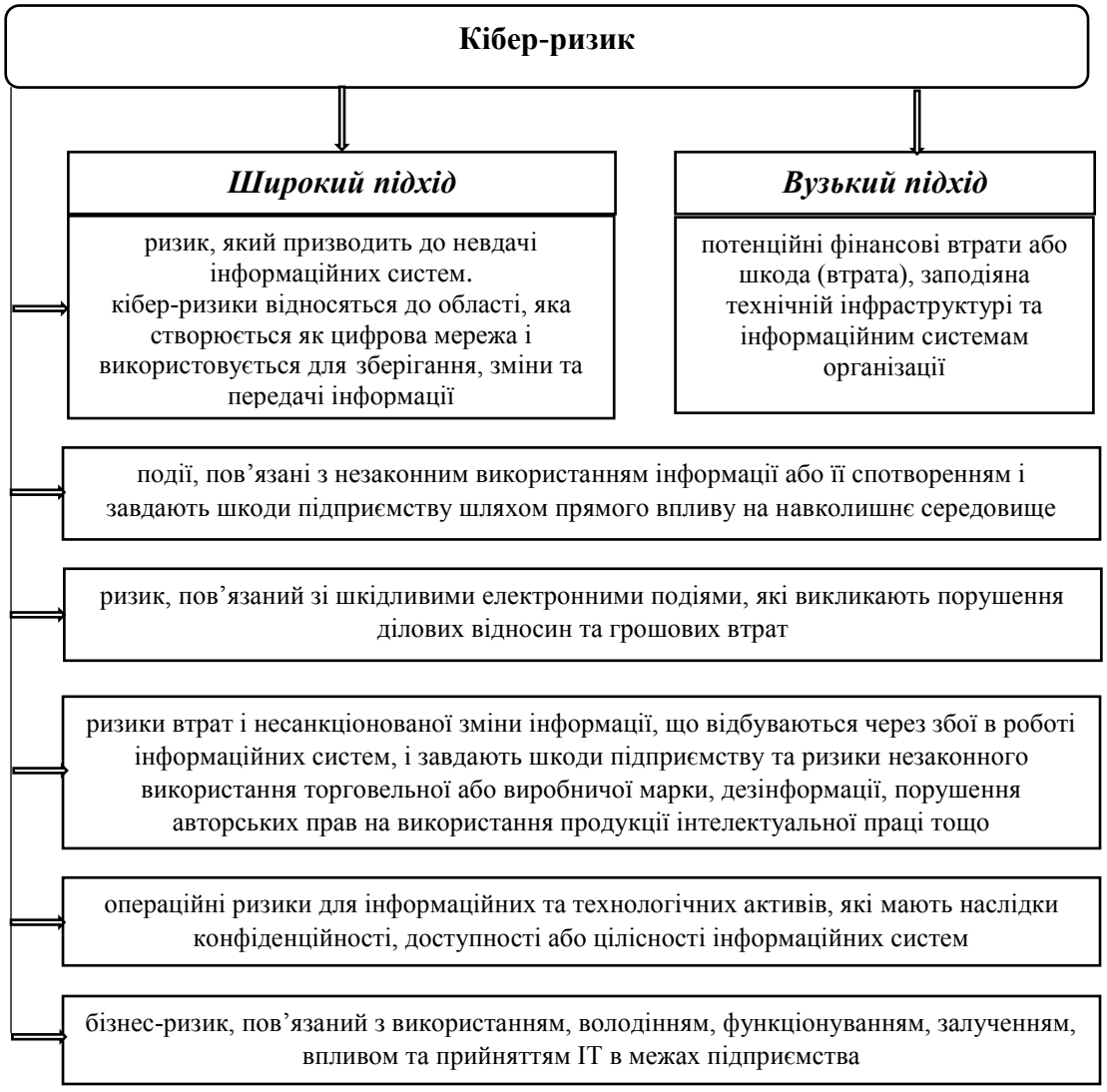

Рис. 1.1. Підходи вчених до визначення суті поняття «кібер-ризик»

Джерело: складено автором за [38, 39, 43, 42, 44, 47, 36]

Однак, наведені підходи не враховують сукупність специфічних особливостей, які розкривають зміст кібер-ризиків [12, 13, 14, 21, 41]:

по перше, об'єктом зазіхань (потенційної втрати) є дані (інформація)

(нематеріальні активи), що несанкціоновано видаляються, спотворюються, порушується їх конфіденційність або унеможливлюється доступ до них (неавторизоване розкриття, зміна або руйнування цифрових активів);

по друге, підмножина сукупних ризиків, які відносяться одночасно до ризиків IT та інформаційної безпеки;

по третє, це ризики реалізації навмисних злочинних дій за допомогою використання IT.

Врахування таких особливостей дозволило трактувати кібер-ризик як специфічний ризик, поява якого зумовлена діяльністю на електронному ринку та використанням IT-технологій.

Кібер-ризики викликані спеціальними видами загроз інформаційної безпеки, що представлені на рисунку А.1 (Додаток А).

1.2. Класифікація кібер-ризиків

У роботі [8] авторами представлено класифікацію кібер-ризиків та здійснено їх групування за такими ознаками: 1) втрата або крадіжка носіїв інформації та мобільних пристроїв; 2) доступ сторонніх осіб до конфіденційної інформації за допомогою вразливих хмарних сховищ; 3) ненавмисне розголошення співробітниками конфіденційної інформації; 4) навмисні дії співробітників (інсайдерів); 5) неконтрольоване копіювання даних співробітниками. Такий підхід дозволив виокремити наступні види кібер-ризиків:

– ризик втрати інформації під час злому паролю доступу або внаслідок DDoS-атаки;

– ризик фінансових втрат від фішінгових атак;

– ризик фінансових втрат через порушення роботи комп’ютерних систем;

– ризик фінансових втрат від кібер-шантажу або вірусного блокування комп’ютерних систем;

– ризик фінансових втрат через викрадення та розголошення персональних даних та інформації.

Кібер-ризики реалізують внаслідок настання таких подій:

1. Нецільові атаки (фішинг, кардинг, sms-шахрайство);

2. Цільові атаки (фінансове шахрайство, розкрадання баз даних, промислове шпигунство, DDoS атаки, вимагання);

3. Атаки зсередини (розкрадання, знищення інформації, сприяння цільовій атаці).

Результати настання кібер-ризиків можуть розглядатися з позиції видів завданих збитків (фінансовий і майновий) та суб'єктів наслідків їх реалізації (1-ша особа, 3-тя особа), наведені на рисунку 1.2.

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

Рис. 1.2. Класифікація наслідків кібер-ризиків

Узагальнюючи наведене вище, наслідки та прояви збитків внаслідок реалізації кібер-ризиків для суб'єктів підприємницької діяльності представлено у таблиці 1.1.

Таблиця 1.1

Наслідки для підприємств від настання кібер-ризиків

Вплив	Збиток
Припинення або уповільнення бізнес-процесів	Втрата клієнтів та прибутку
Втрата конкурентної переваги	
Збиток для бренду та втрата репутації	Зниження вартості бізнесу
Судові розгляди та позови	Витрати на усунення наслідків, штрафи і санкції регулюючих органів

Джерело: розроблено авторами на основі [8].

Отже, у світлі зростання кількості та серйозності кібер-злочинів ризик-менеджмент організацій змушений внести до свого списку ще одну небезпеку – хакерські атаки. З даними ризиками необхідно працювати і шукати шляхи їх оптимізації. Для таких цілей існує три основних напрямки: технологічні рішення безпеки, просвітницька робота в сфері протидії та профілактики кібер-злочинів, а також кібер-страхування.

РОЗДІЛ 2
ОСОБЛИВОСТІ СТРАХУВАННЯ КІБЕР-РИЗИКІВ В УМОВАХ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ

2.1. Наукові підходи до визначення кібер-страхування

Подією, що сприятиме зростанню, в першу чергу, європейського ринку кіберстрахування вважаємо набуття з 25 травня 2018 року чинності регламентного документа Європейського Союзу щодо захисту даних (General Data Protection Regulation, GDPR) внаслідок підвищення обізнаності компаній про ризики, викликаних порушеннями конфіденційності при обробці даних.

Нові правила надають громадянам ЄС більше прав на свою онлайн-інформацію і передбачають штрафні санкції, розмір яких досягає 4% річного доходу компанії при виявленні серйозних порушень.

На думку страхових експертів, цей директивний документ, а також наслідки таких великих кібератак, таких як WannaCry і NotPetya, будуть стимулювати попит на кіберстрахування у Європі. Так, кількість синдикатів Lloyd's, що пропонують кіберстрахування, тільки за 2016 рік збільшилася на 20%. На думку виконавчого директора Lloyd Інги Біль, щорічні прирости брутто-премії європейського кіберстрахування до 2020 року можуть скласти понад $ 2 млрд, що сумарно становитиме близько $ 9 млрд.

Експерти відмічають, що крупні клієнти при прийнятті рішення про співпрацю однією з умов виставляють – наявність поліса страхування кібер-ризиків у своїх партнерів. Про перспективи даного виду страхування говорить і те, що найбільші страхові компанії світу вже мають подібні послуги в своєму портфоліо.

Світовий досвід свідчить, що розвиток страхового ринку сприяє росту національної економіки в цілому, а кібер-страхування – суб'єктів підприємницької діяльності, забезпечуючи їх стабільне функціонування і свободу у прийнятті рішень при здійсненні інвестиційної та інноваційної діяльності в умовах цифровізації економіки. Для конкурентної боротьби підприємствам необхідно впроваджувати нові перспективні технології з метою реалізації послуг нового покоління.

Відбувається цифрова трансформація бізнесу, що тягне за собою появу нових ризиків.

Страховики пропонують послуги зі страхування ризиків, що спричиняють втрати економічних суб'єктів, зумовлені використанням ними обчислювальної техніки та мереж, так зване кібер-страхування.

Приходить і розуміння того, що набагато легше витратити частину коштів на страхування, ніж втратити не лише гроші, але й ділову репутацію. Інформаційні активи компаній дорожчають, відповідно і ймовірність втрат також стрімко зростає. Аналітики роблять прогнози про майбутнє значне зростання попиту на послуги даного виду страхування, зіставні з сьогоднішнім страхуванням майна.

Р. Беме та Г. Шварцем запропоноване наступне визначення кібер-страхування – це передача фінансового ризику, пов'язаного з мережевими та комп'ютерними інцидентами, третій стороні [37]. У таблиці 2.1 згруповано критерії віднесення кібер-ризиків до страхових та види кібер-ризиків, що можуть бути застрахованими.

Таблиця 2.1

Умови прийняття кібер-ризиків на страхування та їх види

Критерії, що дозволяють ідентифікувати кібер-ризик як страховий:	***Види кібер-ризиків, які частково або повністю можуть бути застраховані:***
– випадковість виникнення втрат (проблемна для оцінки); – максимально можлива втрата (не проблематична для оцінки); – середня втрата на подію (не є проблематичною для оцінки); – експозиція втрат (не проблематична для оцінки); – ліміти покриття (проблемні для оцінки); – страхова премія (менш проблематична для оцінки).	– ризик привласнення та використання конфіденційної інформації співробітниками компанії; – ризик отримання хакером інформації про номери кредитних карт або рахунків клієнтів компанії; – ризик розкрадання грошових коштів з рахунків в банку або цінних паперів з рахунку в депозитарії; – ризик розкрадання даних кредитних карт і засобів з них; – ризик втрати або розголошення інформації через помилки співробітника; – перерва в роботі підприємства, його комп'ютерної мережі, сайту; – збитки, пов'язані з розміщенням на сайті страхувальника неправдивої інформації або інформації, що має характер дифамації (приниження честі, гідності та ділової репутації); – ризик втрати матеріального носія, що містить конфіденційну інформацію

Джерело: складено за [36, 32].

Специфічність кібер-ризиків, що можуть бути застраховані проявляється у:

1. Відсутності у страхувальників і страховиків планів з реагування в подібних випадках.

2. Існуванні перспективи суброгації, оскільки більшість подій викликані умисними діями.

3. Доцільності залучення професійних консультантів на етапі укладення договору страхування та врегулювання збитку.

Кібер-страхування – це страховий продукт, що захищає компанію від ризиків, пов'язаних з використанням мережі Інтернет, а також із ризиками, що відносяться до інформаційних технологій, IT-інфраструктури та діяльності підприємства у кібер-просторі. Страховий захист від кібер-ризиків потребують компанії які:

– здійснюють діяльність, яка безпосередньо пов’язана з мережею Інтернет;

– використовують банківські картки, розрахункові системи, а також віддалені системи доступу;

– відправляють через Інтернет конфіденційні особисті дані;

– застосовують інтернет-сайт для залучення покупців або надання і поширення даних про свою діяльність [30].

Договір кібер-страхування покриває збитки страхувальника завдані кібер-атакою, та понесені у результаті перерв у виробництві, втрати і відновлення даних, реагування на інцидент, виплати викупної суми кріптолокерам, розслідування інциденту, а також кібер-злочину з метою фінансової вигоди (шахраї).

З метою підвищення привабливості страхової послуги, страховики додатково розширюють страхове покриття додаванням таких умов як:

– відшкодування витрат на розслідування кібер-злочинів;

– антикризовий піар з метою відновлення репутації;

– витрати на захист у суді і відновлення роботи IT-системи.

Таким чином, кібер-страхування надзвичайно вигідне при великомасштабному інциденті компрометації IT-системи, допомагаючи підприємствам зберігати фінансову стабільність, оперативно повернутися до нормального функціонування і зниження втрат.

2.2. Мета, завдання та принципи страхування кібер-ризиків

Звернення до кібер-страхування спрямоване на досягнення основної мети – забезпечення підприємства компенсаційним ресурсом достатнього за обсягом і за

прийнятну ціну, що досягається за рахунок виконання основних завдань, із дотриманням відповідних принципів (рис. 2.1).

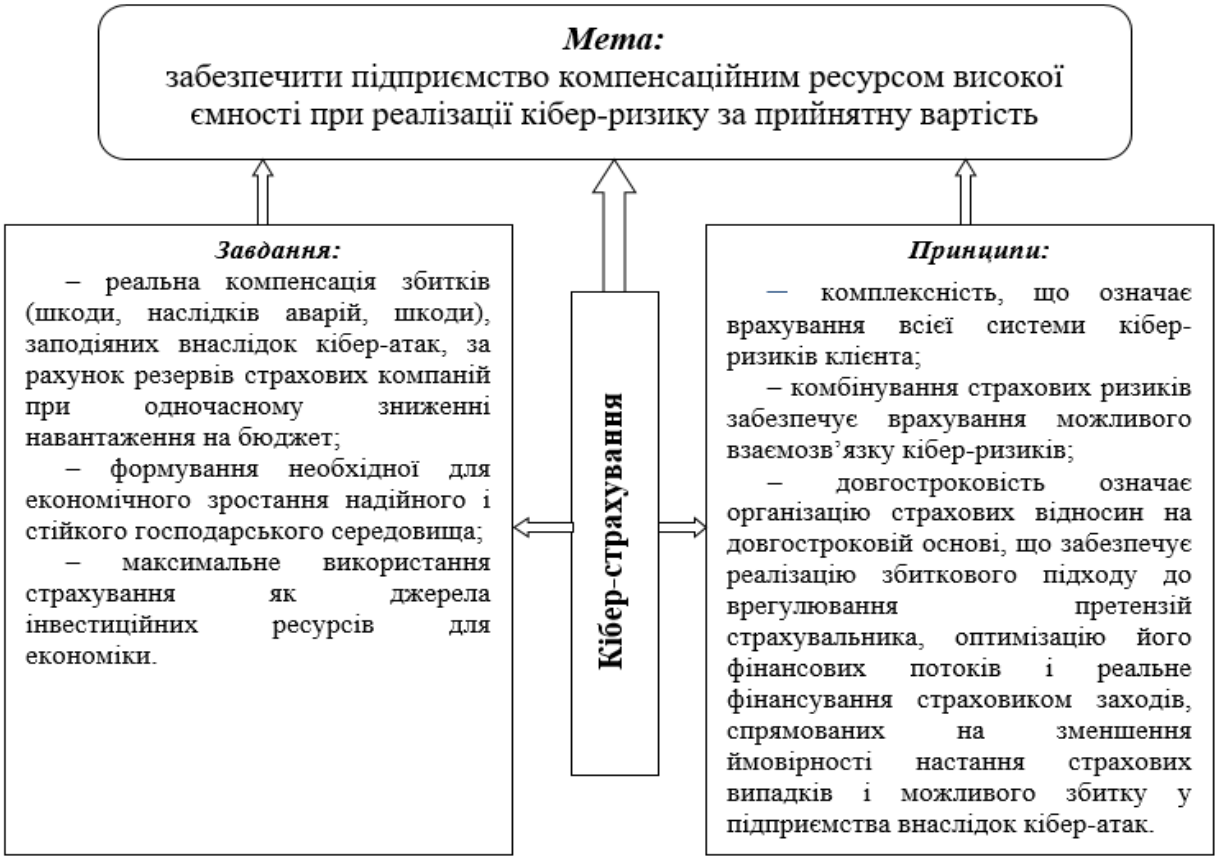

Рис. 2.1. Мета, завдання та принципи кібер-страхування

Джерело: складено за [24, с.61].

В. Братюк зазначає, що страхування кібер-ризиків спрямоване на подолання наслідків втручання кібер-злочинців (відновлення функцій, інформації, комунікацій) та пов'язане з покриттям всіх необхідних для цього витрат, а також на відшкодування збитків, які є результатом простою комп'ютерних систем [4].

Є.С. Сєдов виділив характерні особливості страхування кібер-ризиків (табл. Б.1).

Звичайно, у першу чергу, підприємство зацікавлене у збереженні своїх активів як виробничого, так і іншого призначення, а також у продовженні своєї діяльності навіть у випадку реалізації різного роду ризиків. Основні детермінанти кібер-страхування представлені у таблиці 2.2.

Як бачимо основним завданням кібер-страхування є захист від хакерських атак. Існують певні складнощі в доведенні наявності кібер-атаки. Клієнти матимуть велику спокусу звернутися за страховим відшкодуванням, навмисно, здійснивши

атаку всередині компанії. Страховикові буде вкрай тяжко довести факт шахрайства. Також існує небезпека того, що компанії просто не будуть витрачати кошти на поліпшення систем безпеки, маючи страховий поліс – чекатимуть на виплату страхового відшкодування.

Таблиця 2.2

Детермінанти кібер-страхування [20]

Опис ризику, що покривається страховиком	Прояв ризику	Страхувальники	Переваги для страхувальників	Ризики для страховиків
– ризики, що виникають при використанні електронних даних та їх передачі, включаючи технологічні інструменти, такі як інтернет та телекомунікаційні мережі; – фізичний збиток, який може бути спричинений випадками порушення кібербезпеки, шахрайством, заподіяним зловживанням даними, будь-якою відповідальністю, що виникає внаслідок зберігання даних; а також доступності, цілісності та конфіденційності електронної інформації щодо приватних осіб, компаній чи урядів [40]	Хакерські атаки	Підприємства реального сектору, банки, фінансові компанії, реєстратори цінних паперів, реєстратори прав власності та ін.	– експертиза найбільш суттєвих ризиків; – розробка рекомендацій щодо мінімізації наслідків атаки	– складність доведення кібератаки (можливе внутрішньофірмове шахрайство); – відсутність у страхувальника потреби здійснювати витрати на покращення системи безпеки

У таблиці Б.2 наведено кілька додаткових прикладів нових ризиків, що виникають при впровадженні інновацій та потребують підтримки страховика/перестраховика.

Врахування таких особливостей дозволило трактувати кібер-страхування як складову ризик-менеджменту підприємства, що представляє собою – фінансовий механізм відновлення після значних збитків, метою якого є допомога страхувальникам повернутися до нормального функціонування, зберегти стабільність, платоспроможність та знизити витрати, пов’язані з перервами у виробництві, викликаними дією кібер-ризиків.

З позиції страхувальників кібер-страхування – метод управління ризиками й захист від різноманітних загроз, що виникають при здійсненні електронної комерції.

Захист від кібер-ризиків може послідовно перетворюватися у важливу сферу бізнесу. Кібер-ризики становлять серйозну проблему для страхової галузі, оскільки вона володіє дуже обмеженими даними про довгострокові втрати від них, що унеможливлює проведення оцінки ризику з використанням звичайних моделей.

Крім того, самі ризики змінюються в міру того, як бізнес оцифровується, що вимагає гнучких рішень, які включають набагато більше, ніж просто страхове покриття.

Невідомі кібер-ризики можуть бути виявлені у багатьох існуючих традиційних страхових програмах для бізнесу, оскільки договірні умови або не виключають цих ризиків, або не формують виключень і обмежень з достатньою точністю.

У таблиці Б.3 (додаток Б), представлено характерні види кібер-ризиків і напрями кібер-страхування від кібер-злочинів.

На думку Н. Приказюк, основними проблемами, що стримують розвиток кіберстрахування є (рис 2.2):

Проблема	*Спосіб вирішення*
Невизначеність регулювання відносин у кіберстрахуванні	прийняття у державі законодавства, яке регулює відносини у сфері захисту особистих даних, регламентації вимог щодо способу зберігання, рівня захисту цих даних і визначення відповідних санкцій у разі їх порушення
Нестача інформації для проведення актуарних розрахунків	утворення Бюро даних щодо кібербезпеки. Держава може сприяти утворенню такого Бюро, що значно допомогло б страховим компаніям та ризик-менеджерам управляти ризиками, створювати актуарні моделі для кіберризиків, цим самим скоротивши вартість полісів страхування і зробивши кіберстрахування більш привабливим для компаній
Концентрація (кумуляція) ризиків у разі настання страхового випадку	Перестрахування кіберризиків для страхових компаній державою протягом певного часу.

Рис. 2.2. Проблеми, що стримують розвиток кібер-страхування та способи їх розв'язання

Джерело: складено за [26,25]

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

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

На сучасному етапі функціонування вітчизняного страхового ринку лише деякі страхові компанії можуть запропонувати якісний страховий захист від кіберзлочинності (кібер-ризиків). Відсутня необхідна статистика, законодавча база, судова практика. Недостатньо і кваліфікованих фахівців, що мають уявлення про даний вид ризику та його структуру [15].

Однак, на перспективу, вітчизняні страховики повинні стежити за світовими тенденціями, переймати західний досвід; збирати і аналізувати дані, статистику зарубіжних компаній і готувати платформу для створення власних продуктів із кібер-страхування. Варто звернути увагу на поліс CyberEdge від American International Group (AIG), адже на сьогоднішній день це вершина розвитку кіберстрахування.

Певний рух у цьому напрямі відбувається через страхових брокерів, які мають можливість виходу на світовий ринок кібер-страхування та розміщують ризики вітчизняних підприємств-страхувальників.

Крім того, причинами, що стримують розвиток кіберстрахування в Україні є: невизначенність юридичного статусу цифрових активів; не розробленість методичних підходів до класифікації ризиків використання цифрових активів, відсутність методик оцінки кібер-ризиків та систем ризик-менеджменту адаптованих до потреб цифрової економіки. У розпорядженні страховиків є традиційні страхові продукти (види страхування технічних ризиків), які можуть бути модернізовані під потреби цифрової економіки: страхування машин від поломок, страхування від перерв у виробництві, страхування ризику введення технологічних інновацій, страхування електронного обладнання, страхування ризику втрати прибутку внаслідок поломок промислових машин і технологічного обладнання, страхування післяпускових гарантійних зобов’язань тощо.

РОЗДІЛ 3
НАПРЯМИ АКТИВІЗАЦІЇ РОЛІ СТРАХОВИХ КОМПАНІЙ У ЗАХИСТІ ВІД РИЗИКІВ В УМОВАХ РОЗВИТКУ ІНТЕРНЕТУ РЕЧЕЙ

3.1. Алгоритмізація процедур побудови страхового захисту від кібер-ризиків

Більшість компаній витрачають більшу частину свого часу та ресурсів, створюючи захист в середині компанії, що включає дані, системи та персонал. Це є відправною точкою, але периметр вже не стабільний, а система внутрішнього захисту вже не є достатньо сильною, щоб утримати нападників [16]. Кібер-ризики можуть призводити до прямих та непрямих грошових втрат суб'єктів господарювання. В першому випадку можна легко виміряти збитки в грошовому еквіваленті. В другому – необхідно залучати експерта або фахівця для якісної оцінки величини збитків від наслідків кібер-ризиків в організації [8].

Процес ризик-менеджменту інформаційної безпеки складається з встановлення контексту, оцінки ризику, обробки ризику, прийняття ризику, комунікацій ризику, а також моніторингу та переоцінки ризику інформаційної безпеки.

В процесі менеджменту ризику інформаційної безпеки процедури оцінки ризику і (або) його обробки можуть виконуватися ітеративно, при цьому якщо вдається отримати достатню інформацію для ефективного визначення дій, необхідних для зниження ризику до прийнятного рівня, то завдання виконане, після чого слідує обробка ризику (рис. В.1).

Існують чотири варіанти обробки ризику:

– зниження ризику – рівень ризику повинен бути знижений шляхом вибору заходів та засоби контролю і управління так, щоб ризик який залишився міг бути повторно оцінений як допустимий;

– збереження ризику – рішення зберегти ризик, що не здійснюючи подальших дії, слід приймати в залежності від оцінки ризику;

– запобігання ризику – відмова від діяльності або умови, що викликає конкретний ризик;

– перенесення ризику – ризик повинен бути переданий на сторону, яка може найбільш ефективно здійснювати менеджмент конкретного ризику в залежності від оцінки ризику.

В результаті обробки повинні бути відібрані заходи і засоби контролю та управління для зниження, збереження, запобігання або перенесення ризиків.

У сучасній літературі основна увага приділяється організаційно-технічному забезпеченню інформаційної безпеки і, зокрема, апаратним і програмним засобам захисту інформації. Однак економічні методи забезпечення інформаційної безпеки не менш важливі, ніж технічні.

Мета системи управління ризиками підприємства на основі страхового захисту полягає у зниженні рівня ризиків супутніх діяльності компанії до прийнятного для акціонерів (власників) рівня шляхом передачі ризиків страховику і тим самим сприяння досягненню поставлених перед компанією цілей (рис. 3.1).

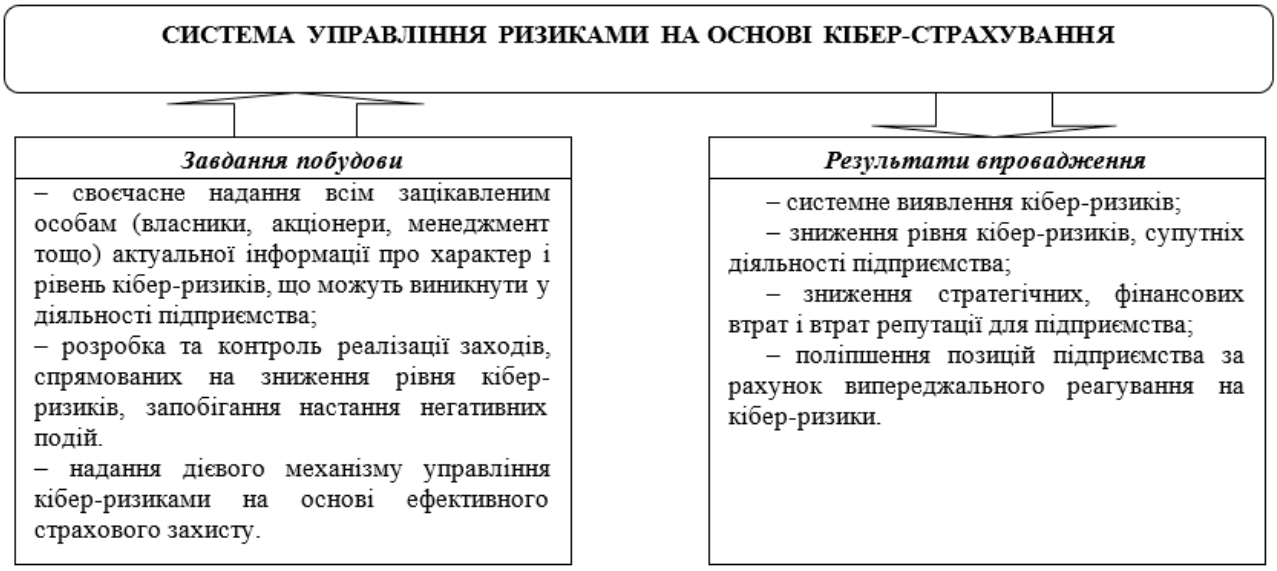

Рис. 3.1. Завдання побудови та результати впровадження системи управління ризиками на основі кібер-страхування

Управління кібер-ризиками на основі побудови страхового захисту підприємства організовується за результатами аналізу його діяльності з урахуванням факторів, що впливають на оцінку можливого збитку. Для ідентифікації ризиків суб'єкти господарювання складають карти ризиків. Структурно-функціональна

модель організації процесу оцінки кібер-ризиків підприємства представлена на рисунку В.2.

Інструментами і методами моніторингу і управління ризиками є перегляд і аудит ризиків, аналіз відхилень і трендів, технічні вимірювання виконання, аналіз резервів [19].

Звернення підприємства до страхової компанії за страховим захистом передбачає усестороннє вивчення страховиком (сюрвеєром, оцінювачем) особливостей та специфіки бізнесу клієнтів з метою формування програми попереджувальних заходів і розробки пакетів страхових продуктів в рамках наявних програм страхового захисту, які найбільш повно відповідають потребам того чи іншого підприємства з урахуванням ймовірності реалізації кібер-ризику виникнення збитків.

В рамках вирішення поставленого завдання побудовано матрицю взаємодії суб'єкт підприємницької діяльності – страхові продукти (табл. 3.1), яка ілюструє попит підприємства на управління конкретним кібер-ризиком підприємства і пропозицію страхової компанії страхової послуги, що відповідає певному ризику [23].

Таблиця 3.1

Матриця взаємодії

суб'єкт підприємницької діяльності – страховий продукт

Елементи виробничого процесу		НДР, ОКР і розробка проектів	Виробництво	Фінанси	Персонал	Логістика, збут
Галузі страхування	Страхові продукти					
Майнове страхування	Страхування від збитків внаслідок перерв у виробництві		+	+	+	
	Страхування будівельно-монтажних ризиків	+	+			
	Страхування інвестиційних проектів	+	+			+
	Страхування фінансових ризиків	+	+	+		+
	Страхування додаткових витрат	+	+	+		+
Страхування відповідальності	Страхування відповідальності підприємств – джерел підвищеної небезпеки		+	+	+	
	Страхування відповідальності за непогашення кредиту	+		+		+
	Страхування відповідальності за забруднення навколишнього середовища		+			+
	Страхування професійної відповідальності	+	+	+	+	

Взаємодія можлива лише за наявності попиту підприємства на управління визначеними ризиками та пропозиції страхової компанії.

3.2. Прийняття рішення про доцільність страхування кібер-ризиків підприємством

В рамках побудови системи страхового захисту підприємства можна сформулювати поняття ефективного кібер-страхування підприємства, під яким розуміється сукупність відносин з перерозподілу, подолання і відшкодування збитку, що характеризуються ефективними умовами страхування та раціональним набором кібер-ризиків, що покриваються страховиками.

Слід, розуміти, що страхування як метод управління ризиком не завжди є універсальним інструментом і його використання має свої межі. Такі обмеження можуть бути пов’язані як з типом ризику і взаємовідносинами учасниками операції страхування так і їх ставленням до ризику.

Відсутність чітких критеріїв прийняття рішень відносно вибору страхування як методу управління ризиком не дозволяє автоматично класифікувати ризики на ті, що підлягають страхуванню, і ті, що не можуть бути застрахованими. Успішність взаємодії страхової компанії та підприємства визначається можливістю і доцільністю взаємодії, а також економічною ефективністю страхового захисту.

Доцільність взаємодії суб’єкта підприємницької діяльності та страхової компанії визначається за результатами якісного і кількісного аналізу можливих збитків (таблиця 3.2). Кількісний аналіз ризику дозволяє провести оцінку доцільності використання системи страхових послуг, що включають покриття від кібер-ризиків.

Одним із широковідомих методів урахування чинників невизначеності є аналізу доречності витрат (аналізу збитків). Для вирішення вводяться до розгляду такі поняття, як області (зони) ризику: зона мінімального ризику, зона допустимого ризику, зона критичного ризику та зона катастрофічного ризику.

Таблиця 3.2

Кількісний і якісний аналіз можливих збитків підприємства

Тип збитку	Зони ризику	Ймовірність, %	Рішення
Незначний	Зона мінімального ризику	0 – 25	Не страхувати
Малий	Зона прийнятного ризику	25 – 50	Самострахування
Середній	Зона критичного ризику	50 – 75	Самострахування, страхування
Великий	Зона катастрофічного ризику	75 – 100	Страхування

Система страхових послуг знаходиться в системі координат зони критичного та катастрофічного ризиків. Адже ризики прийнятного та частково критичного ризику можуть повністю покриваються внутрішніми ресурсами і не потребують залучення зовнішніх страхових фондів.

Параметри функції корисності за умов ризику, власне функція корисності (U) Дж. Неймана і О.Моргенштерна, визначають корисність страхування варіанту *x* з ймовірністю *p(x)*. За своєю суттю премія за ризик (надбавка за ризик) – це сума, яку особа, що приймає рішення, згодна сплатити, за те, щоб уникнути ризику.

Так, зростаюча функція корисності для суб'єкта управління, байдужого до ризику має вигляд: U(x)= a + bx, зростаюча функція корисності для суб'єкта управління, несхильного до ризику, має вигляд: U(x)=log(x +b), де x >– b, а для суб'єкта управління, схильного до ризику справедлива зростаюча функція корисності, яка задана наступною формулою: U(x) = x2, де x >=0.

Область значень функції складає величину L – очікувані втрати. Таким чином, у суб'єкта господарювання несхильного до ризику величина L буде максимальна, а у ризикованого – мінімальна. Графічно функцію ризику суб'єкта, несхильного до ризику зображено на рисунку В.1 (Додаток В).

Порівняльна оцінка економічної ефективності вибору варіанта страхування чи самострахування здійснюється за допомогою методу, який в західній літературі отримав назву метод Хаустона. Суть методу Хаустона полягає в оцінці впливу різних способів управління ризиком на «вартість організації» (*value of organization*). Вартість організації можна визначити через вартість її вільних активів. Вільні (чисті) активи організації – це різниця між вартістю всіх її активів та зобов'язаннями.

При страхуванні підприємство сплачує на початку фінансового періоду страхові премії та гарантує собі компенсацію збитків в майбутньому.

Розглянемо умови, за яких страхувальникові доцільно укладати договір кібер-страхування, а в якому випадку варто вдатися до самострахування (відмовитися від укладення договору страхування із страховою компанією), тобто йдеться про вартість фінансування ризику, під яким розуміють пошук та мобілізацію грошових ресурсів для здійснення превентивних заходів і запобігання збиткам за настання несприятливих подій.

У роботі [3] запропоновано рекомендації до моделювання страхового контракту. Зробимо припущення, що учасники кібер-страхування (страхувальник і страховик) мають різне ставлення до ризику: несхильність і ризик-нейтральність відповідно. тоді цільова функція страхувальника полягає в максимізації його очікуваної користі від укладення страхового контракту:

$$Ef = (1-p)U(H-r) + pU(H-r+h-Q) \rightarrow \max, \qquad (3.1)$$

де p – ймовірність настання DDoS-атаки;

U() – функція корисності страхувальника;

H – величина капіталу страхувальника;

r – величина страхового внеску, що дорівнює добутку суми нетто-ставки і комерційної надбавки ξ_0 на величину страхового відшкодування $r = (p + \xi_0)\, h$;

h – величина страхового відшкодування;

Q – величина збитків від наслідків DdoS-атаки.

Основні «технічні» проблеми аналізу механізмів страхування виникають через нелінійності функції корисності страхувальника. У той же час саме ця нелінійність, відображає несхильність до ризику, робить страхування можливим і взаємовигідним для страхувальника і страховика.

Тому для спрощення моделі розглянемо можливі способи обліку несхильність до ризику, не використовуючи в явному вигляді функцію корисності.

Для цього введемо в його цільову функцію ризикову премію, яка відображатиме цінність страхового відшкодування, одержуваного при настанні страхового випадку, як описано в роботі В.М. Буркова і ін. [6].

Тоді очікувана корисність страхувальника від укладення договору страхування (3.1) з урахуванням сказаного вище може бути виражена як де Δh (h) – «цінність» страхового відшкодування.

Наприклад, між іншим $\Delta h(h) = he^{\xi}$. Використовуючи розкладання експоненти в ряд Маклорена отримуємо, що для досить малих ξ де $\xi \geq 0$ – константа, яка відображає несхильність страхувальника до ризику (нейтральності до ризику відповідає значення $\xi = 0$).

Очікуване значення цільової функції страховика має наступний вигляд:

$$E\Phi = r - ph \rightarrow \max$$

Таким чином, умова участі (individual rationality) для страхувальника має вигляд:

$$r \leq p(1+\xi)h, \tag{3.2}$$

а для страховика:

$$r > ph, \tag{3.3}$$

Умова «морального ризику», що відображає неспонукання страхувальника до зацікавленості у страховому випадку:

$$(1+\xi)h \leq Q, \tag{3.4}$$

Вигідність страхування для страховика оцінюється величиною ЕФ, так як за відсутності договору страхування його корисність дорівнює нулю.

Вигідність страхування для страхувальника може бути оцінена різницею ΔEf між його корисністю в разі укладення страхового договору і в разі його відсутності: $\Delta Ef = p(1+\xi)h - r$.

Сума $\Delta = \Delta Ef + E\Phi$ може розглядатися, як «Міра» взаємовигідності страхового контракту, тоді цільова функції прийме наступний вигляд:

$$\Delta = \xi ph \rightarrow \max \tag{3.5}$$

Завдання пошуку значень параметрів r і h, максимізує очікувану міру взаємовигідності з урахуванням (3.2) – (3.5) зводиться до задачі лінійного програмування, в результаті вирішення якої отриману страхову премію можна трактувати як ануїтет ренти, що виплачується за часовий період.

Основні бізнес-процеси з організації страхового захисту підприємства наведені на рисунку В.2.

Крім того, страхові компанії з позиції суб’єктів господарювання можна розглядати як ризик-консультантів, оскільки останні розробляють галузеві страхові програми та пропонують комплексні страхові поліси, які передбачають захист від кібер-небезпек, що були виявлені при оцінці ризиків діяльності суб’єкта. Страховики вивчають галузеву специфіку діяльності підприємства і формують набір найбільш вірогідних кібер-ризиків та пропонують оптимальне страхове покриття, тобто допомагають підприємствам ідентифікувати ризики і розробити програму захисту від них.

ВИСНОВКИ

Ключові висновки дослідження можна представити такими тезами:

Кібер-ризик – специфічний ризик, поява якого зумовлена діяльністю на електронному ринку та використанням ІТ-технологій. Особливості кібер-ризиків: об’єктом потенційної втрати є дані (інформація) (нематеріальні активи), що несанкціоновано видаляються, спотворюються, порушується їх конфіденційність або унеможливлюється доступ до них (неавторизоване розкриття, зміна або руйнування цифрових активів); підмножина сукупних ризиків, які відносяться одночасно до ризиків ІТ та інформаційної безпеки; ризики реалізації навмисних злочинних дій за допомогою використання ІТ.

Наразі відсутнє усталене трактування поняття «кібер-страхування», проведене дослідження наукових напрацювань українських та зарубіжних вчених дало змогу трактувати його як складову ризик-менеджменту підприємства, що представляє собою фінансовий механізм відновлення після значних збитків, метою якого є допомога страхувальникам повернутися до нормального функціонування, зберегти стабільність, платоспроможність та знизити витрати, пов’язані з перервами у виробництві, викликаними дією кібер-ризиків.

На даний момент складається ситуація, при якій вітчизняні страхові компанії поки не можуть розробити власний підхід до оцінки кібер-ризиків, що стримує зростання популярності цієї послуги в Україні. Вітчизняні страхові компанії, готуючи пропозицію для клієнта, оцінюють ризики компанії за допомогою непрямих ознак і характеристик, таких як: методи управління ризиком в компанії; способи зберігання даних; проведення чи тестування систем інформаційної безпеки та аудиту, а також оцінюють кількість співробітників зайнятих в ІТ. Слід очікувати, що найближчим часом почнуть формуватися більш детальні методики, які все-таки будуть відповідати на пряме запитання щодо оцінки ризиків кібер-страхування.

Запропоновано теоретичне узагальнення науково-методичних підходів і обґрунтуванно практичні рекомендації щодо розробки моделі оцінювання корисності кібер-страхування для суб’єкта підприємницької діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бозен Р., Позднякова Н. Европа объявила войну киберпреступности // Deutsche Welle,1.06.2012 // www.dw.com.

2. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности.– 2013.– №1. – С. 2–9.

3. Борхаленко В.А. Механизмы страхования в управлкнии рисками информационной безопастности // В.А. Борхаленко / Экономический анализ: теория и практика, 2017, т. 16, вып. 2, стр. 379–388 http://www.fin-izdat.ru/journal/analiz/

4. Братюк В.П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні / В.П. Братюк // Актуальні проблеми економіки. – 2015. – № 9. – С. 421-427. – [Електронний ресурс] – Режим доступу: http://nbuv.gov.ua/UJRN/ape_2015_9_54.

5. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.– 288 с.

6. Бурков В.Н., Заложнев А.Ю., Кулик О.С., Новиков Д.А. Механизмы страхования в социально-экономических системах. М.: ИПУ РАН, 2001. 109 с.

7. Введение в «Цифровую» экономику// А.В. Кешелава В.Г. Буданов,В.Ю. Румянцев и др.; под общ. ред. А.В. Кешелава; гл. «цифр.» конс. И.А.Зимненко. – ВНИИГеосистем, 2017. – 28 с. (На пороге «цифрового будущего».Книга первая).

8. Віннікова І.І., Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними // І.І. Віннікова, С.В. Марчук // Східна Європа: економіка, бізнес та управління. – Випуск 5 (16) 2018.

9. Вітлінський В. В. Ризики в індустрії 4.0 / В. В. Вітлінський, В. І. Скіцько // Вісник Черкаського університету. Серія : Економічні науки. - 2016. - № 3. - С. 17-26. - Режим доступу: http://nbuv.gov.ua/UJRN/VchuE_2016_3_5

10. Вітлінський В.В., Ризикологія в економіці та підприємництві : Монографія. / В. В. Вітлінський., Г. І. Великоіваненко – К. : КНЕУ. – 2004. – 480 с.

11. Волосович С. Детермінанти виникнення та реалізації кібер-ризиків / С. Волосович, Л. Клапків // Зовнішня торгівля: економіка, фінанси, право. – 2018. № 3. С. 101–115.

12. Воронова Т. Безопасный интернет / Т. Воронова. – Calaméo: [Електронний ресурс].– Режим доступу: http://ru.calameo.com/books/002793881c6046eb0d2fb

13. Завгородний В.И. Парадигма информационных рисков / В.И. Завгородний. - Финансовый Университет при Правительстве РФ: [Електронний ресурс].– Режим доступу: http://www.fa-kit.ru/main_dsp.php?top_id=591

14. Зайцева О.Н. О необходимости введения понятия «риски адекватности информации» // Фундаментальные исследования. - 2013. - № 1–3. - С. 807–811.

15. Иващенко А.Н., Шарко И.А. Мировой рынок страхования кибер-рисков: перспективы и препятствия для развития в Республике Беларусь // Материалы IX Международной научно-практической конференции студентов «Национальная экономика Республики Беларусь: проблемы и перспективы развития». Минск: БГЭУ, 2016. С. 196–202.

16. Интернет Вещей: инновационные и перспективные технологии – IoT Russia 2015. – [Электронный ресурс] – Режим доступа: http://www.tmtconferences.ru/iot2015.html

17. Карачев О. Интернет вещей: что это такое и с чем его едят? – [Электронный ресурс] – Режим доступа: http://chezasite.com/news/chto-takoe-internet-veshei-82180.html

18. Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки. Information Technology and Security. 2017. Vol. 5. No 1. С. 82–95.

19. Кропотина О.Е. Страхование как метод управления рисками промышленных предприятий / О.Е. Кропотина // Экономика и управление народным хозяйством. – 2009. – №11 /12. – С. 12–14.

20. Курбанова О.Э., Ларионов В.И. Киберстрахование как способ обеспечения информационной безопасности // Материалы Всероссийской заочной научно-практической конференции: Проблемы развития страхового бизнеса в Росии. Под общ. ред. Е.А. Нестеренко. 2017. – С. 55-58.

21. Мишель М. Управление информационными рисками / М. Мишель // Финансовый директор. - 2003. - № 9. - С. 64–68.

22. Мних М. В. Страхування в Україні: сучасна теорія і практика: [монографія] / М. В. Мних – К.: Знання України, 2006. – 284 с.

23. Натальин А. А. Развитие корпоративного страхования в условиях рынка: диссертация. кандидата экономических наук: 08.00.10. / А.А. Натальин – Саранск, 2006. – 172 с.

24. Пономарёв А. Н. Разработка модели процесса корпоративного страхования. Имущественное корпоративное страхование / А. Н. Пономарёв // Вестник ВГУ. Серия: Экономика и управление. – 2009. – №2. – С.61-68.

25. Приказюк Н. В. Необхідність та можливість впровадження нових страхових продуктів у страховій системі (на прикладі кіберстрахування). Економіка і фінанси. 2016. № 12. С. 109–117.

26. Приказюк Н.В. Прогресивний досвід зарубіжних країн у вирішенні проблем розвитку кіберстрахування / Н.В. Приказюк, М.В. Кукурудзяк // Вісник Одеського національного університету. Серія: «Економіка». – 2016. – Том 21. Вип. 2. – С. 164-168.

27. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування: Аналітична записка / Національний інститут стратегічних досліджень // www.niss.gov.ua.

28. Семенова Е.Д. Становление нового цифрового мира и проблемы менеджмента кибер-рисков [Текст] / Е.Д. Семенова, К.И. Тарасова // Маркетинг і менеджмент інновацій. 2017. № 3. С. 236–244. – [Електронний ресурс] – Режим доступу: http://10.21272/ mmi.2017.3-22.

29. Сєдов Є. С. Деякі аспекти страхування кібер-ризиків / Є. С. Сєдов // Інноваційні напрямки розвитку страхового ринку України : зб. матеріалів III Міжнар. наук.-практ. конф. (19–20 квіт. 2016 р., м. Київ) / М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана» ; [редкол.: О. О. Гаманкова (голова) та ін.]. – Київ : КТ «Забєліна-Фільковська Т. С. і компанія Київська нотна фабрика», 2016. – С. 288–291.

30. Страхование кибер-рисков [Электронный ресурс]. – Режим доступа: https://www.arsenalins.ru

31. Тинькова А.А., Замотайкина А.А. Особенности и преимущества платформы Watson IoT для Интернета вещей // Nauka-rastudent.ru. – 2017. – No. 03 (039) / [Электронный ресурс] – Режим доступа. – URL: http://nauka-rastudent.ru/39/4148/

32. Цена информационной безопасности и страховая защита откибер – рисков. [Электронный ресурс]. Режим доступа: http://strahovkunado.ru/insur/strakhovan.

33. Якушев В. Кібербезпека-2018: чого чекати бізнесу? – [Електронний ресурс] – Режим доступу: https://mind.ua/openmind/20180414-kiberbezpeka-2018-chogo-chekati-biznesu. Global Economic Forum, The Global Risks Report 2017. 12thEdition. URL: http://wef.ch/risks2017

34. 5 ways to make global e-commerce easier for everyone. December, 2017. URL: https://www.weforum.org/ agenda/2017/12/ecommerce-trade-wto-growth-opportunity

35. Allianz Risk Barometer Top Business Risks 2016 [Electronic resource]. – 2016. – № 5 – Access mode: http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf

36. Biener C., Eling M., Wirfs J.H. (2015) Insurability of cyber risk: an empirical analysis. Working papers on risk management and insurance, 151. Available at: http://www.ivw.unisg.ch/~/ media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf [Accessed 15/04/16].

37. Böhme R., Schwartz G. (2010) Modeling cyber-insurance: towards a unifying framework. WEIS. Available at: http://econinfosec.org/archive/weis2010/papers/session5/weis2010_ boehme.pdf [Accessed 12/04/16].

38. Calderon C., Marta E. (2007) A taxonomy of software security requirements. Avances en Sistemas e Informatica, 4 (3), pp. 47-56.

39. Cebula J., Young L. (2010) A taxonomy of operational cyber security risks. Software Engineering Institute, Carnegie Mellon University. Available at: http://resources.sei.cmu.edu/ library/asset-view.cfm?AssetID=9395 [Accessed 12/04/16].

40. CRO Forum. The Cyber Risk Challenge and the Role of Insurance. December 2014. URL : http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance.

41. Data scarce for insurers covering cyber risks. Business Insurance. [Електронний ресурс].– Режим доступу: http://www.businessinsurance.com/article/20150610/NEWS06/150619981/1251

42. Donnelly C., Englund M., Nielsen J.P., Tangaard C. (2014) Asymmetric information, self-selection and pricing of insurance contracts: the simple no-claims case. Journal of risk and insurance, 81 (4), pp. 757-780.

43. Firesmith D. (2004) Specifying reusable security requirements. Journal of object technology, 3 (1), pp. 61-75.

44. Gerasimenko V.A. (1994) Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh [Data protection in data processing systems]. Moscow: Energoatomizdat Publ.

45. 2018.iforum.ua/ru/speakers/alexandra-gladyshevskaya/

46. Marotta A. A Survey on Cyber-Insurance / Marotta A., Martinelli F., Nanni S., Yautsiukhin A. – Bologna, Italy: Unipol Gruppo Finanziario S.p.A., 2015. – 52 p.

47. Ol'ga A. Mirsanova The Bonus-Malus System as the policyholders' classification method in cyber-insurance / Economics: Yesterday, Today and Tomorrow. 6`2016

48. Schröder M. Industry 4.0 And Its Impact On Supply Chain Risk Management [Електронний ресурс] / M. Schröder, M. Indorf, W. Kersten // 14th International Conference «Reliability and Statistics in Transportation and Communication (RelStat)». – Riga, 15-18 October 2014. – Режим доступу: http://www.tsi.lv/sites/default/files/editor/science/Conferences/RelStat14/schroeder_indorf_kersten.pdf

ДОДАТКИ

Додаток А

Таблиця А.1

Головні ризики ведення бізнесу в 2016 році

(побудовано згідно з Allianz Global Corporate & Specialty [35])

Фактори ризику	Ранг					
	Світ у цілому	Європа	Азія	Африка і Середній схід	Північна і Південна Америки	Австралія
Переривання бізнесу (включаючи порушення в ланцюзі постачань товарів)	1	1	1	5	1	2
Розвиток ринку (волатильність, конкуренція, стагнація ринку)	2	2	2	1	4	1
Кібер-інцидент (кібер-злочинність, витік даних, помилки IT-систем)	3	3	5	5	2	4
Природні катастрофи	4	6	3	3	3	5
Зміни в законодавстві та регулюванні (економічні санкції, протекціонізм)	5	4	7	3	5	7
Макроекономічні події (програми жорсткої економії, підвищення цін на сировинні товари, інфляція / дефляція)	6	5	4	1	8	3
Втрата репутації або вартості бренду	7	7	6	–	6	5
Пожежі, вибухи	8	8	8	8	6	8
Політичні ризики (в т.ч. війна, тероризм)	9	10	10	7	–	–
Крадіжка, шахрайство	10	–	–	9	9	–

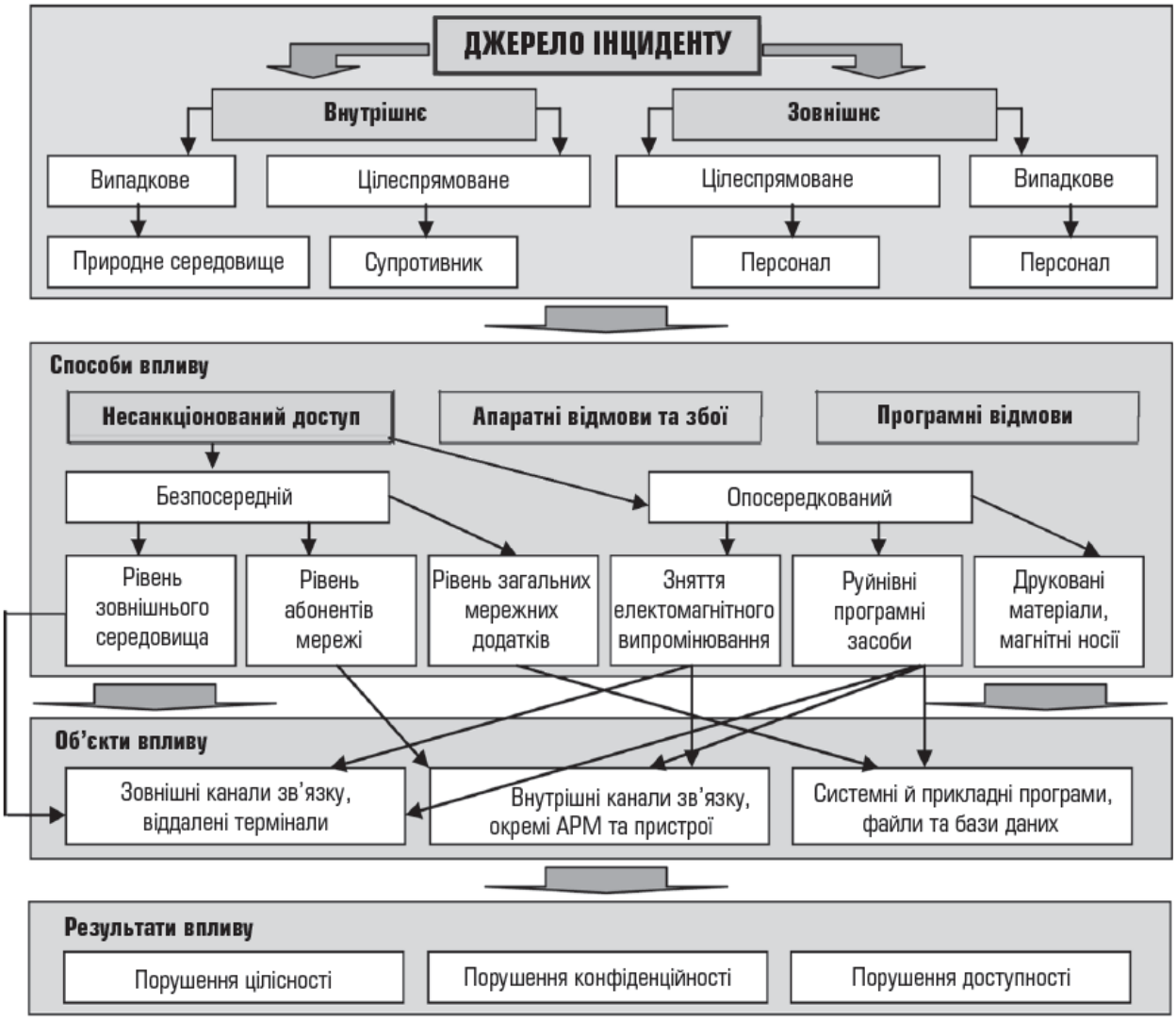

Рис. А.1. Класифікація джерел інцидентів, а також способів, об'єктів та результатів їхнього впливу[5, с. 28]

Таблиця А.2

Топ-10 кібер-ризиків у 2017 році

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

Джерело: розроблено авторами на основі [8, 33]

Додаток Б

Таблиця Б.1

Особливості страхування кібер-ризиків

Риса (особливість)	*Характеристика*
Брак досвіду страховиків і відповідних стандартів	Кібер-страхування – це новий вид страхування, і страховики ще не мають чіткої стандартизованої процедури
Еволюціонування інформаційних систем	Комп'ютерні системи швидко еволюціонують, з'являються нові технології, які можуть змінити природу кібер-ризиків
Інформаційна асиметрія	Страховик не завжди має доступ до тієї ж самої інформації, що і страхувальник. Найчастіше ця інформація є засекреченою
Еволюція кібер-атак	Техніки і прийоми, які використовують кібер-злочинці, постійно змінюються, і ці зміни є непередбачуваними
Взаємозалежність безпеки	Рівень захисту однієї системи часто залежить від захисту інших: вірус може проникнути в систему через канал, створений з компанією-партнером
Нестача статистичних даних	Відсутність статистичних даних про інциденти не дає змоги страховикам визначити надійність їхніх полісів, так як ця інформація часто є конфіденційною і не підлягає розголошенню.
Складність оцінити збитки	Це пов'язано з природою інформаційних активів (вартість ноу-хау чи вартість репутації)
Проблеми з визначенням покриття	Важко визначити, від чого саме страхувальник хоче застрахуватися, а страховик у свою чергу не може точно визначити, чи готовий він це покрити
Винятки та обмеження	Поліси зі страхування кібер-ризиків містять безліч винятків та обмежень щодо покриття
Відповідальність	Коли була здійснена кібер-атака, необхідно встановити рівень відповідальності за збитки і визначити, хто несе відповідальність за шкоду. У деяких випадках це можуть бути власники систем, в інших – розробники програмного забезпечення тощо
Час для пред'явлення претензій	Багато атак відбуваються непоміченими. Порушення у роботі системи можуть бути виявлені вже після нападу. Крім того, деякі атаки є надзвичайно тривалими (наприклад, напади можуть зайняти кілька місяців). Питання про те, яким чином страховики повинні відшкодувати витрати, залишається відкритим

Джерело: [29, 46]

Таблиця Б.2

Приклади нових ризиків, що виникають при впровадженні інновацій та потребують страхового/перестрахового захисту

Тип страхування	Опис покривається ризику
Відповідальність за спільне використання підрядників	Страхування для малого бізнесу (наприклад, підрядників, таких як персональні тренери, фотографи), яке охоплює виключення або обмеження
Покриття для будинку спільного використання	Страхове покриття для спільного проживання в будинках на короткий термін; Страхування майна на основі блокчейна
Покриття для спільного використання автомобілів	Страхове покриття для програм автопарку і спільного використання автомобілів

Кібербезпека у комплекті зі страхуванням	Підтримка гарантії захисту даних від програмного забезпечення; виявлення крадіжки особистих даних; захист і шахрайство в поєднанні зі страхуванням
Страхування на вимогу для короткострокового використання	Страхування безпілотників на вимогу для розважальних і комерційних рейсів; страхування короткострокової оренди для ринку важкої техніки
Відповідальність за використання нових технологій	Індивідуальне страхування для нової технології (наприклад, гарантії інфраструктури IoT, гарантія продуктивності Clean Tech, відповідальність за роботів, відповідальність за 3D-друк, обмін криптовалюти).

Таблиця Б.3

Характерні види кібер-ризиків і напрями кібер-страхування

Види кібер-ризиків	Напрями кібер-страхування ризиків
Ризик втрати інформації та порушення роботи систем при зламі пароля доступу або внаслідок DDoS-атаки	За сутністю відноситься до кібер-ризику втрати інформації та порушення роботи комп'ютерних систем. Кібер-страхування відшкодує витрати на поновлення діяльності інформаційної технології, наприклад, web-сайту.
Ризик фінансових втрат через порушення роботи комп'ютерних систем	За сутністю відповідає ризику втрати впущеної вигоди в offline-страхуванні. Напрям страхування захищає IT-підприємства від втрат з вини кібер-злочинців у разі порушення роботи комп'ютерних систем. Напрям страхування є доцільним для захисту online-магазинів, медіа-кінотеатрів, систем трекер-торентів.
Ризик фінансових втрат за регрес-позовами при викраденні, розголошенні або використанні персональної інформації	Сутність полягає в ризику втрат від регрес-позовів власників даних при викраденні, розголошенні та використанні кібер-злочинцями їх персональної інформації. Цей напрям страхування відшкодовує збитки підприємств за регрес-позовами власників персональної інформації.
Ризик фінансових втрат за здирництвом при вірусному блокуванні комп'ютерних систем	Сутність полягає в кібер-вимаганні (здирництві) через примушення до сплати (наприклад, шляхом SMS) за розблокування інформаційних систем або інформації при попередньому блокуванні вірусом програм комп'ютерів або баз даних. Кібер-страхування покриває витрати на розблокування інформаційних систем при доведенні витрат та фіксації кібер-злочину для страхувальника.
Ризик фінансових втрат на відновлення програм-ного забезпечення та (або) інформації вгаслі-док дії кібер-злочинців	За сутністю є аналогом майнового страхування та відноситься до кібер-ризику фінансових втрат при пошкодженні програмного забезпечення та (або) інформації внаслідок дії кібер-злочинців. Кібер-страхування відшкодовує витрати на відновлення програмного забезпечення та (або) інформації.

Джерело [1, 2, 27]

Додаток В

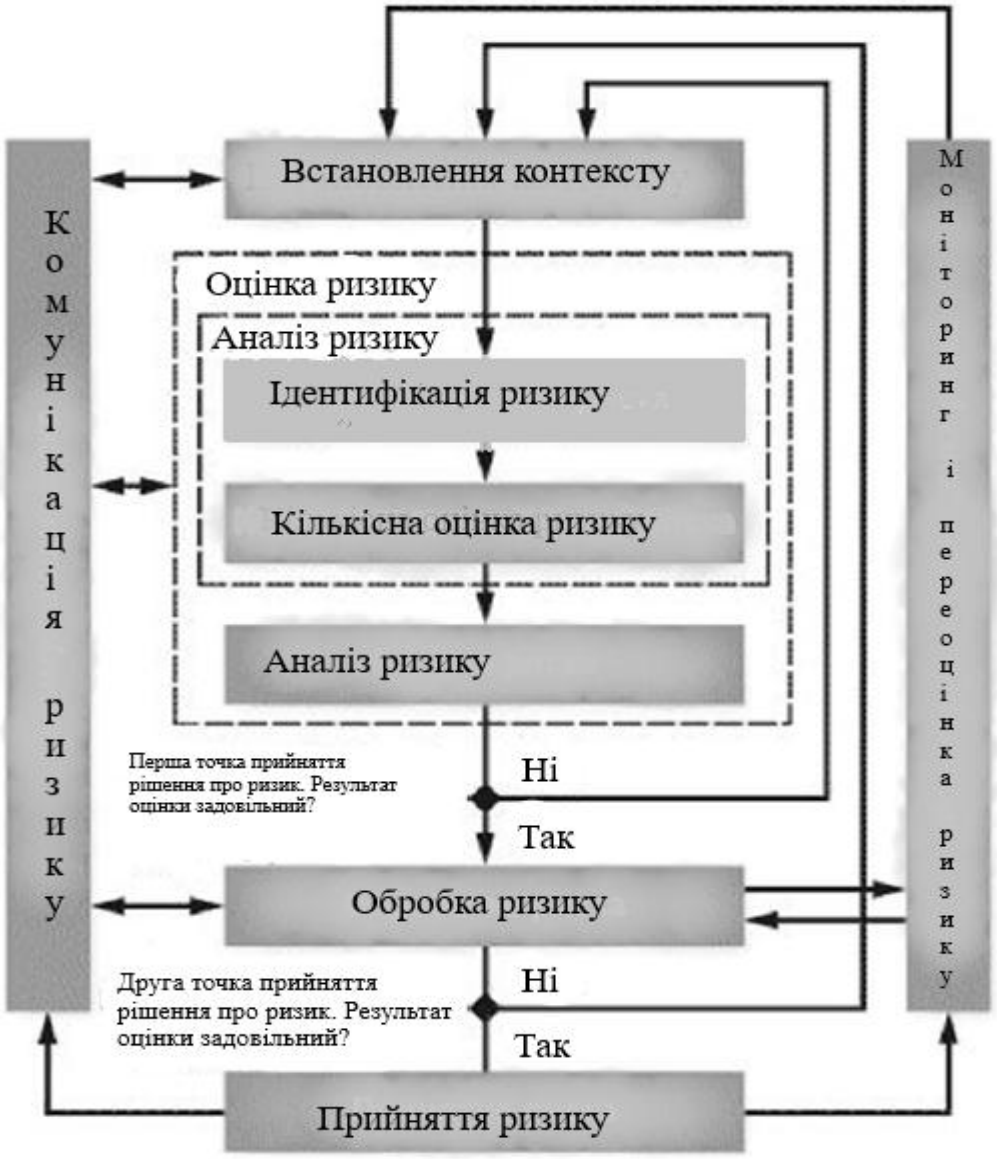

Рис. В.1. Процес менеджменту ризику інформаційної безпеки

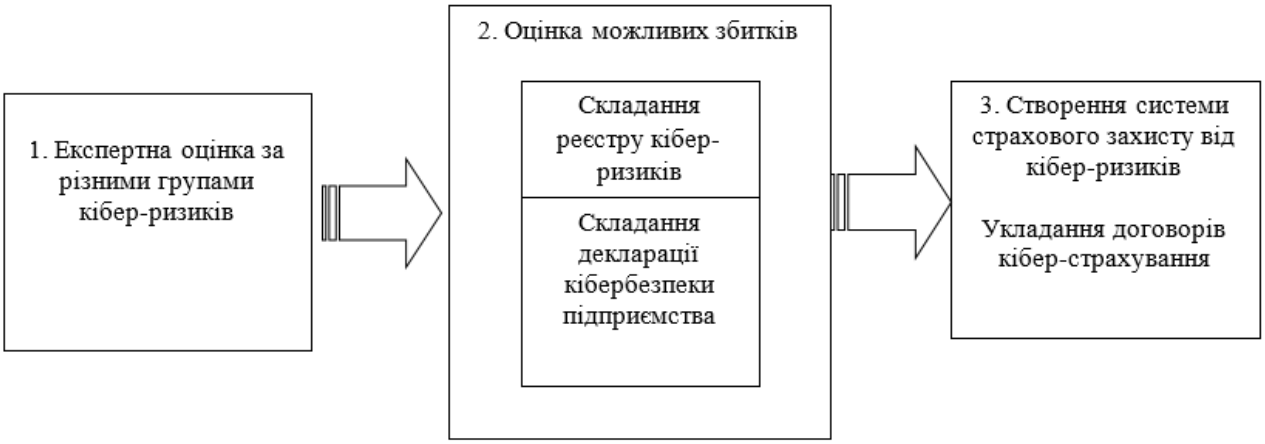

Рис. В.2. Структурно-функціональна модель оцінки кібер-ризиків підприємства

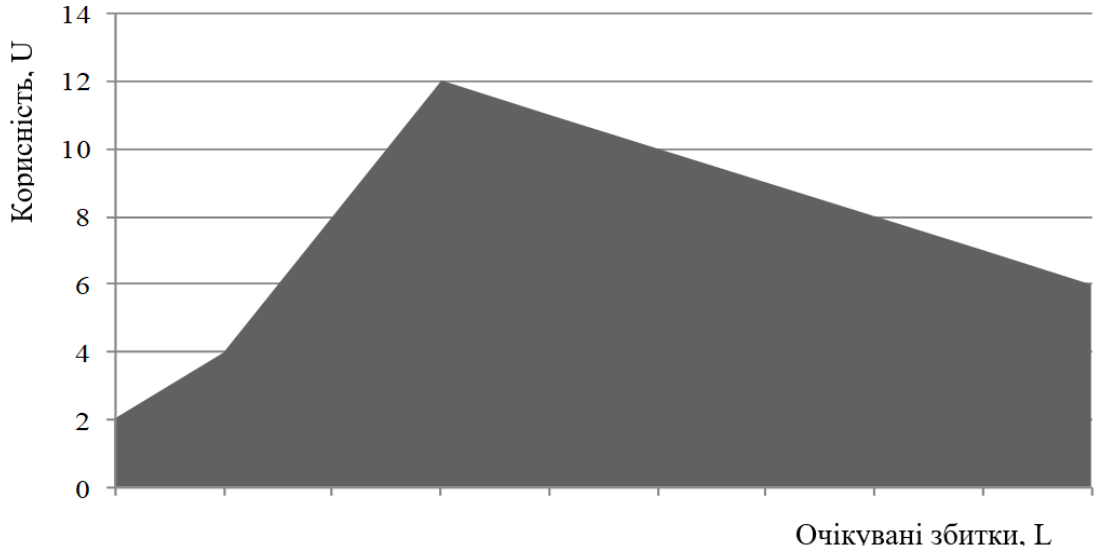

Рис. В.3. Функція корисності підприємства, несхильного до ризику

Рис. В.4. Бізнес-процеси з організації кібер-страхування підприємства

Побудовано автором за [22]