НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК

«До захисту допущено»

Завідувач кафедри

_____ Дмитро ЛАНДЕ

“___”_____2022 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-науковою програмою «Системи, технології та математичні методи кібербезпеки»

зі спеціальності 125 «Кібербезпека»

на тему: Оцінювання рівня загроз на рівні інвестицій в кібербезпеку для виробничої інфраструктури

Виконав здобувач ступеня магістра ___2_ курсу, групи ____ФБ-01мн_____
(шифр групи)

Урсол Олексій Ігорович_____ _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник Гальчинський Леонід Юрійович _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент Корнага Ярослав Ігорович _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Здобувач ступеня магістра _____
(підпис)

Київ – 2022 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський)
Спеціальність – 125 «Кібербезпека»
Освітньо-наукова програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2022 р.

ЗАВДАННЯ
на магістерську дисертацію здобувачу ступеня магістра

Урсол Олексій Ігорович _____
(прізвище, ім'я, по батькові)

1. Тема дисертації: Оцінювання рівня загроз на рівні інвестицій в кібербезпеку для виробничої інфраструктури

науковий керівник дисертації Гальчинський Леонід Юрійович,
кандидат.техн.н., доцент кафедри інформаційної безпеки
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «____» _____ 2022 р. № _____

2. Термін подання здобувачем дисертації 06.06.2022 р.

3. Об'єкт дослідження: Сфера кібербезпеки відносно потенційних загроз _
_____

4. Предмет дослідження є методики оцінки ризику на рівні інвестицій ___
_____
_____
_____

5. Перелік завдань, які потрібно розробити: Проаналізувати стандарти інформаційної безпеки; Проаналізувати модель інвестування в кібербезпеку; проаналізувати методики оцінки Cy-VaR; Удосконалити існуючу методику оцінки Cy-VaR; Виконати апробацію удосконаленої методики
_____

_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу: 11 ілюстрацій

_____
_____

7. Орієнтовний перелік публікацій: публікація на тему: Оцінювання ризику кіберзагроз підприємства з метою визначення необхідниих витрат для певного рівня кіберзагроз

_____
_____

8. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Проаналізувати інформаційної безпеки та концептуалізувати ризики	01.02.2022	Виконано
2	Проаналізувати модель інвестування і кібербезпеку	15.03.2022	Виконано
3	Зробити первинний аналіз та зробити висновки на базі цього аналізу	01.04.2022	Виконано
4	Проаналізувати методики оцінки Cy-VaR	18.04.2022	Виконано
5	Удосконалити існуючу методику оцінки Cy-VaR	24.04.2022	Виконано
6	Виконати апробацію відносно удосконалення	28.04.2022	Виконано
7	Оформлення пояснювальної записки	28.04.2022	Виконано
8	Підготовка до захисту	13.05.2021	Виконано

Здобувач ступеня магістра _____ Олексій УРСОЛ
(підпис) (власне ім'я, ПРІЗВИЩЕ)

Науковий керівник _____ Леонід ГАЛЬЧИНСЬКИЙ
(підпис) (власне ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

Робота обсягом 85 сторінок включає 11 ілюстрацій, 3 таблиці, 9 джерел літератури та 1 додаток.

Об’єктом дослідження є сфера кібербезпеки відносно потенційних загроз.

Предмет досліджень є методики оцінки Cy-VaR.

Методи дослідження – аналіз методики оцінки Cy-VaR.

Метою роботи є вирішення проблеми застосування оцінки Cy-VaR на конкретних потенційних загрозах організації.

Результати роботи можуть використовуватися для проведення дослідження по оцінці Cy-VaR на конкретній компанії.

Ключові слова: кібербезпека, Cy-VaR, моделювання Монте-Карло, кіберризик.

ABSTRACT

Work volume 85 page includes 11 illustrations 3 tables, 9 source of literature and 1 application.

The object of the study is the cybersecurity of potential threats.

The subject of the research is the analysis of the Cy-VaR assessment methodology.

Research methods - analysis of Cy-VaR assessment methods.

The aim of the work is to solve the problem of applying Cy-VaR assessment to specific potential threats to the organization.

The results of the work can be used to conduct research on Cy-VaR estimates for a specific company.

Key words: cybersecurity, Cy-VaR, Monte Carlo modeling, cyber risk.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Cy-Var – Cyber Value at Risk

ПЗ – програмне забезпечення;

GDPR – General Data Protection Regulation

IT – інформаційні технології

DIS – проект міжнародного стандарту

FDIS – остаточний проект міжнародного стандарту

IEC – Міжнародна електротехнічна комісія

ВСТУП

Планування інвестицій в інформаційну безпеку є десь між мистецтвом і наукою. У даній роботі розглядаються та порівнюються існуючі наукові підходи та обговорюється зв'язок між моделями інвестицій у безпеку та показниками безпеки. Метою даної роботи є поглиблення застосування цінності під ризиком у кібер-сфері, з особливою увагою до її потенційної ролі в оцінці інвестицій у безпеку. Кіберризик є фундаментальним компонентом загального ризику, з яким стикається будь-яка організація. Щоб спланувати розмір інвестицій у безпеку та оцінити подальше зниження ризику, менеджерам настійно необхідно визначити його кількісно. Відповідно, вони можуть прийняти рішення про можливість розподілу залишкового ризику з третьою стороною, наприклад, страховою компанією. Останнім часом методи управління кіберризиками включають деякі заходи, засновані на квантилях ризику, які широко використовуються у фінансовій сфері. Вони посилаються на цінність під загрозою, яка в кібер-контексті має назву кіберцінності під загрозою (Cy-VaR).

Ця робота організована наступним чином: у 1 розділі буде проведено аналіз предметної області. У розділі 2 розглядаються основні особливості та складні питання Cy-VaR. Обговорюється можливе використання цієї міри ризику для підтримки інвестиційних рішень у кібер-контексті та пропонуються нові показники безпеки, засновані на ризиках. 3 розділ презентує удосконалення методики оцінки Cy-VaR та виконання апробації даної методики.

1 Аналіз предметної області

1.1 Стандарти інформаційної безпеки

Кіберзлочинність стає все більш поширеною. І в міру того, як ми поглинаємо цифрову епоху, так звану четверту промислову революцію, вона стає все більш складною та серйозною, що має жахливі наслідки. Оскільки кіберзлочинці стають все більш витонченими, кіберзлочинність вплинула на всі аспекти нашого життя. Оскільки пандемія COVID-19 посилила нашу залежність від цифрових систем, не дивно, що кібербезпека була знову представлена як одна з основних світових загроз у Global Risk Report 2022. Збої в кібербезпеці стали набагато гіршими, загрожуючи довгостроковому процвітанню.

Побудова надійної системи кібербезпеки та прогнозування загроз є важливими аспектами боротьби з кіберзлочинністю, але без надійних і складних планів управління кіберризиками неможливо досягти ні стійкості, ні управління.

Кіберзлочинність – це національне та міжнародне явище, яке швидко зростає, що впливає на бізнес, уряди та суспільство в цілому. Масштаби та складність цієї незаконної діяльності мають далекосяжні та катастрофічні наслідки, а проблема ускладнюється тим фактом, що кіберзлочинці діють через національні кордони, експлуатуючи технічну інфраструктуру.

Системи інформаційних технологій (IT), мережі та критична інфраструктура – це все це об’єкти для керівних принципів кібербезпеки. У середовищі продукту, системи, процесу, стандарт кібербезпеки встановлює як функціональні, так і гарантійні критерії. Кібератаки є дорогими, завдають шкоди і становлять зростаючу загрозу для бізнесу, уряду та суспільства. На щастя, арсенал стандартів допомагає залишатися на крок попереду конкурентів. Добре розроблені стандарти кібербезпеки є хорошим сигналом для придбання продуктів безпеки, оскільки вони є послідовними серед виробників продуктів.

Стандарти кібербезпеки зазвичай не залежать від реалізації та охоплюють широкий спектр особливостей, від математичного визначення криптографічного методу до специфікації функцій безпеки у веб-браузері. Вимоги користувачів мають бути задоволені, але стандарт також має бути реалістичним, оскільки ціни мають бути низькими, щоб відповідати критеріям. Крім того, навіть якщо вироби перевіряються на відповідність стандарту, вимоги стандарту повинні бути підтверджені; інакше користувачі не зможуть судити про безпеку.

Стандарт ISO[1] «Документ, створений консенсусом і затверджений визнаним органом, який надає правила, норми чи рекомендації для широкого та повторюваного використання», відповідно до Міжнародної організації зі стандартизації (ISO).

Характеристика дій або їх результатів з метою встановлення найвищого рівня порядку в конкретній ситуації. Було розроблено кілька стандартів кібербезпеки, щоб допомогти підприємствам краще керувати ризиками безпеки, запровадити засоби контролю безпеки, які відповідають нормативним і нормативним вимогам, а також досягти ефективності та економічної ефективності. У світі наведено широкий огляд стандартів кібербезпеки та підкреслено деякі з найважливіших світових, регіональних, національних, промислових та національних стандартів. Також розповідається про переваги наявності стандартів і про те, як підприємства можуть залучитися до стандартних досліджень і розробок.

Міжнародна організація зі стандартизації (ISO) — це абревіатура англійської назви. Міжнародна організація зі стандартизації розробляє стандарти, щоб гарантувати, що продукти та послуги є безпечними, надійними та високоякісними, а виробничі процеси базуються на найефективніших ресурсах та мають найменший вплив на навколишнє середовище. Управління якістю, екологічна безпека, енергоменеджмент та інші теми охоплюються стандартами ISO.

Як виникають стандарти ISO? Міжнародна організація зі стандартизації поділяє процес виробництва стандартів на шість етапів. Нижче наведено кроки:

1. Стадія пропозиції. Коли бізнес-організації або групи споживачів роблять запит, робиться перший крок у розробці нового стандарту. Відповідний комітет ISO вирішує, чи дійсно потрібен новий стандарт.
2. Етап підготовки. Для створення робочого проекту нового стандарту формується робоча група. Робоча група складається з спеціалістів та зацікавлених сторін у предметі; коли проект буде визнано придатним, батьківський комітет робочої групи обирає, який етап буде наступним. Етап введення в експлуатацію Члени батьківського комітету розглядають та коментують проект стандарту під час цього необов'язкового етапу. Комітет може перейти до наступного кроку після досягнення згоди щодо технічного змісту проекту.
3. Етап запиту. На цьому етапі проект стандарту називають проектом міжнародного стандарту (DIS). Він надсилається членам ISO для зворотнього зв'язку та, зрештою, для голосування. ISO публікує DIS як стандарт, якщо він схвалений на цьому етапі без будь-яких технічних змін. В іншому випадку він переходить до етапу затвердження.
4. Етап затвердження. Проект стандарту представляється членам ISO як остаточний проект міжнародного стандарту (FDIS). Вони переважно підтримують нову норму.
5. Стадія публікації. Якщо члени ISO погодяться, FDIS буде опубліковано як офіційний міжнародний стандарт, якщо члени ISO його схвалять.
6. Члени ISO голосують за схвалення стандартів. Принаймні дві третини учасників повинні проголосувати «за» стандарт, але не більше однієї чверті учасників має проголосувати «проти».

Як підприємства отримують сертифікат ISO?

Для компанії процедура сертифікації ISO може бути дорогою, тривалою та потенційно катастрофічною. Перш ніж вживати будь-яких заходів для отримання сертифікації, визначення необхідності сертифікації може бути найкритичнішим етапом.

1. Першим етапом сертифікації є визначення того, чи є вона економічно ефективною. Нижче наведено деякі з причин, чому організації проводять сертифікацію:
2. Норми необхідні. Деякі фірми та продукти повинні бути сертифіковані, щоб відповідати галузевим вимогам.
3. Комерційні вимоги. Деякі підприємства вимагають, щоб сертифіковані продукти та послуги відповідали основним стандартам, навіть якщо сертифікація не є вимогою законодавства.
4. Специфікації замовника. Незважаючи на те, що сертифікація вимагається галузевими стандартами або правилами, деякі клієнти, наприклад державні установи, можуть віддати перевагу або потребувати її.
5. Консистенція покращилася. Великі фірми можуть використовувати сертифікацію для забезпечення постійної гарантії якості в бізнес-підрозділах та на міжнародному рівні. Виконання клієнта. Клієнти, які використовують продукт або послугу в різних країнах і країнах, прагнуть узгодженості. Дотримання стандартів також може допомогти визнаній фірмі у вирішенні проблем споживачів.

Порядок сертифікації ISO визначається стандартом та сертифікуючим органом. Організаціям може знадобитися спочатку вивчити та вибрати відповідний орган сертифікації для популярних стандартів.

Багато країн, у тому числі Україна, використовують стандарти ISO. ДСТУ ISO — назва української версії стандартів.

Перш за все, наявність чинного на підприємстві сертифікату ISO дає впевненість у безпеці продукції, яку купує споживач. Ці загальноприйняті стандарти визначають виробничі характеристики та стандарти, відповідно до яких повинні виготовлятися товари та послуги. Саме завдяки стандартизації споживач може бути впевнений у належній якості продукції та послуг.

По-друге, до розробки стандартів залучаються не лише виробники та постачальники послуг, а й організації споживачів з різних країн. Це означає, що продукція та послуги сертифікованих компаній повністю відповідають вимогам

усіх споживачів.

Це вагомі причини звернути увагу на наявність або відсутність сертифікатів ISO на підприємствах.

Усі стандарти ISO мають позначку, яка визначає сферу їх застосування. Цифри після двокрапки в назві стандарту вказують на те, про що стандарт (якість, екологія тощо), а цифри після нього вказують рік його затвердження.

Стандарти взаємодіють різними способами. Деякі стандарти є додатковими, тобто вони допомагають або покращують вимоги іншого стандарту. Наприклад, ISO часто випускає стандарти з кількох частин, які можуть бути доповнювальними, причому кожна частина є окремим томом, який розглядає різні аспекти основної проблеми. Деякі стандарти можуть суперечити один одному, що призводить до розбіжностей або невідповідностей між стандартами, що може призвести до таких проблем, як технологічна несумісність або відповідність закону. Інші стандарти є дискретними, тобто вони не мають прямого впливу один на одного. Існують також прогалини в стандартах, коли не було розроблено жодного офіційного стандарту для певної галузі безпеки, проте пропозиція може існувати. Прогалини в стандартах часто виникають, коли технології розвиваються занадто швидко, щоб стандарти не відставали. За інших обставин виникає недійсність, оскільки не було досягнуто угоди щодо технології чи стандарту.

ISO/IEC 27000 - міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (IEC) разом публікують ряд міжнародних стандартів, включаючи стандарти інформаційної безпеки (IEC). Серія містить найкращі методи та рекомендації щодо інформаційної безпеки щодо побудови, розробки та обслуговування системи управління інформаційною безпекою.

Стандарт BS7799 Британський стандарт був підготовлений для менеджерів бізнесу та їх персоналу надати модель для встановлення та керування інформаційною безпекою системи управління (ISMS). Прийняття СУІБ має бути стратегічним рішенням організації.

BS7799 дає рекомендації щодо управління інформаційною безпекою для використання тих, хто відповідає за ініціювання, документування, впровадження

або підтримання безпеки в своїй організації. BS7799 також визначає вимоги до встановлення, впровадження та документування управління інформаційною безпекою системи.

BS7799 насправді «повний набір елементів керування, що містить найкращі методи роботи з інформаційною безпекою»

Це міжнародно визнана інформаційна безпека. Стандарт призначений для забезпечення спільної основи для розробки організаційні стандарти безпеки та ефективні методи управління безпекою. Він визначає вимоги до контролю безпеки, які мають бути запроваджені відповідно до потреб окремих організацій. Крім того, це гарантує наявність контролю ефективний – цінний інструмент як для IT-департаменту, так і для спільноти IT-аудиту.

BS 7799 [2] допомагають ідентифікувати управління та зменшити діапазон загроз, яким інформація постійно розкривається. Після відповідності вони забезпечують організації з впевненістю та задоволенням знаючи, що вони є захист їхньої інформації за допомогою засобів контролю, які широко використовуються добре керованими підприємства. Це чудова основа для розробки або покращення структура безпеки організації.

Сертифікація та відповідність Відповідність стандарту BS7799-2 вимагає, щоб організація впровадила та задокументували свою Систему управління інформаційною безпекою (СУІБ) у відповідно до цілей контролю, визначених у BS7799-2:2002 документаціях. Сертифікація BS7799-2 надає докази та впевненість, що організація має відповідати цілям контролю, викладеним у стандартній документації. Сертифікація визначає сферу діяльності організації ISMS та будь-які виключення цілей контролю. Для того, щоб отримати сертифікацію, організація повинна спочатку досягти відповідності встановленим вимогам у настанові BS 7799-2:2002. Після того, як це було досягнуто. Процес сертифікації вимагає зовнішньої перевірки з боку акредитованого BS7799 аудитора. Аудитор працюватиме в сертифікованому органі або BSI. Там вони проведуть аудит організацій ISMS відповідно до засобів контролю, викладених у BS 7799-2:2002. Після завершення аудиту організація отримає сертифікат BS7799-

2. У сертифікаті буде детально описано сферу діяльності організації СУІБ та декларацію застосовність (SOA).

1.2 Концептуалізація моделей ризиків

Багато основних стандартів інформаційної безпеки, наприклад ISO 27000 та BS7799 пов’язані з проблемою оцінки та дослідження інформаційних загроз. Ці стандарти широко використовуються сьогодні і відповідають багатьом міжнародним вимогам, але вони не враховують додаткових аспектів. Ці підходи обмежують оцінку відповідно до чинних нормативних актів, які регулюють рішення про рівень інформаційної безпеки на основі інформації, наданої клієнтом, або інформації, зібраної під час аудиту компанії. Регуляторні показники, такі як інвестиції в інформаційну безпеку, вартість створення пакету захисту, вартість впровадження небезпеки та потенційні збитки, в першу чергу оцінюються при оцінці інформаційних ризиків, і, таким чином, є досить обмежуючими змінними в оцінці. Сьогодні комплексна оцінка інформаційних ризиків має враховувати ряд факторів, серед яких чотири основних: соціально-психологічні показники зловмисника, технічний рівень захисту компанії чи об’єкта, ймовірність конкретної загрози конкретному зловмиснику та звичайно, стабільність компанії. Це не всі ознаки, які можуть бути присутніми в процесі оцінки інформаційних та фінансових ризиків компанії, але вони є найбільш істотними при проектуванні захисних систем. Коли ці чотири показники використовуються для комплексної оцінки компанії, можна отримати інформацію про кожен із охоронюваних об’єктів, співробітників, які можуть бути злочинцями, і суб’єкта атаки, можливих зовнішніх зловмисників або принаймні уявлення про тип зовнішнього зловмисника, загрози, що відображають недоліки. Однак найбільш широко використовувані методи аналізу і дослідження ризиків, як зазначено в міжнародних і національних стандартах, мають ряд недоліків, у тому числі

надмірно загальний концептуальний і рекомендаційний характер подання матеріалів, що фактично виключає можливість врахування та значно знижує об'єктивність і точність результатів.

Тому варто спочатку звернути увагу на концептуалізацію моделей ризиків. Даною ідеєю можна скористатись у роботі [3]. Автор даної роботи намагається виокремити певні концептуальні моделі (специфікації) ризиків, в рамках яких можна інтерпретувати практично всі відомі прояви ризику і які можна використовувати як шаблони при виконанні аналізу ризиків.

Модель "небезпека – ризик". Назва моделі походить від поняття ризику як прояву (наслідків) небезпек різного походження. Наслідком реалізації створених ними небезпек або загроз, згідно з цією моделлю, є сукупність можливих негативних подій, кожна з яких характеризується парою параметрів: вірогідністю реалізації та розміром шкоди, яка настане, якщо ця подія відбувається. Необхідною умовою формування ризику є наявність численних можливостей можливого розвитку поганих подій (ризик травмування), тобто неясність на рівні наслідків прояву небезпек. Механізм розвитку ризику в процесі контакту людини з природою, техносферою, тісно пов'язаний з цією парадигмою, особливо важливою для захисту інформації. Ми надамо деяку формалізацію елементів, безпосередньо пов’язаних з існуванням небезпек, щоб ознайомитися з їх атрибутами. Почнемо з визначення двох типів об’єктів. Перший – це об’єкт ризику (ОР). Це людина, і з її існуванням і діяльністю пов'язані об'єкти з багатьох сфер, таких як підприємства, торгово-економічні, медичні та інші організації та установи, державні органи, політичні партії, міжнародні організації тощо. Причина (ціль) його існування (діяльність, функціонування) є визначальною у визначенні ОР, а для більш-менш складних речей мета може бути комплексною, векторного характеру.

Далі йде категорія джерел небезпеки (ОН). Небезпека — це особливість середовища ОР, яка відноситься до ймовірності того, що це середовище матиме негативні наслідки для ОР. Застосування такого впливу описується у вигляді загрози за певних умов. Загалом, рівень невизначеності при аналізі та розв’язанні

практичних завдань дуже різний, і ми маємо різні причини цієї невизначеності, як зазначалося раніше. Одним із джерел сумнівів є недостатня інформація про ОР, його структуру, режими роботи, властивості та параметри. В результаті ми не можемо однозначно зв'язати набір значень компонентів вектора X зі значеннями елементів вектора Y, тобто ми не знаємо, як стан ОР впливає на ефективність його функціонування (якість продукції чи послуг). Ця неоднозначність ускладнює техніку нормалізації стану ОР шляхом нейтралізації ризиків, в яких він функціонує. Слід зазначити, що вихідна концептуальна модель аналізу та інтерпретації ризику базується на виділенні невизначеності, породженої наявністю небезпек, що породжує ризикову ситуацію, звідси й назва «модель небезпека – ризик». Невизначеність щодо структури, розмірів і властивостей PR можна знайти в усіх моделях ризику, і це є важливою, але не визначальною рисою їх представлення.

Концептуальна модель "невизначеність – ризик". Друга теорія походження ризику базується на передумові наявності природної невизначеності в результатах конкретних дій на початку операції. Ми отримуємо типову ризикову ситуацію, коли ця вихідна невизначеність нашаровується на ситуаційну різноманітність можливих наслідків (рішень) з кількісною оцінкою ймовірності кожного з них. «Невизначеність – ризик» — це модель ризику, заснована на цій концепції.

Варто зазначити, що природна невизначеність часто є наслідком спільної дії ряду випадкових елементів, вплив яких визначає статистичну стабільність характеристик невизначеності в цілому. В результаті, якщо ці якості можна визначити і включати розрахунки або вимірювання, то можливе ефективне рішення початкової ризикової ситуації. Аналітично, шляхом мінімізації конкретного типу інтегрованої оцінки ризику – так званого середнього ризику, який враховує та оцінює багато елементів ризику одночасно. Тобто однією з відмінних характеристик концептуальної моделі «невизначеність – ризик» є реальна можливість виявлення найкращого шляху виходу з ризикової ситуації. На жаль, цей оптимізм стримується наявною невизначеністю критерію, що створює можливість для багатьох ідеальних оцінок (у цьому прикладі - середніх і

медіанних оцінок). Окрім теорії вимірювання та розпізнавання, є також теорія ігор, портфельне інвестування тощо.

Модель "можливості – ризик / шанс". Модель можливостей, заснована на ризику та випадковості. Підхід «можливість – ризик/випадок» є ще однією концептуальною моделлю генерування ризику. Ця модель зазвичай використовується для зображення обставин, які виникають під час управління фінансовими та економічними небезпеками, щодо співвідношення між ризиком і прибутком, а також коли ризик виникає при спробі максимізувати прибуток при мінімізації збитків. Ця модель ризику характеризується так званими спекулятивними ризиками[4,5], які мають потенціал як для негативного (збитки), так і для позитивного (прибуток) результатів, причому останній, тобто можливість позитивного результату, зазвичай позначається терміном «шанс». Концепція «можливість – ризик/шанс», з іншого боку, не обмежується фінансово-економічною сферою. Ця модель корисна, коли виникає потреба генерувати велику кількість можливих варіантів дій, подій, рішень тощо, тобто коли ситуація багатоальтернативного ризику створюється штучно, а не в результаті небезпек чи інших природних факторів. Наприклад, знайти та вивчити можливі прийнятні рішення в даній ситуації, сфері діяльності тощо. Модель «можливість – ризик», зокрема, дозволяє адекватно описувати ситуації, що виникають при використанні сценарного підходу до прогнозування можливих наслідків витоку конфіденційної чи конфіденційної інформації[6], аналізу та узагальнення бізнес-загроз, аналітичних послуг[7], досліджень і так далі. Розглянемо використання концептуальної схеми «можливість-ризик» у сфері прикладних математичних моделей при вирішенні задачі структурної ідентифікації складної системи, а саме вибору структури апроксимаційної моделі. практичне визначення областей. Суб'єктом цього ризику є математична модель реального об'єкта (складної системи), що базується на експериментальних даних, зібраних під час дослідження або під час експлуатації цього об'єкта. Коли об’єкт моделювання має складну внутрішню структуру і дослідник не знає, як вона працює (як у випадку з так званим «чорним ящиком»), об’єктивну мету математичної моделі стає важко

досягти. Побудова наближеної моделі, яка лише формально відтворює (копіює) поведінку реального предмета на сукупності емпірично зібраних даних щодо значень його вхідних і вихідних параметрів, є виходом із цієї проблеми (змінні, координати тощо). Тобто, створюючи наближену модель, немає потреби турбуватися про змістовно-оперативну близькість моделі до реального механізму дії об'єкта. У результаті з'являється багато різних типів наближених моделей, деякі з яких можуть бути згенеровані дослідником. Кожна альтернатива має власний набір переваг і недоліків, тому вибрати оптимальний варіант наближеної моделі є складним завданням. Це стандартна проблема вибору, і відповідь додає до невизначеності, вимагаючи вибору критерію рішення (подібна ситуація вже розглядалася вище для концептуальної моделі «невизначеність – ризик», де кожен із двох критеріїв оптимальності відповідав своєму оптимальне рішення).

Запропоновано три концептуальні моделі формування ризику, кожна з яких має різне джерело (природу походження) невизначеності, що є необхідною передумовою для створення ризикової ситуації. Першу концептуальну модель ризику, модель ризику-ризику, буде найбільш доцільно використовувати на етапі проектування системи захисту інформації (СЗІ), зокрема на початковому етапі цього процесу, при оцінці рівня інформаційної безпеки підприємства за результатами передпроектного аудиту. За відсутності спекулятивних ризиків доцільно використовувати третю концептуальну модель у форматі «ризик-ризик» при розгляді архітектури та елементів СЗІ: сторона, що захищає, просто мінімізує витрати на розробку СЗІ (однак це обмеження не застосовується можливість отримати можливий прибуток є основним активуючим фактором). Нарешті, історично недосконала інформація про загрози, втрати (втрати), їх ймовірності, інтенсивність та рівні може зробити модель ризику невизначеності доцільною для використання разом із двома раніше описаними моделями.

Наступний розглянутий підхід стандартизований метод визначення необхідного обсягу витрат на безпеку СЗІ та захист даних. Запропонований метод спочатку визначає активи, загрози та вразливі місця систем СЗІ шляхом аналізу ризиків безпеки, а потім пояснює метод оцінки необхідних інвестицій у безпеку.

Управління ризиками безпеки, що зазвичай застосовується організацією, складається з:

1. Ідентифікація активів бізнесу. Інформація та ресурси, які є корисними для організації, називаються активами. Актив необхідно оцінити після його визнання. Оцінити матеріальні активи просто, оскільки вони вимірюються в грошах і включають амортизацію. Прикладами матеріальних активів є фізична інфраструктура (наприклад, сервери, робочі станції та мережеве обладнання) та програмне забезпечення інформаційної системи. Нематеріальні активи, такі як бізнес-дані, організаційні знання, репутація компанії та інтелектуальна власність, що знаходяться в організаційній структурі, часто важче оцінити. При оцінці активів їх часто поділяють на різні категорії або класи[8,9]. Використовуючи класи, легше побачити типові загрози безпеці. Вони також допомагають організаціям визначити пріоритети життєво важливих активів. Різні класи активів визначаються різними методологіями оцінки ризиків. Якщо більше класів точніше, то менше класів заощаджує час, коли справа доходить до обговорення та вибору відповідного позначення класу. Критичні, помірні та низькі класи активів є прикладами парадигми трьох класів. Прикладами важливих активів є фінансові дані, інтелектуальна власність, інформація про банківський рахунок та інші життєво важливі активи. Внутрішня корпоративна інформація, замовлення на закупівлю, мережеві ініціативи та інформація на внутрішніх веб-сайтах є прикладами помірних активів. Інформацію про низькі класи активів часто можна знайти на загальнодоступних веб-сторінках, оголошеннях для преси, брошурах продуктів і технічних посібниках.
2. Визначення загрози та оцінка потенційну шкоду, яку може завдати успішний удар. Інформаційні активи компанії під загрозою. Будь-яка ймовірна подія, яка має несприятливий результат, вважається небезпекою. Організації повинні чітко визначити небезпеку для своїх інформаційних активів, щоб покращити безпеку та розробити стратегію та політику безпеки. Загрози активам організації поділяють на кілька категорій, включаючи мережі, програмне забезпечення, дані та фізичні компоненти. Стихійні лиха та людська діяльність

є найпоширенішими видами небезпек, причому загрози, спричинені людиною, є або зловмисними, або нешкідливими. Крадіжка, втрата або знищення активів організації, шахрайство, несанкціонований доступ до онлайн-сервісів, зараження шкідливим кодом, розкриття особистих даних і крадіжка персональних даних – усе це приклади згубних людських загроз. Згідно з більшістю статистичних даних, частота проблем безпеки та конфіденційності зростає. Згідно з опитуванням CSI 2007 року, зловживання мережею, зловмисне програмне забезпечення та крадіжка ноутбуків/мобільних пристроїв є трьома найпоширенішими типами атак безпеки[8].

3. Уразливості безпеки, які можуть бути використані зловмисниками. Уразливості зазвичай пов’язані з технологічними проблемами, але вони також можуть бути викликані людським компонентом. Користувачі, які передають свої паролі або використовують слабкі паролі, не розуміють чи ігнорують політику безпеки, відкривають надійну електронну пошту, переглядають веб-сайти або завантажують шкідливе програмне забезпечення, викликають цю форму вразливості. Розкриття вразливості програмного забезпечення стало головною темою, яка викликала бурхливі дебати серед вчених. У той час як спільноти з відкритим кодом стверджують, що відкритість покращує захист активів, інші експерти та постачальники програмного забезпечення стверджують, що відкритість є більш цінною для зловмисників. Ідентифікація вразливостей як зовнішніх ефектів, що пропонуються, і конкретних предметів, які вважаються засобом обміну на різних ринках уразливості, є одним із механізмів безпеки. Це означає, що постачальник або власник системи надає стимул від першої особи, який демонструє вразливість, при цьому стимул з часом збільшується, оскільки власник системи отримує впевненість у безпеці. Аукціон — це альтернативний механізм, за допомогою якого хтось, хто знає про вразливість, повідомляє про це, а інші демонструють готовність заплатити за це.
4. Оцінка ризику безпеки. Після визначення ризиків безпеки їх слід оцінити на предмет потенційної втрати та ймовірності виникнення. Оцінка ризику – це

процес визначення можливого впливу окремого ризику шляхом зважування ймовірності його виникнення та наслідків, якщо це станеться. Це допомагає фірмам визначити відповідні засоби контролю та системи безпеки, у які слід інвестувати, щоб оптимізувати економічні вигоди. Існує безліч підходів до оцінки ризику на вибір. Кількісний аналіз ризиків має на меті обчислити числові значення ймовірності та впливу ризику, а також витрати та переваги впровадження систем контролю та безпеки. Метою контролю безпеки є зниження ризику до такої міри, що граничні витрати на додавання засобів контролю дорівнюють вартості додаткової економії на інцидентах безпеки. Замість того, щоб надавати активам точну фінансову вартість, прогнозовані збитки та вартість засобів контролю та систем, якісний аналіз ризику спрямований на оцінку відносних цінностей, на відміну від кількісного підходу. Найпоширенішим методом проведення якісного аналізу ризику є використання комбінації анкет та спільних семінарів. Як якісні, так і кількісні методи мають свій набір переваг і недоліків. Проблема з кількісним аналізом ризику полягає в тому, що не існує загальновизнаного підходу до розрахунку вартості активів, а також вартості засобів контролю та систем, які необхідно запровадити. Перевага якісного методу полягає в тому, що він вимагає меншої кількості людей для завершення процесу, а також усуває необхідність точної оцінки активів і контролю витрат. Недоліком якісного методу є те, що результати часто неоднозначні, оскільки вони базуються на відносній вартості активів. Малому бізнесу з обмеженими ресурсами в цілому комфортніше з якісним підходом.

5. Стратегії мінімізації ризиків. Після визначення та оцінки ризиків, організація вибрати обирає найбільш правильну стратегію, щоб максимально мінімізувати ризик. Стратегії включають чотири головних напрямки:
   5.1. Усунувши причину ризику або ризику активів, ви можете уникнути загроз і атак. Зазвичай це ситуація, коли серйозність небезпеки переважає переваги володіння чи використання певного активу, наприклад повністю відкритого інтернет-з’єднання.

5.2. Впроваджуйте відповідні технології та методи (наприклад, брандмауери, антивірусні системи тощо) або встановлюйте належні політики безпеки, щоб зменшити ризик використання активу (наприклад, паролі, контроль доступу, блокування портів тощо). Основною стратегією управління ризиками є пом'якшення.

5.3. Передача ризику шляхом часткової передачі ризику організаціям, що надають охоронні послуги, або шляхом придбання страховки[10]. Цей тип передачі ризику останнім часом набуває значення як підхід до застосування заходів безпеки в компанії.

5.4. Вжиття заходів безпеки як вартість ведення бізнесу. Утримання ризику – це підхід до управління ризиками, при якому вартість інвестування або страхування від ризику переважає загальні втрати з часом.

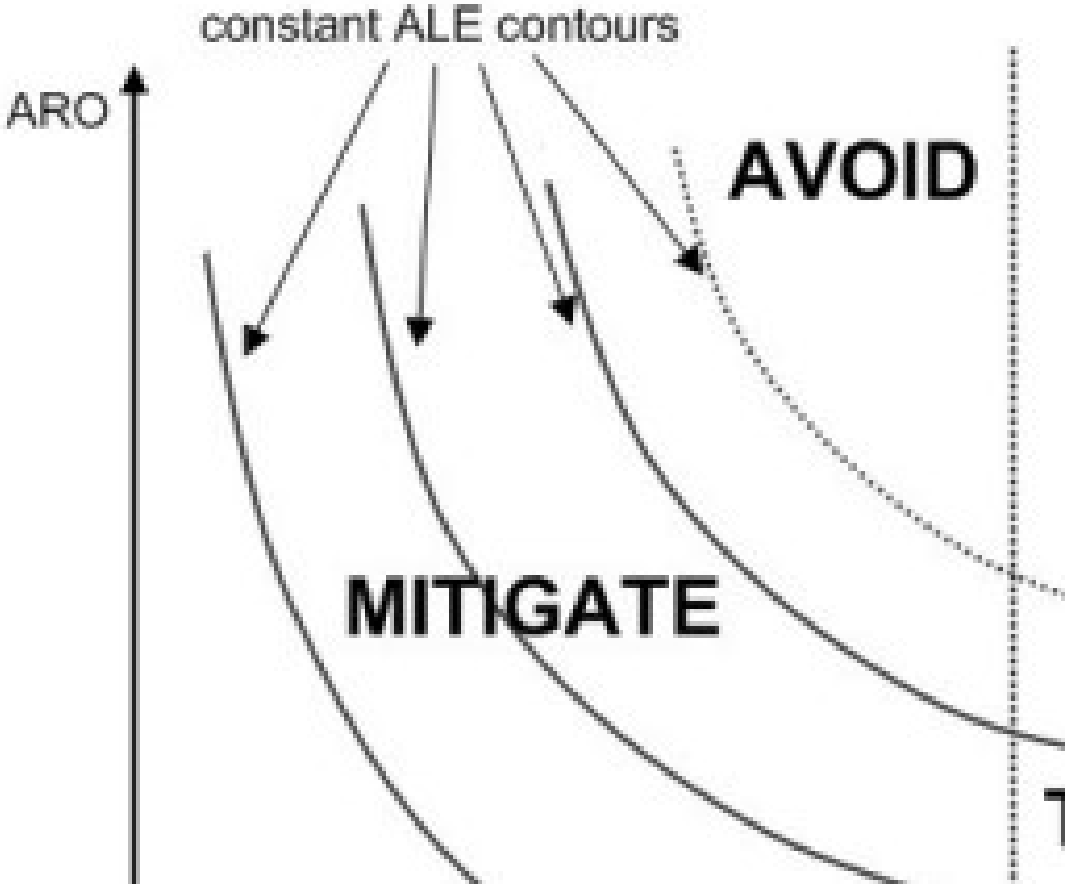

Рисунок 1.1: Стратегії мінімізації ризиків

Оптимальне застосування цих тактик не завжди може бути досяжним, що вимагає компромісу або використання комбінації обох. На рис. 1.1 зображені різні стратегії. Оцінку ризиків безпеки можна розділити на чотири регіони, кожен з яких характеризується трьома кордонами. Перша межа визначає найнижче значення річної частоти випадків (ARO), при якому ризик загрози може бути прийнятним. Наприклад, можна ігнорувати небезпеки зі значеннями частоти менше ніж раз на 1000 років. Друга межа – це максимальна очікувана річна тривалість збитків ALE, за якою вплив може бути катастрофічним. Однією з можливих відповідей на цей тип небезпеки є передача ризику страховій компанії або зниження кількості випадків понад ліміт. Третя межа — максимальне значення ALE, яке визначає уникнення загрози. Інвестування в безпеку може допомогти пом’якшити інші небезпеки.

Управління ризиками інформаційної безпеки є серйозною проблемою для всіх підприємств. Результатом дослідження є рекомендація, яку можна розробити за допомогою стандартизованого підходу. Методична основа, яка використовується в процесі управління ризиками для визначення активів, є відправною точкою для цього підходу. Це дає чудові знання про те, що і чому слід захищати в конкретній організації. Аналіз загроз інформує корпорацію про небезпеки та виклики, з якими вона стикається в глобальних бізнес-процесах. Поєднання цих методологій дає повне розуміння впливу, який інформаційна безпека може мати на існуючі бізнес-операції. Крім того, аналіз уразливості визначає, де і як може проявитися небезпека. Для визначення ймовірності загрози можна використовувати комбінацію виявлених уразливостей та відповідних процедур зменшення ризику. Після того, як ризик буде визнаний, фінансові показники можна використовувати для оцінки інвестицій, спрямованих на зниження ризику. Наразі не існує стандартної методології для оцінки фінансового ризику, пов’язаного з подіями безпеки, і рекомендується використовувати комбінацію індексів, об’єднаних або скоригованих у кожному конкретному випадку, оскільки вартість засобів захисту може значно відрізнятися. Деякі включають витрати на апаратне забезпечення, програмне забезпечення та

послуги, а інші включають внутрішні витрати, такі як непрямі накладні витрати та довгострокові наслідки для продуктивності. Кожен з індексів, ROI, NPV та IRR, має переваги, але їх самостійне використання не є відповідним підходом. В результаті поєднання цих методологій є найкращим способом оцінити необхідні інвестиції.

1.3 Модель інвестицій в інформаційну безпеку: Представництво ресурсів та організаційне навчання

Захист інформаційних технологій (IT) сьогодні залишиться ключовим завданням для організацій, яким необхідно захистити свої IT-системи, дані, інтелектуальну власність та бізнес-процеси від атак, неправильного використання або технічних збоїв. IT-загрози можуть призвести, наприклад, до порушення виробничих і сервісних процесів, а також до крадіжки даних, що в свою чергу призводить до економічної шкоди, включаючи втрату продуктивності та доходу, втрату репутації [11]. Багато інцидентів безпеки пов’язані з кіберзлочинністю, яку можна розглядати як галузь, що розвивається. Галузі реагують на нові загрози інформаційній безпеці за допомогою великих інвестицій в IT-безпеку. Ландшафт IT-безпеки пронизаний не лише технологічними, а й фінансовими проблемами. Враховуючи бюджетні обмеження, ключовим економічним питанням для організацій є питання про те, які з їхніх активів (процесів, систем тощо) потребують якого рівня захисту, які контрзаходи безпеки (наприклад, брандмауери, системи виявлення вторгнень, навчання безпеки чи політики безпеки) забезпечити цей захист і скільки вам потрібно витратити на такі контрзаходи Для аналізу економічних проблем IT-безпеки запропоновано широкий спектр підходів з різних дисциплін, включаючи мікроекономіку фінанси, управління ризиками та теорію організації. Аналіз цих підходів дозволяє сформулювати три дослідницькі запитання:

1. Чому і як можна використовувати багатотеоретичну перспективу, засновану на «погляді на ресурси» та «теорії організаційного навчання», щоб структурувати та керувати дослідженнями у сфері інвестицій в інформаційну безпеку?

2. Якою мірою література сприяла розгляду ключових питань інвестування в інформаційну безпеку?

3. Які прогалини в дослідженнях інвестицій в інформаційну безпеку ще не вирішені? Підхід, заснований на загальноприйнятих «поглядах, заснованих на ресурсах» і «теорії організаційного навчання», заснований на прагненні забезпечити як статичні, так і динамічні (тимчасові) захист ресурсів організації на рівні компанії. Прийняття лише однієї теорії неминуче призводить до ігнорування статичної або динамічної перспективи. Використання мультитеоретичного підходу дозволяє запропонувати нову теоретичну модель інвестування в інформаційну безпеку

Ефективність та економічність інвестицій в інформаційну безпеку вже давно є важливою темою дослідження. Нині існують три міждисциплінарних напрямки досліджень, пов’язаних з інвестиціями в інформаційну безпеку:

1. Мікроекономічні підходи, засновані на теорії ігор;
2. Фінансовий аналіз на основі рентабельності інвестицій (ROI), чистої приведеної вартості (NPV) та внутрішньої норми прибутку (IRR);
3. Підходи до управління, засновані на теорії рішень, управлінні ризиками та теорії організації. Поєднання різноманітних теорій і підходів призводить до формування багатотеоретичної моделі, що дозволяє використовувати методи цих напрямів дослідження в комплексну модель, засновану на представленні ресурсів і теорії організаційного навчання.

Розробка теоретичної моделі інвестицій в інформаційну безпеку є складним завданням, оскільки природа контрзаходів різноманітна, охоплюючи стратегічні та оперативні питання з урахуванням правові, технічні та організаційні аспекти; інвестиції в інформаційну безпеку спрямовані не на отримання прибутку, а на зниження ризику, тобто вони є успішними, якщо «нічого не сталося», а отже,

потенційні результати (вигоди чи збитки) часто є нематеріальними. Прикладами нематеріальних результатів є переваги відповідності нормативним вимогам та довіри суспільства. Інвестування в процеси або продукти інформаційної безпеки не дає прямої віддачі, але може мати позитивний вплив на ефективність організації, якщо зменшує потенційні ризики. Також необхідно брати до уваги взаємодоповнюваність попередніх перспектив. По-перше, підходи, які використовують перспективу ex-ante, спрямовані на забезпечення підтримки прийняття рішень шляхом оцінки витрат і вигод від можливих інвестицій. По-друге, підходи, які використовують перспективу ex-post, відображають інвестиції, зроблені в минулому, і оцінюють, чи був бюджетний розподіл компанії ефективним. Перші дві з цих проблем можна вирішити на основі ресурсного погляду, тому що (a) різноманітні активи, такі як системи, дані або процеси, які необхідно захистити, можуть бути змодельовані як ресурси і (b) як матеріальні, так і нематеріальні ресурси, такі як брандмауери та знання безпеки, можуть бути чітко розглянуті. Теорія організаційного навчання особливо підходить для вирішення третьої проблеми, оскільки враховує здатність компанії вивчати та інтегрувати цикли часу та динамічного зворотного зв'язку. Загалом, як ресурсний погляд, так і теорія організаційного навчання, які є визнаними теоріями в літературі ІС, забезпечують відповідну теоретичну базу для дослідження інвестицій в інформаційну безпеку.

Поданувище інформацію про інвестиції в інформаційну безпеку можна оцінити з двох точок зору: з точки зору представлення ресурсів і теорії організаційного навчання. Ці дві точки зору доповнюють одна одну.

Погляд, заснований на ресурсах, за своєю суттю є статичним і зосереджується на володінні ресурсами та можливостями. Це означає, що він не враховує динаміку та часові ефекти. Навпаки, теорія організаційного навчання враховує такі ефекти, як прогрес у навчанні, досягнутий внаслідок минулих помилок організації з часом, що гарантує, що організація перетворює «інформацію на цінні знання, що, у свою чергу, підвищує її здатність довго термін адаптація». Таким чином, це дозволяє організації реагувати на середовище, що

динамічно змінюється.

Ресурсний погляд, запропонований у, вступає в силу і охоплює основні фактори (див. рис. 1), які необхідно враховувати при прийнятті інвестиційних рішень, наприклад, макроекономічні, конкурентне та цільове середовище компанії. Перевага погляду на основі ресурсів полягає в тому, що вона теоретизує різні компоненти фірми, її оточення та взаємовідносини один з одним і, на відміну від організаційної теорії навчання, не зосереджується на організації та її компонентах в деталях.

З точки зору "аналіз ресурсів" ключова пропозиція витоку ресурсних уявлень полягає в тому, що компанія має придбати та контролювати цінні, рідкісні, унікальні та незамінні ресурси та можливості для досягнення стійкої конкурентної переваги. Ресурсів фірми включають «всі активи, можливості, організаційні процеси, атрибути фірми, інформацію, знання тощо, контрольовані фірмою, які дозволяють фірмі розробляти та впроваджувати стратегії, що підвищують її ефективність та ефективність.

Інвестиції в інформаційну безпеку є підвидом (загальних) інвестицій в IT, і тому ресурсний погляд підходить для генерування інвестицій в інформаційну безпеку з трьох причин:

1. Небезпечні IT-ресурси або активи (IT-системи, дані, процеси тощо), які необхідно захистити, а також ресурси IT-безпеки, які забезпечують захист, можна моделювати як ресурси, що охоплюють обидва матеріальні ресурси, такі як брандмауери, і нематеріальні ресурси, включаючи знання про безпеку.[12]
2. Для структурування інвестицій в інформаційну безпеку в літературі ІБ використовувався ресурсний погляд. Певним прикладом є використання уявлення, засноване на ресурсах[13], для оцінки гіпотез щодо розміру організації, порушень безпеки та обговорює зв’язок поглядів на основі ресурсів та інвестицій у безпеку. Центральні елементи ресурсно-орієнтованого підходу також можна знайти в[14].

3. Ресурсна презентація вже послужила теоретичною основою для оглядів літератури в галузі ІС, наприклад «Модель цінності бізнесу в галузі інформаційних технологій». Ми зосередимося на презентації на основі ресурсів, яка була адаптована до інвестиційного контексту інформаційної безпеки[12], як показано на рис. 1.2

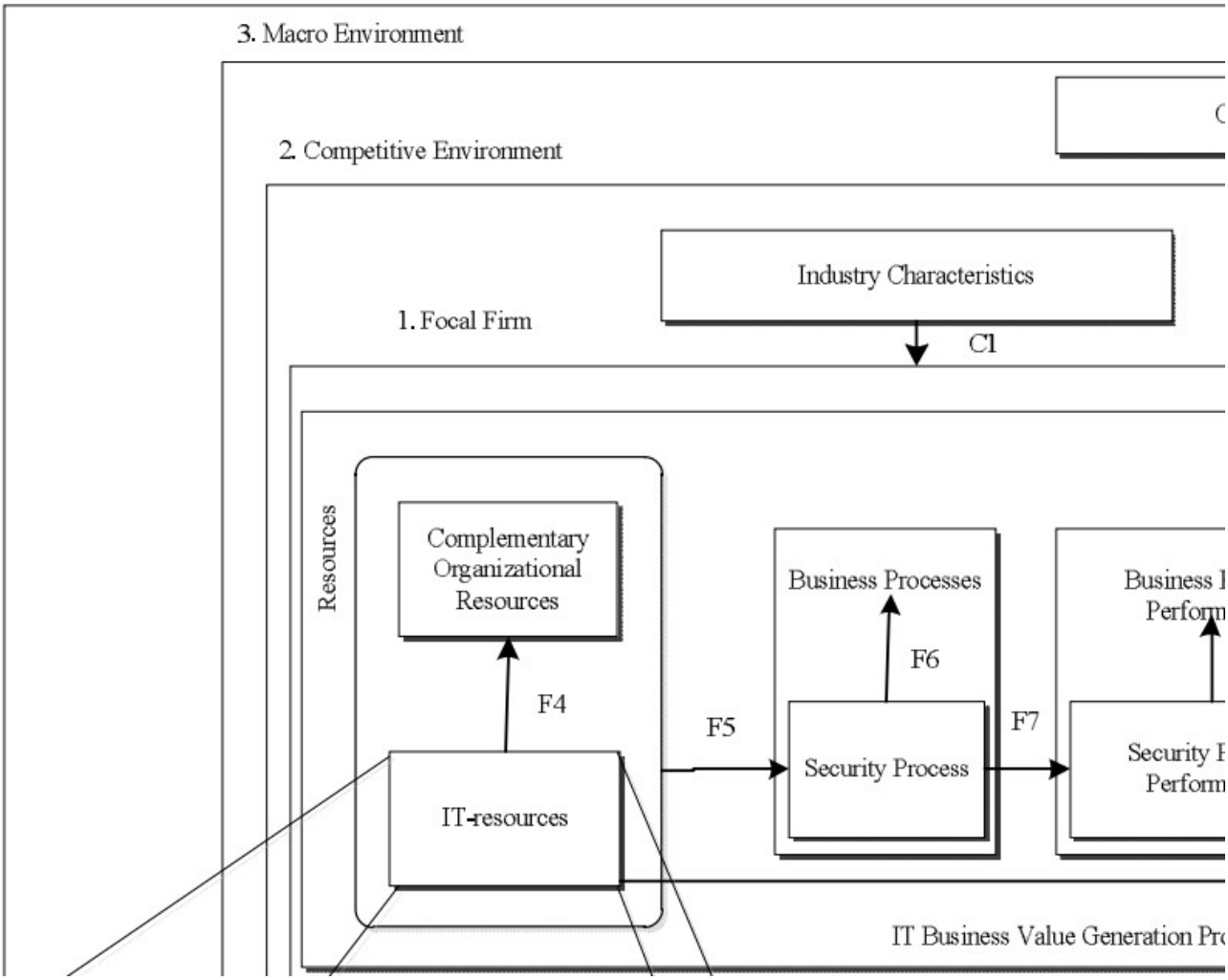

Рисунок 1.2 Ресурсно-орієнтована презентація інвестицій в інформаційну безпеку

На рис. 1.2 співвідношення між конструкціями означає «можна покращити». Впливи M1, C1 і C2 описують зовнішні фактори, які впливають на інвестиційні рішення інформаційної безпеки організації. Характеристики країни, такі як рівень розвитку або державне регулювання, впливають на інвестиційні рішення фірми у сфері інформаційної безпеки, що відображається в результаті впливу M1.

Конкурентоспроможність, регулювання, технологічні зміни та інші галузеві

фактори (C1) і торгові партнери, такі як покупці та постачальники (C2), впливають на рішення фірми інвестувати в інформаційну безпеку.

Вплив від F1 до F10 відображає вплив інвестицій у різні ресурси IT-безпеки в рамках спеціалізованої фірми. F1 відноситься до впливу ресурсів технології безпеки IT на технологічні ресурси, що не є безпечними, наприклад, інвестиції в брандмауер для захисту незахищених IT-ресурсів, таких як дані. Оскільки значна кількість інцидентів безпеки спричиняється людьми, а не технічними збоями чи зловмисниками[15], F2 розглядає вплив людських ресурсів IT-безпеки на незахищені технологічні IT-ресурси. Наприклад, семінари та тренінги з безпеки зосереджені на захисті даних. Вплив F3a пов'язаний з впливом людських ресурсів IT-безпеки на ресурси технологій IT-безпеки (наприклад, семінари з використання систем виявлення вторгнень) з F3b, навпаки (наприклад, системи, що контролюють передачу файлів, попереджають співробітників і, отже, тренують їх поінформованості). Вплив F4 пов'язаний з впливом IT-ресурсів на додаткові організаційні ресурси, наприклад, створення компанії, доступ до якої може бути захищений системами аутентифікації. Інвестування в ресурси IT-безпеки та додаткові організаційні ресурси може покращити бізнес-процеси або запустити нові (вплив F5). Вплив F6 відноситься до того, що процеси інформаційної безпеки призначені для захисту бізнес-процесів та їх основних ресурсів. Процеси безпеки є підтипами бізнес-процесів, оскільки «процес безпеки приречений на провал, якщо він не захищає бізнес-процес». Безпека у ефективність процесу вимірюється за допомогою продуктивності процесу безпеки (вплив F7). Ефективність процесу безпеки впливає на продуктивність бізнес-процесу, який є результатом зв’язку бізнес-процесу з процесом безпеки і концептуалізується як вплив F8. Процес створення цінності для IT-бізнесу, включаючи ресурси, процеси, ефективність бізнесу та безпеку, безпосередньо впливає на продуктивність організації (вплив F9). Вплив F10 означає «прямий зв’язок між IT та загальною продуктивністю фірми, минаючи вплив IT на бізнес-процеси».

Ми використовуємо теорію організаційного навчання, запропоновану в контексті інвестицій в інформаційну безпеку (див. рис. 3). Організаційне навчання

визначається як зміна знань організації, оскільки фірма з часом набуває досвіду.

Модель організаційного навчання включає три взаємопов’язані конструкції: контрольні змінні, стратегії дій та наслідки. Відповідно до вихідної моделі, відносини визначаються як «впливають» (стрілки на рис. 1.3).

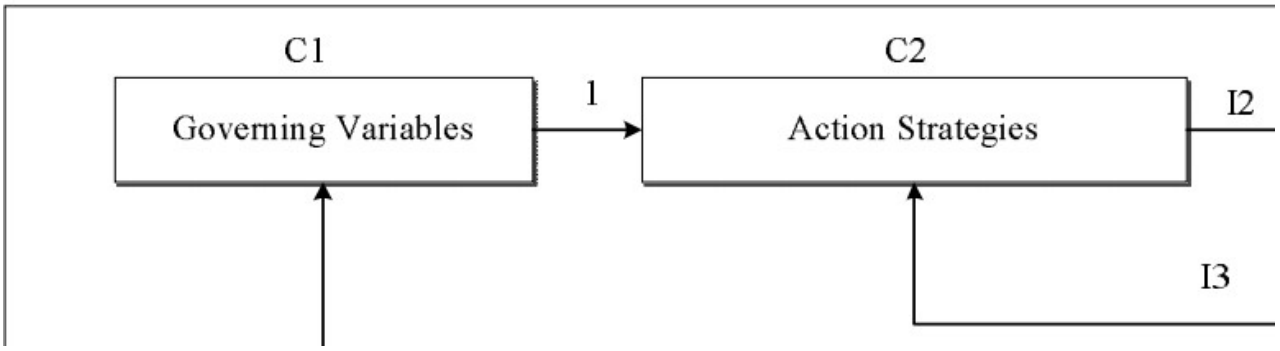

Рисунок 1.3 Взаємозв'язок елементів організаційної теорії навчання

Керуючі змінні (конструкція C1) - це цілі, до яких прагне компанія. Оскільки організації приводять свої дії у відповідність зі своїми цілями[16], регуляторні змінні впливають на інвестиційні рішення у сфері інформаційної безпеки (вплив I1). Наприклад, однією з цілей може бути дотримання державних і галузевих нормативних актів, таких як закон штату про захист інформації в інформаційно-телекомунікаційних системах. Стратегії дій (конструкція C2) є «послідовністю рухів» призначений для досягнення конкретних цілей, що вимірюються регуляторними змінними. У нашому випадку стратегії дій – це інвестиції в ресурси IT-безпеки, такі як впровадження брандмауера або системи виявлення вторгнень.

Стратегії дій впливають на наслідки (вплив I2). Прикладом є інвестиції в цехи безпеки, які, як очікується, зменшать кількість інцидентів з безпекою, спричинених працівниками.

Наслідки (конструкція C3) включають усі результати, пов’язані з інвестиціями в інформаційну безпеку, незалежно від того, чи є вони навмисними чи ненавмисними, продуктивними чи контрпродуктивними. Наслідки можуть відповідати регуляторним змінним, якщо фірма обрала відповідну стратегію дій. Прикладними наслідками є зменшення кількості інцидентів безпеки або

збільшення доступності послуг. Впливи 3 (I3) і 4 (I4) є додатковими можливостями навчання, які відображають, наскільки добре фірма намагається оцінити свої інвестиційні рішення в цій галузі інформаційної безпеки.

«Вплив I3» відноситься до одноциклового навчання, яке включає коригування, узгоджене з «існуючим набором правил і норм», тобто воно не пов’язане зі змінами контрольних змінних. Наприклад, навчання з одним циклом відбувається, якщо наслідком стратегії дій є зменшення кількості інцидентів безпеки, і фірма оцінює позитивний результат, щоб переконатися, що обрана стратегія дій є найкращою без зміни контрольних змінних.

Вплив I4 відноситься до процесу навчання, що відбувається за подвійним контуром і включає модифікації «фундаментальних правил і норм, що лежать в основі дій і поведінки». У випадку інвестиційного сценарію інформаційної безпеки таке навчання відбувається, якщо наслідки інвестиційних рішень не відповідають цілям і спонукають компанію переоцінити нормативні змінні та інвестувати по-іншому. У той час як навчання з одним циклом є загальноприйнятою моделлю дій, навчання з двома циклами забезпечує «зворотний зв’язок і більш ефективне прийняття рішень». Тим не менш, «переважна кількість навчальних процесів, що реалізуються в організації, є одним циклом, оскільки він призначений для виявлення та виправлення помилок, щоб робота була завершена, а дія залишалася в рамках заявлених рекомендацій». Зверніть увагу що конструкції C1–C3 з експозиціями I1 та I2 мають на увазі послідовність часу, тоді як експозиції I3 та I4 описують дві можливості процесів оцінки та навчання фірми, спрямованих на виправлення їхніх потенційних помилок та прийняття більш ефективних та ефективних рішень у майбутньому.

1.4 Інтегрована модель інформаційної безпеки

Інвестиційна модель [17]. Ми об’єднуємо ресурсний погляд, як показано на

рис. 1.2, і теорію організаційного навчання, як показано на рис. 1.3, у багатотеоретичну модель (див. рис. 1.4), яка зберігає переваги обох початкових теорій: інтегрована модель враховує переоцінку інвестицій в інформаційну безпеку шляхом динамічного включення зворотного зв'язку з одиничного та подвійного циклу навчання для коригування відповідних стратегій дій. Крім того, інтегрована модель створює специфічні для компанії компоненти, такі як бізнес-процеси та ресурси безпеки, що робить її сумісною зі встановленим набором досліджень щодо представлення на основі ресурсів.

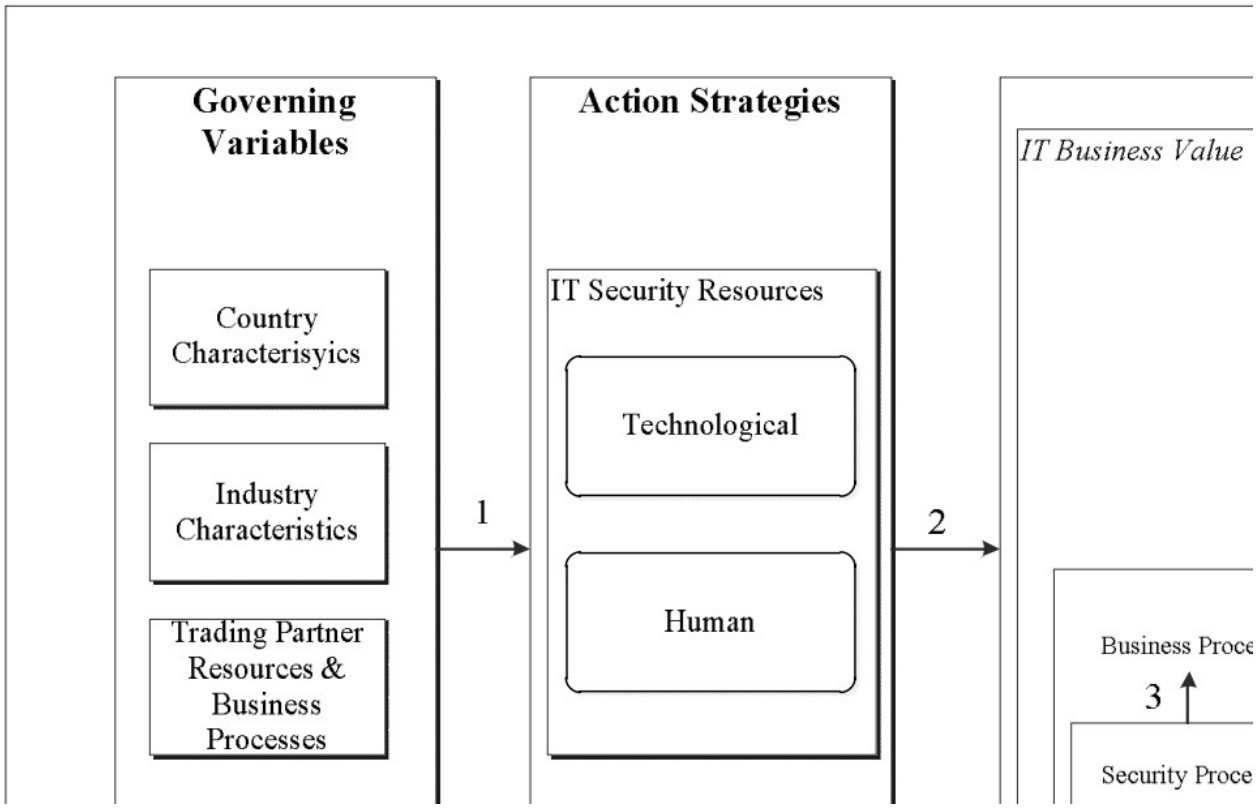

Рисунок 1.4 Інтегрована модель інвестування в інформаційну безпеку

Вихідні теорії ми поєднуємо так: особливості країни, галузеві характеристики та ресурси торгових партнерів, а також бізнес-процеси впливають на фірми при прийнятті інвестиційних рішень у сфері інформаційної безпеки; тому ці фактори класифікуються як регуляторні змінні. Контрольні змінні впливають (вплив 1 на рис. 3) на інвестиційні рішення в ресурси IT-безпеки, які узгоджуються зі стратегіями дій. Наприклад, державні норми певної країни вимагають певних інвестицій для проходження аудиту безпеки. Інвестиції в

технологічні або людські ресурси інформаційної безпеки пов’язані зі стратегіями дій. Це означає, зокрема, що інвестиції в навчання, освіту або підвищення рівня обізнаності щодо безпеки є частиною стратегій дій, оскільки вони стосуються людських ресурсів IT-безпеки. Інвестиції в ресурси IT-безпеки впливають на наслідки, відображені у Впливі 2. Наслідки включають вплив інвестицій на ресурси, які не є захищеними, процеси безпеки, продуктивність процесу безпеки та загальну ефективність організації. Впливи від 3 до 6 у межах наслідків взяті з точки зору ресурсів. Одно- і двоконтурні цикли навчання (ефекти 7 і 8) взяті з теорії організаційного навчання; вони представляють петлі зворотного зв'язку щодо наслідків для контрольних змінних і стратегій дій. Визначення та приклади впливів, представлені на рис. 4. Синтез знань про інвестиції в інформаційну безпеку базувався на новій теоретичній моделі інвестицій в інформаційну безпеку (див. рис. 4). Ця модель заснована на інтегральному застосуванні презентації на основі ресурсів та теорії організаційного навчання. Відповідь на поставлені дослідженням питання та усунення пов’язаних з цим прогалин має не лише академічне значення, а й управлінські наслідки.

Дане поєднання двох точок зору, а саме з точки зору представлення ресурсів і теорії організаційного навчання дозволить враховувати такі ефекти, як прогрес у навчанні, досягнутий внаслідок минулих помилок організації з часом, що гарантує, що організація перетворює «інформацію на цінні знання, що, у свою чергу, підвищує її здатність довготермінової адаптації». Таким чином, це дозволяє організації реагувати на середовище, що динамічно змінюється. Також Ресурсний погляд вступає в силу і охоплює основні фактори, які необхідно враховувати при прийнятті інвестиційних рішень, наприклад, макроекономічні, конкурентне та цільове середовище компанії. Перевага презентації на основі ресурсів полягає в тому, що вона теоретизує різні компоненти фірми, її оточення та взаємовідносини один з одним і, на відміну від організаційної теорії навчання, не зосереджується на організації та її компонентах в деталях.

Проте дана модель не дає можливості математично обрахувати застосування даної моделі на конкретному прикладі виробничої інфраструктури.

Медот може лежати в основі створеня моделі інвестування в кібербезпеку чи оцінку ризиків на рівні інвестицій в кібербезпеку. Опираюсь на поєднання теорії організаційного навчання та точки зору аналізу ресурсів це дасть змогу конкретній організації реагувати на середовище, що динамічно змінюється віднсно ресурсів та часу.

Висновок до першого розділу

Стандарти інформаційної безпеки — це загальноприйняті стандарти або рекомендації щодо конкретних дій чи результатів. З іншого боку, індивідуальні стандарти часто виготовляються та використовуються різними способами. Ці відмінності можуть вплинути на те, чи буде новий стандарт прийнятий швидко та легко, а отже, чи будуть альтернативи використані чи зникнуть. У результаті стандарти часто описуються унікальними характеристиками його розробки та передбачуваного застосування, такими як процес розробки стандарту, метод регулювання, застосовність стандарту для різних аудиторій і доступність стандарту для громадськості.

Запропоновано три концептуальні моделі формування ризику, кожна з яких має різне джерело (природу походження) невизначеності, що є необхідною передумовою для створення ризикової ситуації. Це дасть змогу

Управління ризиками інформаційної безпеки є серйозною проблемою для всіх підприємств. Результатом дослідження є рекомендація, яку можна розробити за допомогою стандартизованого підходу. Методика починається з систематичної системи визначення активів у процесі управління ризиками. Це дає чудові знання про те, що і чому слід захищати в конкретній організації. Аналіз загроз інформує корпорацію про небезпеки та виклики, з якими вона стикається в глобальних бізнес-процесах. Поєднання цих методологій дає повне розуміння впливу, який інформаційна безпека може мати на існуючі бізнес-операції. Крім того, аналіз

уразливості визначає, де і як може проявитися небезпека. Для визначення ймовірності загрози можна використовувати комбінацію виявлених уразливостей та відповідних процедур зменшення ризику. Після того, як ризик буде визнаний, фінансові показники можна використовувати для оцінки інвестицій, спрямованих на зниження ризику. Наразі не існує стандартної методології для оцінки фінансового ризику, пов'язаного з подіями безпеки, і рекомендується використовувати комбінацію індексів, об'єднаних або скоригованих для кожного окремого випадку, оскільки вартість засобів захисту може значно відрізнятися. Деякі включають витрати на апаратне забезпечення, програмне забезпечення та послуги, а інші включають внутрішні витрати, такі як непрямі накладні витрати та довгострокові наслідки для продуктивності. Кожен з індексів, обговорених у цій статті, ROI, NPV та IRR, має переваги, але їх самостійне використання не є відповідним підходом. В результаті поєднання цих методологій є найкращим способом оцінити необхідні інвестиції.

Представлено модель інвестування в інформаційну безпеку, засновану на двох усталених теоріях ІБ: уявлення на основі ресурсів і теорії організаційного навчання. Відповіді на питання, що виникають у результаті аналізу інтегрованої моделі інвестицій в інформаційну безпеку, можна отримати не тільки керувати майбутніми дослідженнями, але також мають управлінські наслідки, які допоможуть фірмам приймати інвестиційні рішення у сфері інформаційної безпеки

2 Методика оцінки Cy-VaR

2.1 Метрики оцінки безпеки

Планування інвестицій в інформаційну безпеку є десь між мистецтвом і наукою [20]. Щоб структурувати експозицію, виробнича функція безпеки високого рівня розбивається на два кроки: вартість безпеки зіставляється з рівнем безпеки, який потім зіставляється з перевагами. Це дозволяє структурувати джерела даних і показники, переосмислити поняття продуктивності безпеки та розрізняти джерела невизначеності, як помилку вимірювання та поведінку зловмисника. Рівень безпеки — це змінна в моделі, яка підсумовує якість захисту. Як і вартість безпеки, можна припустити, що вона втілена в детермінованому стані, хоча її ще важче виміряти. Причина в тому, що якість захисту не обов'язково є скалярним, а деяким дискретним станом, який має бути відображений (принаймні) в порядковому масштабі. Детерміновані показники включають рівень виправлення, наявність та конфігурацію систем виявлення вторгнень, чи встановлені антивірусні сканери на ПК кінцевих користувачів тощо. Незважаючи на те, що ці індикатори часто є грубими та гучними, ці індикатори передають певну інформацію про фактичний рівень безпеки. Таким чином, різні моделі процесів для якісної оцінки безпеки в організаціях можуть бути пов'язані з кількісними моделями інвестицій у безпеку. Крім того, рівень безпеки часто ми

можемо спостерігати за допомогою стохастичних індикаторів, де невизначеність відображає поведінку зловмисника. Прикладами для цієї категорії є типові заходи щодо інцидентів систем виявлення вторгнень та вірусних сканерів, наприклад, фактичні показники помилкової тривоги та пропущені показники виявлення. Можна зауважити, що наша декомпозиція виробничої функції безпеки корисна, якщо показники рівня безпеки (частково) спостерігаються. Оскільки, зокрема, змінні, що стосуються переваг моделей інвестицій у безпеку, важко виміряти та схильні до помилок, може бути дуже корисно включити допоміжний пункт для кількісної оцінки рівня безпеки. Таким чином, перший і другий кроки виробничої функції безпеки можна оцінити незалежно, перевірити на правдоподібність і порівняти з найкращими практиками галузі.

Відповідне зауваження стосується поняття продуктивності безпеки. Як показано на рис 2.1, продуктивність безпеки визначається кривизною функції, яка відображає вартість безпеки на рівень безпеки. Це відображає збільшення рівня безпеки на одиницю витрат на охорону, можливо, беручи до уваги зменшення граничної прибутку. Оскільки друга функція на стороні вигод є набагато більш специфічною для окремої організації (наприклад, через відмінності в активах, що піддаються ризику), наше визначення продуктивності безпеки має переваги при порівнянні ефективності витрат на безпеку між організаціями.

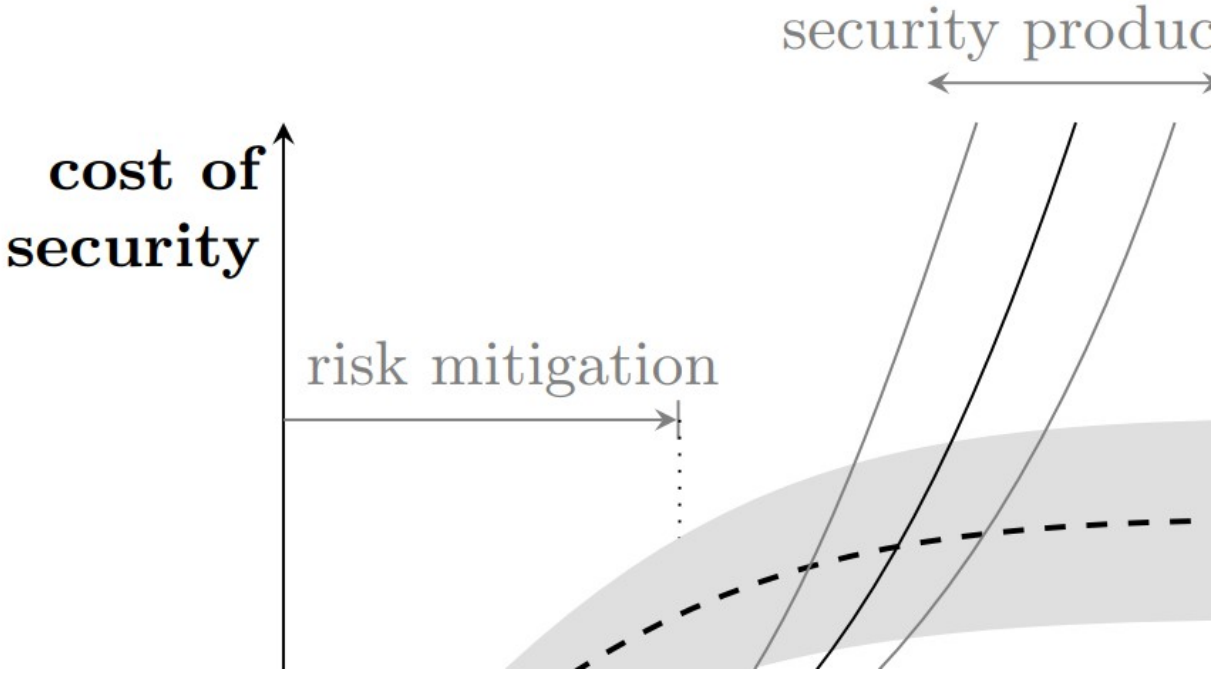

Рисунок 2.1. Декомпозиція виробничої функції безпеки на два кроки

Другий крок у виробничій функції безпеки пов’язаний із складністю відображення інцидентів із втратами. Точніше, рівень безпеки зіставляється з попередженими інцидентами, які потім можна перевести на користь безпеки. Менше інцидентів може бути пов’язано або з більшою кількістю атак, які не вдалися, або через меншу кількість атак [17]. Більшість технологій захисту впливає на перший фактор, але відмінності в продуктивності безпеки можна використовувати для балансування інвестицій. Це особливо актуально, якщо другий фактор (менша кількість атак) не є специфічним для організації, але впливає на інших.

Як зазначалося вище, вигода від безпеки значною мірою залежить від вартості активів, що піддаються ризику. Це відкриває банку черв’яків для оцінки нематеріальних інформаційних активів. Для стислості ми приділимо огляд цієї теми. Припустимо наразі, що відома вартість усіх активів, постраждалих від інциденту. Тоді ми можемо відрізнити ситуації, коли ця величина накладає верхню межу на збитки, від ситуацій, коли втрати можуть перевищувати вартість активів. Прикладами останнього є випадки зобов’язань або вторинних витрат на відшкодування активу. Ми використовуємо ширший термін витрат на

відшкодування, щоб підвести всі прямі та непрямі витрати, пов'язані з подією збитку. За своєю природою втрати і, отже, витрати на відновлення є випадковими величинами, які приймають додатні значення і часто концентрують масу ймовірності на нулі (у випадку, коли інциденту не відбувається). Ці випадкові величини можна підсумувати в скалярах (наприклад, за їх моментами), однак не без втрати інформації. Ми дотримуємося конвенції в теорії рішень і висловлюємо очікувані вигоди після перетворення за допомогою функції корисності, яка приймає як параметр неприйняття ризику особи, яка приймає рішення. Якщо передбачається, що організації нейтральні до ризику (це виправдано для бізнесу), функція корисності є функцією ідентифікації. Зайве говорити про те, що випадковий характер втрат ускладнює не тільки попередню перспективу інвестицій у безпеку (Які заходи ми маємо вжити?), але й оцінки ex-post (Чи ми вжили правильні заходи?). Те, що здається правильним чи неправильним в одному стані світу (тобто, реалізація випадкової змінної атаки), не обов'язково є однаковим в інших станах. Так чи інакше, становище менеджера з безпеки в організації завжди буде залежати від поєднання навичок та удачі. Принаймні з точки зору ex-ante, зовсім нещодавні дослідження вказують на те, що нечітка логіка може бути інструментом для боротьби з великим ступенем невизначеності у прийнятті рішень щодо безпеки. Однак поки ще рано говорити, чи ці концепції реалізуються на практиці і чи дають вони правильний тип сигналів, які можна інтерпретувати як на технічному, так і на управлінському рівні.

З визначеними трьома змінними, що представляють інтерес, залишаються відкритими питання, як виміряти або оцінити їх значення і як розрахувати важливі критерії прийняття рішень для конкретних інвестиційних рішень.

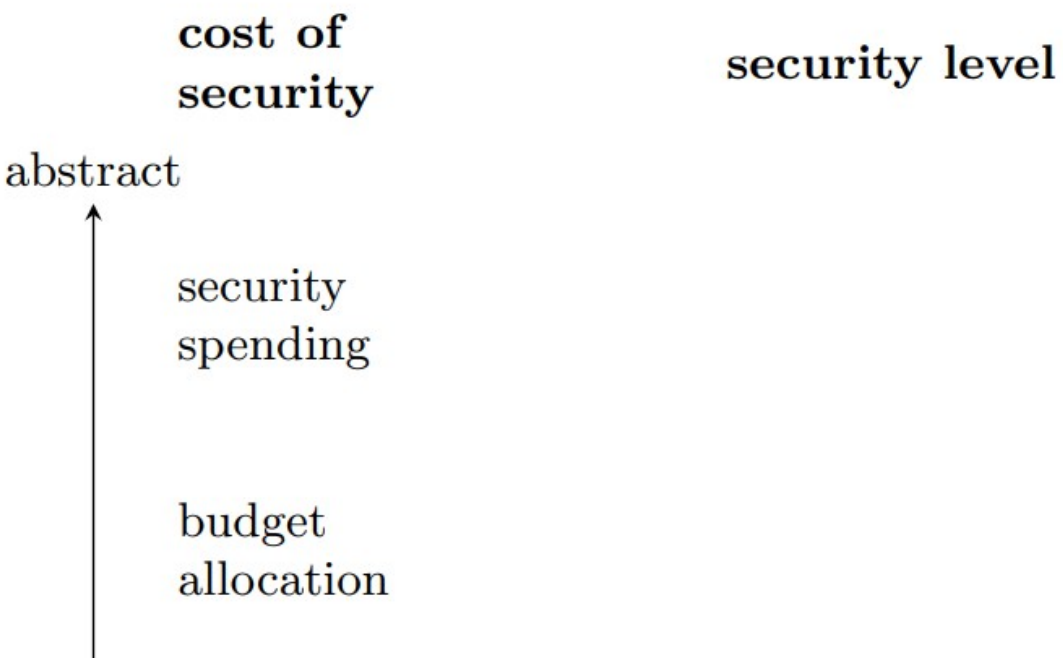

Рисунок 2.2. Показники інвестицій у безпеку, структуровані за рівнем абстракції; стрілки вказують на збільшення труднощів у вимірюванні

На рис. 2.2 показані різні індикатори інвестицій у безпеку з внутрішніх джерел та пов'язані з ними змінні в інвестиційній моделі. Показники, що відповідають вартості та користі безпеки, упорядковані по вертикалі за рівнем абстракції. Технічні показники рівня безпеки за своєю природою є конкретними та специфічними для використовуваної технології. Оскільки на цьому рівні відбувається перехід від принципово детермінованих станів до імовірнісних величин, ці показники зручно організувати вздовж цього виміру по горизонталі. З боку витрат, витрати на безпеку означають загальну суму бюджету організації на безпеку. Це показник інтересу для встановлення бюджету. Для даного бюджету наступним більш конкретним рівнем є визначення стратегії безпеки (\Куди інвестувати?"). Це передбачає розподіл бюджету на типові альтернативи в управлінні ризиками (пом’якшення, уникнення, передача, утримання) та на типи інвестицій у безпеку (проактивні проти реактивних, технічні чи організаційні тощо). Ще більш конкретна вартість заходів індивідуального захисту. Для багатьох показників цю вартість легко спостерігати (наприклад, за цінником).

Вимірювання витрат на безпеку на більш абстрактних рівнях стає дедалі складнішим, оскільки необхідно враховувати непрямі витрати, що виникають у результаті певних заходів і взаємодії між ними.

Ієрархія на стороні вигод приблизно симетрична до сторони витрат. Єдина відмінність полягає в тому, що збережені витрати на відшкодування та попереджені прямі втрати є випадковими величинами (або реалізацією в перспективі ex-post, якщо вони взагалі спостерігаються), тоді як очікувані вигоди відображають річну грошову вартість з поправкою на ризик.

Основна мета метрики - порівняти альтернативи. Хоча порівняння в часі або між організаційними підрозділами можна проводити з конкретними технічними показниками рівня безпеки, порівняння між заходами захисту або варіантами розподілу бюджету вимагають, щоб основні показники були в одному масштабі. Це пояснює, чому найбільш популярні показники в інвестиціях у безпеку розраховуються як співвідношення витрат і вигод на більш високому рівні абстракції. Протягом останнього десятиліття була проведена значна робота з адаптації принципів і метрик теорії інвестування для інвестицій у безпеку. Найбільш помітним є поняття рентабельності інвестицій (безпеки) (ROSI/ROI) [20]. Серед кількох варіантів ми віддаємо перевагу той, що нормується вартістю безпеки,

$$\text{ROSI} = \frac{benefit\ of\ cost - cost\ of\ security}{cost\ of\ security} \qquad (2.1)$$

Більш високі значення ROSI означають ефективніші інвестиції в безпеку. Зауважте, що поняття дохідності в ROSI є широким, оскільки запобігти збиткам не є прибутковістю у вузькому сенсі. Крім термінологічної суперечки, ці показники також скептично ставляться до практиків, які знайомі з проблемами збору статистичних даних для рідкісних подій. Тим не менш, ці показники, здається, залишаються необхідним компромісом для виправдання витрат на безпеку в організації. Звичайною практикою є прийняття (або обґрунтування) бюджетних рішень на основі стандартної теорії інвестицій, оскільки це полегшує порівняння між інвестиціями в різних сферах. Це так часто відзначали, що

найбільше щорічне опитування менеджерів із корпоративної інформаційної безпеки в США включає конкретне запитання. Згідно з цим, ROSI використовують 44% організацій-респондентів. Чиста теперішня вартість (NPV) і внутрішня норма прибутку|два інших стандартних інвестиційних індикатора, які дозволяють дисконтувати, але мають ті самі застереження|наступають 26% і 23% відповідно. Мабуть, менеджери з безпеки не мають вибору, ніж прийняти термінологію корпоративних фінансів.

2.2 Управління та передача кіберризиками

Компанії по всьому світу стикаються з кількома проблемами в управлінні впливом збільшення взаємозв'язку на їхній бізнес. Справді, кіберризик є фундаментальним компонентом загального ризику, на який звертаються організації, і очікується, що його значення зростатиме. За даними Allianz Global Corporate & Specialty (AGCS)[18], «кіберзлочинність зараз коштує світовій економіці понад 1 трлн доларів США — більше ніж один відсоток світового ВВП — на 50 % більше, ніж два роки тому. У той же час, загроза переривання бізнесу через атаки програмного забезпечення-вимагача, технічний збій або через ланцюжок поставок, серйозніші наслідки від злому даних і ризики, що виникають у зв'язку з прискоренням цифровізації після Covid-19, є великою. Спалах пандемії, перерви в бізнесі та кіберризики тісно взаємопов'язані, Екстремальні сценарії відносяться до найгірших подій, які можуть вразити бізнес. У сфері кіберризиків вони можуть мати дуже великий фінансовий вплив, і саме тому наукове співтовариство приділяє все більше уваги цьому питанню. Офіцери з ризиків сильно стурбовані можливістю надзвичайно поганого результату, який базується на квантилях міри ризику, такі як вартість під ризиком (VaR), що використовуються для оцінки суми грошей, необхідної для проведення таких подій. VaR був офіційно введений JP Morgan у 1995 році. Це показник ризику,

який повідомляє нам, за даного рівня впевненості, передбачувану втрату в найгіршому випадку за певний період часу. Нещодавно було виявлено потенційну корисність цієї міри ризику в кібер-сфері. На основі принципів VaR та в інтересах допомоги організаціям, які стикаються з проблемами кібербезпеки, ініціатива Всесвітнього економічного форуму «Партнерство для кібернебезпечності» запровадила модель для вимірювання та кількісної оцінки впливу кіберзагроз на бізнес та ризику їх. Ця модель, яка є відомою як cyber value-at-risk (Cy-VaR), пропонує відправну точку для кількісної оцінки ризику та намагається внести більше дисципліни в цю сферу, навіть якщо вона потребує подальших удосконалень та тестування в цій галузі. Зокрема, обговорюється потенційне використання цього показника ризику для підтримки інвестиційних рішень, а також пропонуються нові показники ризику, які базуються на Cy-VaR. Наша ідея ґрунтується на тому, що ефективний процес управління ризиками має враховувати екстремальні випадки, коли кіберінцидент є досить серйозним, щоб спричинити великі збитки. Таким чином, інструменти та показники, що підтримують інвестиційні рішення, повинні спиратися не лише на традиційну очікувану вартість, а й на несподівані втрати, беручи до уваги небажані події рентабельності інвестицій у безпеку (ROSI) на основі класичної рентабельності інвестицій (ROI). Іншим показником, який використовується в теорії інвестицій для оцінки інвестицій, є чиста приведена вартість (NPV), а в рамках інформаційних технологій пропонується більш складний розрахунок NPV.

Управління ризиками дозволяє системі впоратися з наслідками невизначеності на ділову активність. Відповідно до міжнародних стандартів (ISO, BS7799), метою управління ризиками є створення та захист вартості. З цією метою він покращує ефективність організації, заохочуючи до інновацій та підтримуючи досягнення поставлених цілей. Для того, щоб процес управління ризиками був ефективним, необхідно враховувати деякі фундаментальні принципи. Завдання управління ризиками повинні бути пропорційними рівню ризику, з яким справляється організація, відповідно до інших видів діяльності в організації, і вони повинні бути комплексними та вбудованими в організацію.

Нарешті, вони повинні бути активними та реагувати на майбутні та мінливі ризики. Серед ризиків, з якими стикається підприємницька діяльність, операційні ризики випливають із зовнішніх подій або поганих і неплідних внутрішніх систем, людей і процесів. Кіберризики належать до категорії операційних ризиків, навіть якщо вони мають особливі характеристики. У зв'язку з цим добре відомо, що середовище кіберризиків постійно розвивається через нові технології та швидкий розвиток комп'ютерних інформаційних систем. Техніки атаки постійно змінюються, і їх можна виконувати легко і дешево. Кібер-ризики продовжують розвиватися, і підприємства вирішують все більшу кількість нових проблем, які включають більші та дорожчі зломи даних, зростання кількості випадків компрометації (спуфінгу) ділової електронної пошти з програмним забезпеченням-вимагачем, а також можливість судового розгляду після події. Як наслідок, багато компаній усвідомлюють, що кіберризики є ключовим компонентом управління ризиками підприємства (ERM), і їхня головна мета — посилити стійкість до кібер; тобто «здатність систем і організацій протистояти кіберподіям, що вимірюється комбінацією середнього часу до відмови та середнього часу до відновлення»

Управління ризиками безпеки включає виявлення, оцінку та лікування ризиків, пов'язаних із цілісністю, доступністю та конфіденційністю активів організації, усвідомлюючи, що залишковий ризик необхідно прийняти. Справді, прийняття найкращих процедур кібербезпеки та встановлення різних контрзаходів не гарантують уникнення кіберінцидентів, незважаючи на їх неабияку вартість. Прийняття залишкового ризику є частиною кіберзахисту разом із спробою керувати ним з метою бути стійким. Альтернативи мінімізації ризику включають зменшення ризику, передачу, уникнення та прийняття. Пом'якшення ризику стосується зусиль, спрямованих на його зменшення (тобто, зменшення ймовірності ризикованої події, її впливу або того й іншого). Передача ризику означає розподіл тягаря потенційних збитків з іншою стороною: страхування є можливим варіантом передачі ризику. Уникнення ризику передбачає рішення уникнути ризикованої події (наприклад, відмовитися від ризикованої частини

бізнесу), а прийняття ризику – це спосіб прийняти ризик як вартість ведення бізнесу. Це рішення має сенс, коли вартість інвестування або страхування від нього має перевищувати загальні втрати з часом.

Як відомо, ризик — це можливість зазнати шкоди або втрати. Це пов’язано з можливістю інциденту в залежності від майбутніх загроз і вразливостей. Кіберзагрози можуть спровокувати небажані результати, що випливають із шкоди системі чи організації. Вони можуть бути зовнішніми або внутрішніми, і можуть бути викликані окремими особами або організаціями. Кіберуразливості – це наявні недоліки або слабкі місця, які можна використати і призвести до інциденту. Втрати є наслідками інцидентів і називаються «впливом». Вони можуть бути матеріальними (наприклад, фінансові санкції або втрата доходу) або нематеріальними (втрата репутації), згідно з ураженими активами. Таким чином, ризик можна визначити як поєднання загрози, вразливості та впливу. Менеджери повинні приймати обґрунтовані рішення щодо толерантності до ділових ризиків і, як наслідок, вони повинні планувати інвестиції в кібербезпеку та інші стратегії пом'якшення чи передачі. Вони повинні оцінити ймовірність зазнати шкоди. Більше того, вони повинні вимірювати ефективність дій зі зменшення ризику, оцінюючи будь-яке зниження ризику в результаті деяких інвестиційних витрат.

Окрім зменшення ризиків та уникнення ризиків, фінансовий ризик інцидентів із безпекою може бути переданий третім сторонам, зокрема кіберстрахувальникам. Якщо премія нижча, ніж різниця між вигодою та вартістю безпеки, це вигідний варіант інвестування. Зауважте, що якщо страховий ринок знаходиться в рівновазі, це справедливо лише в тому випадку, якщо організації або не схильні до ризику, або краще поінформовані про свій конкретний ризик, ніж страховик. Проте на практиці ринок кіберстрахування виглядає недостатньо розвиненим, імовірно, через три перешкоди, що характеризують кіберризик: взаємозалежну безпеку, корельований ризик та інформаційну асиметрію. Якщо ця ситуація зміниться в майбутньому, страховики, швидше за все, вимагатимуть, щоб були вжиті заходи захисту від усіх відомих загроз. Тому кіберстрахування скоріше слід розглядати як доповнення до інвестування у заходи захисту або

передані сторонні операції безпеки, а не як заміну. Для забезпечення підтримки визначеного рівня безпеки страховики можуть співпрацювати з постачальниками послуг безпеки та радити своїм клієнтам передавати їм операції з безпеки (див. мал. 2.3). Аутсорсинг, який можна вважати як заміна кіберстрахування, є кращим перед кіберстрахуванням. Однак у цій моделі постачальники послуг безпеки беруть на себе повну відповідальність за потенційні збитки. Нам невідомо жодного постачальника, який би це запропонував на практиці. Тому ефективно цей результат слід інтерпретувати як поєднання аутсорсингу безпеки та кіберстрахування. Таке поєднання фактично обіцяє кращі результати, ніж лише кіберстрахування.

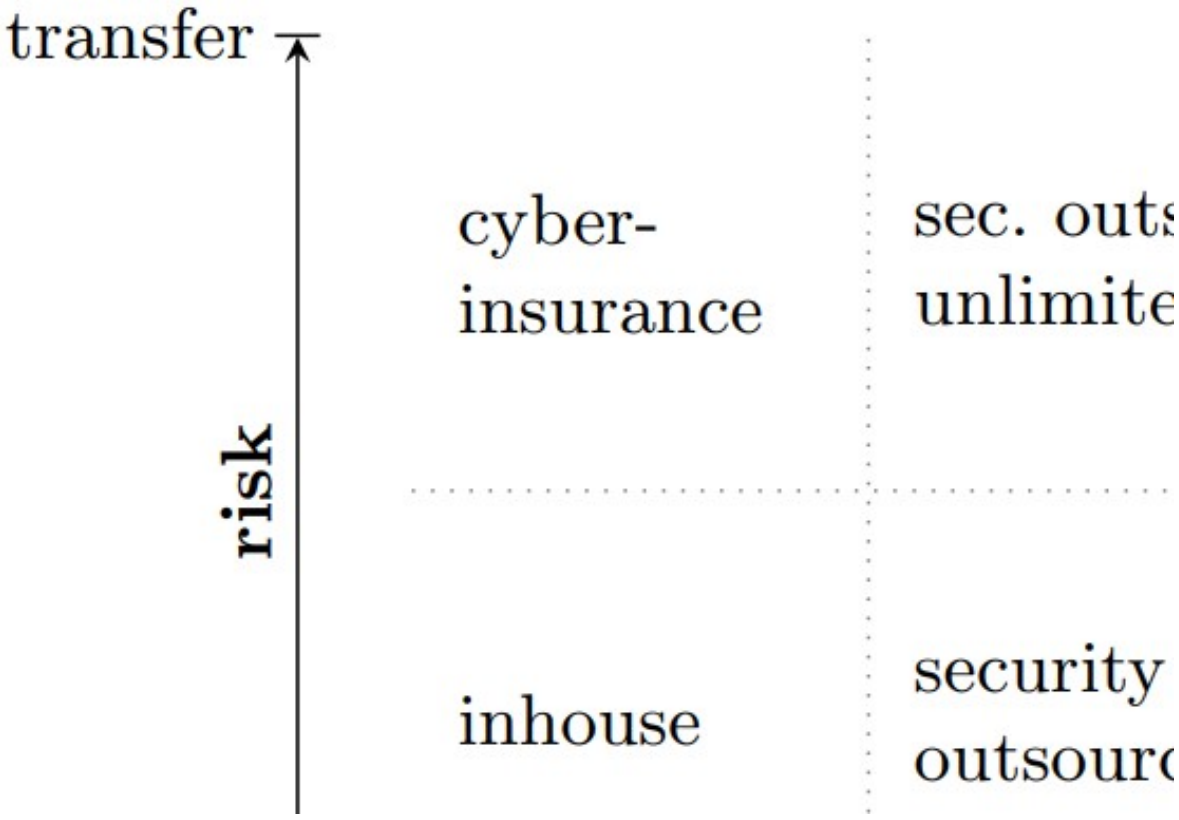

Рисунок 2.3. Ортогональне співвідношення передачі кіберризиків та аутсорсингу операцій з безпеки

2.3 Роль кіберцінності під загрозою

Відповідно до вищезазначених питань, в останні роки VaR почали впроваджувати в контексті кібербезпеки, і було зроблено багато зусиль, щоб адаптувати цей захід ризику до методів, спеціально розроблених для оцінки кіберризиків. Ці нові моделі, які називаються Cy-VaR, пропонують «вищому керівництву з єдиним номером ризику та статистичною ймовірністю зрозуміти загальний ризик кібербезпеки підприємства». Cy-VaR має дві основні цілі: «допомогти фахівцям з ризиків та інформаційної безпеки сформулювати кіберризики у фінансовому плані» і «дозволити керівникам бізнесу приймати ефективні рішення та досягати балансу між захистом організації та веденням бізнесу».

Cy-VaR заснований на концепції VaR, яка є мірою ризику, запропонованою JP Morgan у 1995 році як «передбачувана втрата в найгіршому випадку на певному рівні довіри». VaR вважається основним заходом ризику. Він дуже популярний, оскільки він інтуїтивно зрозумілий, а його числові значення легше інтерпретувати, порівняно з іншими показниками ризику. Більше того, про це зазначають регулятори в угодах Базель II та Базель III.

VaR при фіксованому рівні довіри a є [0, 1] визначається як найменше число l, таке, що ймовірність того, що втрата L перевищить l, не перевищує ($1 - a$):

$$\mathrm{VaR}_a(\mathrm{L}) = \inf[l \in R | P(L > l) \leq 1 - | a] \qquad (2.2)$$

$\mathrm{VaR}_a(L)$ – це a-квантиль q_a функції розподілу втрат L. У фінансовому та актуарному контексті традиційними значеннями для а є a = 0,95, a = 0,99 і a = 0,995. Кілька організацій використовуються для оцінки VaR як компонента їхньої корпоративної оцінки ризиків, у той час як лише небагато організацій використовують VaR для кіберризиків. Раніше цими ризиками керували просто уникаючи атак або швидке відновлення. Тим не менш, технічні огляди засобів контролю безпеки не можуть допомогти кількісно оцінити економічний вплив кібератак. Менеджери повинні кількісно оцінити кіберризики, спланувати розмір інвестицій у безпеку та оцінити подальше зниження ризиків. Більше того, вони повинні вирішити питання про можливість розподілу залишкового ризику з

третьою стороною, наприклад, страховою компанією. Обґрунтування моделей цінності під ризиком, що застосовуються до кібер-доменів, допомагає вирішити ці проблеми.

Справді, Cy-VaR дозволяє досліджувати наслідки додаткових загроз і порівнювати, як різні конфігурації контролю безпеки можуть допомогти обмежити залишковий ризик у міру зростання загрози. Підхід розподілу збитків є найвідомішим підходом до вимірювання операційного ризику та розрахунку регулятивного капіталу. В актуарній сфері це дуже популярний статистичний підхід, і він спирається на концепцію, що втрати можуть виникати випадково за частотою та серйозністю відповідно до характерних розподілів. Зокрема, частота та тяжкість втрат незалежно від кожного залежать від статистичного розподілу, а параметри оцінюються безпосередньо з даних. Розглянемо загальну суму L всіх втрат, що виникають за певний період часу; тобто сукупні втрати,

$$L = \sum_{j=0}^{N} X_j, \;\; N = 0,1,2, \ldots \qquad (2.3)$$

де X_j ($J = 1, \ldots, N$) — суми одиничних втрат. $L = 0$, коли $N = 0$. Обидва кількість N окремих подій; тобто частота атак у розглянутий період часу та відповідні індивідуальні суми втрат $X_1, \ldots, X_N$, які представляють серйозність пошкодження для кожної атаки, є випадковими величинами. Щоб отримати складний розподіл L, частота та серйозність цих втрат моделюються окремо.

На рівні Cy-VaR схема повинна передбачати сценарії, де присутні більше однієї загрози. Нарешті, і в довгостроковій перспективі, схема повинна охоплювати різні страхові продукти і пов’язувати їх з організаціями, щоб спочатку обґрунтувати системний ризик. Системний ризик виникає, коли катастрофічні події стосуються кількох організацій одночасно. Охоплюючи страхові продукти та пов’язуючи їх з організаціями з конкретними активами, схема дозволяє нам розглянути сценарії, коли одна і та ж політика запускається в кількох організаціях протягом короткого періоду часу. вхідними є файли даних, які відповідають схемі, а результатом є розподіл Cy-VaR, який розраховується за допомогою моделювання Монте-Карло.

2.4 Критичні питання оцінки кібер-цінності під час ризику

Підхід до аналізу ризиків ґрунтується на припущенні, що структура, організація та середовище організації ІС та тип інформації, що обробляється, дуже неоднорідні [6]. З цієї причини кожна фірма має дуже різні вимоги до безпеки. Інформація має зовсім інші потреби в захисті, які не можуть бути задоволені стандартними засобами керування. З цієї причини необхідність запобіжних заходів має бути визначена шляхом детального аналізу ризиків. Підхід до аналізу ризиків враховує як вразливі місця, так і загрози. Якщо обидва поєднуються, виникає ризик. Крім того, він враховує наслідки ризику (тобто втрати, шкоди) на активах фірми. Основна структура аналізу ризиків полягає в тому, щоб вибрати частини архітектури (технічні чи організаційні), які слід оцінити, потім проаналізувати потреби в захисті, проаналізувати загрози, вразливості та вплив на бізнес, а потім визначити відповідні контрзаходи. Для низьких потреб у захисті аналіз ризику часто поєднується з базовим підходом або аналізом уразливості. Методи аналізу ризиків розрізняються в основному за такими аспектами: підхід до структури проблеми, метод вимірювання та визначення впливу. Для структурування проблеми часто застосовуються методи моделювання або сценарного аналізу. Розмір ризику зазвичай розраховується шляхом множення ймовірності та збитку для обчислення очікуваних збитків. Для спрощення обчислень часто використовується порядкова або напівметрична шкала. Модель збитків є життєво важливою для порівняння ризиків і втрат – на диво, немає загальноприйнятої моделі для розрахунку збитків. Різні моделі варіюються від повністю підзвітних результатів (наприклад, модель втрат Базель II) до охоплення підходів, що включають втрату репутації, тимчасове падіння частки та інші якісні змінні. Метою методики має бути максимальна об'єктивність і довготривала достовірність результатів. Історичні дані є передумовою для знань експертів, які переважно базуються на проекції історичного сприйняття ризику та

досвіду на майбутнє. Проблема полягає в тому, що розпізнається лише невеликий відсоток усіх спроб порушення безпеки. Одним із завдань офіцерів безпеки є покращення якості даних шляхом покращення методів і політики ідентифікації. Ще один момент – це потреба в даних методів і потреба в інформації різних зацікавлених сторін. Наприклад, бізнес-одиниці абсолютно не потребують кількості спроб порушення безпеки. Для кількісної оцінки впливу простою сервера на бізнес, Переваги і недоліки полягають у аналізі ризиків, що є єдиним методом планування безпеки, який враховує вразливості, загрози та вплив на бізнес для оцінки ризиків безпеки. Однак існує велика різноманітність методологій для аналізу ризиків. Багато з них або орієнтовані на бізнес, або на технології. Більшість із них вимагають великої кількості аналітиків ризиків, оскільки вони не дають порад щодо виконання аналізу ризику, наприклад, визначення втрат, відокремлення відповідних частин архітектури ІС тощо. модель планування безпеки із засобами ліквідації збиткових засобів контролю. Тому що корпоративна оцінка ризиків безпеки часто не проводиться, дуже важко констатувати покращення безпеки після реалізації інвестицій у безпеку

Щоб отримати достовірну оцінку Cy-VaR, необхідно враховувати вразливість, активи та профіль потенційних зловмисників (див. Рисунок1). За даними Агентства Європейського Союзу з кібербезпеки (ENISA), вразливість пов’язана з появою недоліку, дизайну або помилки впровадження, яка може спричинити несподівану подію, яка впливає на безпеку інформаційної системи. Небажана подія може бути певною або невизначеною, і вона може бути викликана одним або серією подій. Користувачі можуть бути значним джерелом уразливостей; справді, навмисно чи ні, багато співробітників часто є слабкою ланкою успішної кібератаки (наприклад, випадкова публікація конфіденційної інформації, відсутність зберігання портативних комп’ютерів, що містять дуже конфіденційну інформацію). Крім того, оцінка вразливості організації залежить від її попередньої здатності протидіяти успішним атакам і від рівня зрілості її системи безпеки. Відсутність стандартних налаштувань зрілості в різних галузях зменшує ефективність кібернетичної цінності під ризиком. Справді, наслідком

може бути суб’єктивна, а не об’єктивна кількісна оцінка загрози. Пропонує ться кілька звітів про досвід і деякі тематичні дослідження щодо рейтингу зрілості інформаційної безпеки, пропонуючи всебічний огляд та підсумок цієї сфери, що розвивається.

Ще одним основним елементом моделей Cy-VaR є ідентифікація матеріальних і нематеріальних активів, які знаходяться під загрозою. Зокрема, нематеріальні активи (тобто людський капітал, репутація, знання, досвід тощо), які становлять до 80% вартості організації, тепер визнані важливими для надання компанії та нації. Після ідентифікації активи повинні бути оцінені, а це завдання щодо нематеріальних активів може бути досить складним. Останнім кроком є класифікація активів на окремі категорії, які полегшують визначення загального ризику безпеки. Ми помічаємо, що оцінити економічні та фінансові наслідки кіберінциденту важко через особливий характер інформаційних активів.

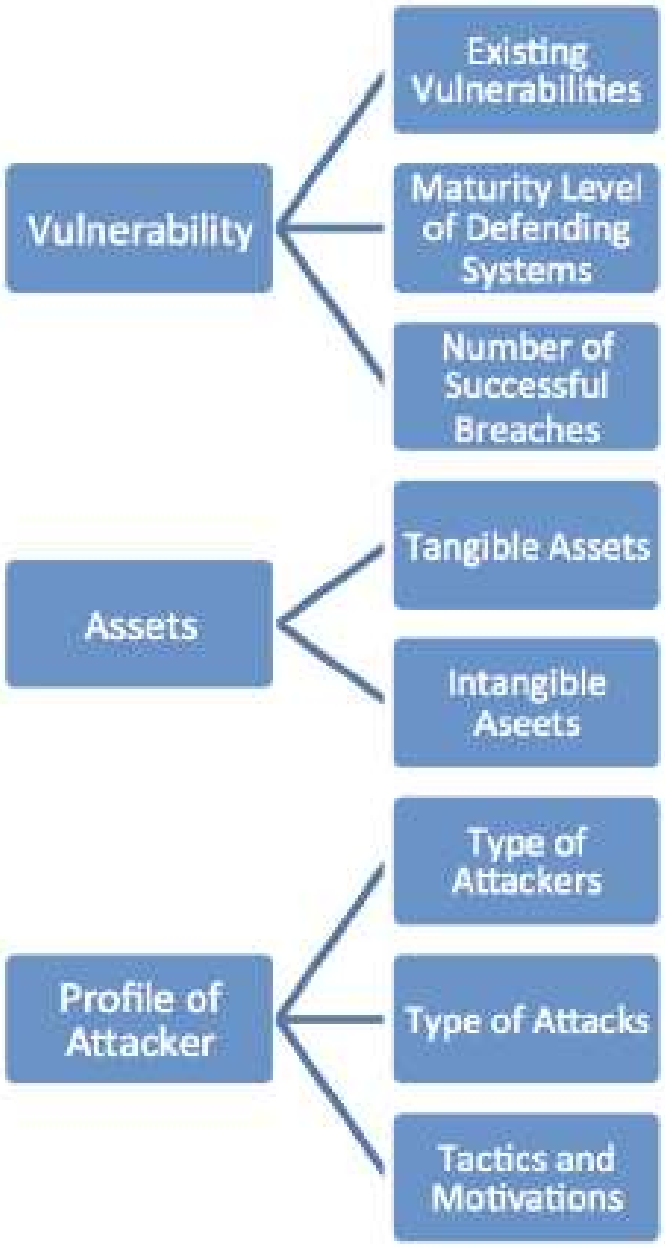

Рисунок 2.4. Компоненти ризику кібер-цінності.

Третій елемент — це профіль потенційних зловмисників (див. рис. 8), тобто тип зловмисників, їх мотивація та тип атаки, до якої вони схильні. За типом зловмисників можна виділити чотири типи: кіберзлочинці, хактивісти, спонсоровані державою зловмисники та інсайдерські загрози. Кіберзлочинці здійснюють кіберзлочини з метою отримання прибутку шляхом крадіжки конфіденційної інформації компанії або особистих даних. На сьогоднішній день

вони є найбільш провідним і найактивнішим типом нападників. Хактивісти - це окремі особи або групи хакерів, які діють на основі релігійних переконань або соціальної та політичної ідеології. Зловмисники, спонсоровані державою, мають особливі цілі, які відповідають основним інтересам їхньої країни. Нарешті, інсайдерські загрози надходять як від штатних, так і від тимчасових працівників, а також від клієнтів і підрядників. Погрози можуть бути мотивовані зловмисною, випадковою або недбалою поведінкою. У своїй доповіді за 2019 рік Всесвітній економічний форум WEF перерахував найпоширеніші кібератаки. з якими може зіткнутися окрема особа чи організація. Серед іншого ми знаходимо атаку грубої сили, за допомогою якої зловмисники використовують метод проб і помилок, щоб успішно вгадувати паролі, наповнення облікових даних, яке використовується для вкрадених облікових даних для доступу до облікового запису користувача. Одним із найпоширеніших видів кібератак є фішинг, який полягає у надсиланні електронних листів із джерела, що здається довірою, для отримання особистої інформації. Нарешті, ми згадуємо зловмисне програмне забезпечення, яке є шкідливим програмним забезпеченням, завантаженим в систему без будь-яких видимих ознак.

Основна мета ефективної боротьби з кібератаками сильно залежить від оцінки ймовірності успішної атаки. Дійсно, швидкість появи дійсно важко оцінити, оскільки зловмисники адаптуються, а зміни в їхніх стратегіях непередбачувані. Щодо оцінки ймовірності успішної атаки, то це теж непросте завдання. Причина в тому, що не вистачає історичних даних про частоту та тяжкість атак. Однією з причин можуть бути перешкоди обміну інформацією, пов'язані з тим, що компанії не хочуть розголошувати кіберінциденти, яким вони зазнали, оскільки це може завдати величезної вторинної шкоди. Ситуація змінюється і в Європі через GDPR (загальний Регламент захисту даних, введений у травні 2018 року. GDPR передбачає суворіші правила, такі як вимога сповістити регулятора та власника даних про порушення даних. Для компаній, які не виконають вимоги, запроваджуються високі штрафи: вони можуть бути оштрафовані на стільки ж як 4% світових доходів. Оцінюючи Cy-VaR, ми не

можемо ігнорувати, що рівень безпеки однієї системи може залежати від безпеки інших. Як наслідок, зловмисник потенційно може використовувати систему через канал, яким організація ділиться з партнером із набагато нижчим рівнем безпеки. Крім того, щоб оцінити ризик за допомогою Cy-VaR, важливо враховувати залежності між трьома компонентами (уразливість, активи та профіль зловмисника). Наприклад, вразливість системи в основному залежить від її актуальності активів потенційних зловмисників і загальна поведінка в спільноті зловмисників. Таким чином, ризик зазнати кібератаки тісно пов'язаний з активами компанії та профілем зловмисника. Підхід до боротьби з відсутністю достовірних даних стосується методів експертного оцінювання.

2.4 Кіберцінність під ризиком при оцінці інвестицій в інформаційну безпеку

Важке завдання для компаній – визначити, скільки ресурсів інвестувати в різні бізнес-проекти [21]. Труднощі є особливо великими, якщо ці проекти, замість того, щоб принести негайну економічну віддачу, мають своєю основною метою запобігання майбутніх втрат. Інвестиції в кібербезпеку мають саме цю особливість. Кожен євро, чи гривня інвестовані, щоб зробити ваші бізнес-мережі та пристрої безпечнішими, не призводить до негайного виграшу для компаній, а без відповідних показників інвестицій у безпеку керівництву важко приймати будь-які інвестиційні рішення. Звичайно, значне зниження кіберризиків може бути амбітною метою, яка стикається з обмеженнями витрат і бюджету. Отже, необхідно визначити «оптимальний» рівень ризику, нижче якого вартість інвестиції перевищать вигоди від зниження ризику. Традиційний компроміс між ризиком і прибутковістю, характерний для фінансових інвестицій, поступається місцем компромісу між ризиком і меншими витратами. Як відомо, рівень ризику можна визначити як добуток очікуваної ймовірності та очікуваної тяжкості неприємної події. Мета інвестування в IT-безпеку полягає в тому, щоб знизити

ймовірність інцидентів або зменшити потенційні втрати від небажаної події, або і те, і інше. Важливо оцінити вплив певного заходу безпеки на ці параметри. Багато внесків у літературі пропонують адаптувати показники теорії інвестицій до оцінки інвестицій у безпеку. Найбільш популярним є поняття рентабельності інвестицій у безпеку (ROSI), що спирається на класичну рентабельність інвестицій (ROI). ROI — це показник ефективності, який оцінює ефективність інвестицій або порівнює результат різних інвестицій. Він вимірює прибуток або збиток, отриманий від інвестування певної суми грошей. ROI — це відсоток або коефіцієнт, який розраховується шляхом ділення вигоди (прибутку) від інвестиції на її вартість. Як адаптацію рентабельності інвестицій до оцінки інвестицій у безпеку, ROSI визначається наступним чином (Enisa 2012):

$$ROSI = \frac{\Delta L - l_0}{l_0} \tag{2.4}$$

де ΔL – це зменшення втрат, отримане від інвестиції з початковою вартістю I_0 і представляє вигоду від інвестицій. Дійсно, рівняння (2) можна переписати в термінах очікуваних сукупних втрат *E[L]* наступним чином:

$$ROSI = \frac{\Delta E[L] - l_0}{l_0} \tag{2.5}$$

з $\Delta E[L] = E[L_t]$ - $mE[L]$. Скорочення втрат $\Delta E\ [L]$ вимірюється в термінах очікуваних сукупних втрат *E[L]* за певний період, як *L* визначено в рівнянні (1). *mE[L]* – це очікувана тривалість пом'якшення втрат у результаті інвестування в безпеку. Інвестиція вважається прибутковою, якщо ефект зменшення ризику перевищує очікувані витрати. У багатьох матеріалах про кібербезпеку очікувані втрати часто називають очікуваною тривалістю річних втрат (ALE), яка визначається як добуток очікуваної тривалості одноразових втрат (SLE), помножений на річну частоту виникнення (ARO). Посилаючись на одну небажану подію, SLE – це очікувані збитки через ризик. ARO — це міра ймовірності виникнення ризику, що еквівалентна кількості подій такого типу за звітний період. Ефективні інвестиції знижують ALE, а зменшення втрат визначається кількісно різницею ALE без інвестицій та пом'якшеним ALE. Відповідно до тенденції запозичувати показники оцінки інвестицій у фінансовий [21] автор

пропонує більш складний розрахунок чистої приведеної вартості (NPV). Як відомо, NPV визначається теперішньою вартістю різниці майбутніх надходжень та відтоків, де ставка дисконтування є альтернативною вартістю

капітал. Ця ставка дисконтування є екзогенною, оскільки є мірою, отриманою з середовища інвестицій. Модифікована NPV:

$$\mathrm{NPV}_0 = -l_0 + \sum_{t=1}^{T} \frac{\Delta E[L_t] + \Delta C_t * i_{ROE,t}}{(1+i)^t} \quad (2.6)$$

де l_0 є початковими інвестиціями, $\Delta E[L_t]$ вимірює зменшення річного очікуваного збитку як вигоду від інвестицій, а ΔC_t включає зменшення витрат капіталу як позитивний ефект від інвестування в безпеку, при цьому $i_{ROE,t}$ є цільовою прибутковістю. на власний капітал, встановлений організацією. Ставка дисконтування і є безризиковою ставкою. Цей підхід підходить для багатоперіодних інвестицій і враховує перевагу часу. Може бути важко визначити витрати на IT-безпеку. Причина полягає в необхідності оцінити як прямі витрати (наприклад, установка, технічне обслуговування, навчання), так і непрямі витрати (наприклад, через зміни в мотивації співробітників або зміни робочих процесів). Іншим важливим питанням є оцінка ефектів пом'якшення інвестицій в безпеці. Ефективний процес управління кіберризиками повинен враховувати, що деякі екстремальні випадки можуть спричинити величезні збитки. Спостереження, які спочатку здаються винятковими, насправді не можуть бути неузгодженими з рештою даних, якщо вони належать до довгохвостого розподілу. Тому інструменти та метрики, що підтримують інвестиційні рішення, також повинні покладатися на несподівані втрати, беручи до уваги небажані хвостові події.

Такий підхід може допомогти прийняти відповідні інвестиційні рішення на основі особистих уподобань щодо ризику замість того, щоб вибирати рішення, які розглядають лише очікуване зменшення збитків. З огляду на це, цей внесок має на меті відобразити, що Cy-VaR може надати додаткову інформацію в процесі прийняття рішень щодо інвестицій у безпеку.

З цією метою ми пропонуємо ROSI з поправкою на ризик (RaROSI), яка враховує найгірші випадки. Ідея полягає в тому, щоб розглянути різницю між очікуваною втратою без ефекту пом’якшення інвестицій *E[L]* та втратою в

найгіршому випадку за даного рівня довіри *a*, пом'якшеної інвестиціями:

$$RaROSI = \frac{\Delta U[L] - l_0}{l_0} \quad (2.7)$$

де $\Delta U[L] = E[L]$ - mCyVaR(a*)* з mCyVaR(a), що є пом'якшеним значенням очікуваної втрати в найгіршому випадку при заданому рівні довіри a. Цей параметр відображає ступінь неприйняття ризику особи, яка приймає рішення; у міру зростання рівня довіри зростає і Cy-VaR. RaROSI може доповнювати та збагачувати інформацію, надану ROSI, включаючи показник кіберризику, виражений Cy-VaR.

Що стосується формули NPV (Рівняння (6)), ми можемо помітити, що у фінансовому контексті VaR також називають капіталом під ризиком (CaR); тобто сума капіталу, яка зазнає будь-яких несподіваних втрат. З цієї точки зору, ми вважаємо, що зменшення нарахування капіталу ΔC_t в (5) можна виміряти в термінах Cy-VaR.

Інші показники ризику фінансової та банківської сфери можуть бути використані в кіберсфері. Зокрема, ми маємо на увазі показники ефективності з поправкою на ризик (RAPMs). RAPM – це коефіцієнт прибутковості ризику, який можна оцінити попередньо, враховуючи очікувані прибутки та поточну величину ризику. Це також може бути перевірено ex post, як частка між фактично отриманим прибутком і VaR, фактично зафіксованим протягом певного періоду.

Серед цих показників ризику ми знаходимо рентабельність капіталу з поправкою на ризик (RAROC), яка вперше була застосована на початку 1990-х років. RAROC – це змінений показник рентабельності інвестицій, який враховує елементи ризику. Це дозволяє налаштувати чисельник і знаменник рентабельності інвестицій на основі ризику:

$$RAROC = \frac{E(u) + i * VaR(a)}{VaR(a)} \quad (2.8)$$

з *E[u],* що вказує очікуваний прибуток. У чисельнику (7) ми маємо суму очікуваного прибутку та прибутку, отриманого від інвестицій за безризиковою ставкою виділеного капіталу (VaR) у разі несподіваних збитків.

Застосовуючи цей захід ризику до інвестицій у кібербезпеку, ми можемо

записати:

$$CyRAROC = \frac{\Delta E[L] - l_0 + i * CyVaR(a)}{CyVaR(a)} \quad (2.9)$$

з *E(u) = ΔE[L]* - l_0, як визначено у формулі ROSI. Отже, очікуваний прибуток вимірюється через очікуване скорочення збитків *ΔE[L]* за вирахуванням інвестиційних витрат l_0.

Висновок до 2 розділу

У даному розділі було проаналізовано вибір метрик у безпеку. Основна мета метрики - порівняти альтернативи. Хоча порівняння в часі або між організаційними підрозділами можна проводити з конкретними технічними показниками рівня безпеки, порівняння між заходами захисту або варіантами розподілу бюджету вимагають, щоб основні показники були в одному масштабі. Також було проаналізовано методику ролі кібер-цінності ризику.

Апробація оцінки ризиків на основі Cy-Var

3.1 Моделювання Монте-Карло

Підхід розподілу збитків є найвідомішим підходом до вимірювання операційного ризику та розрахунку регулятивного капіталу [22]. Щоб обчислити Cy-VaR активу, важливо визначити основні показники або змінні, які впливають на вартість цього активу. Наприклад, у фінансах показники для оцінки коливань вартості портфеля визначаються шляхом декомпозиції портфеля на простіші поняття, для яких встановлюються основні фактори ринкового ризику. Після ідентифікації наборів даних для обчислення Cy-VaR, необхідно спиратися на методи моделювання. Яскравим прикладом розрахунку є метод моделювання Монте-Карло. Моделювання Монте-Карло подібне до історичного моделювання, з тією різницею, що створені сценарії засновані на розподілах історичних даних, а не на розрахунках значення на основі змін, що спостерігаються для кожної окремої точки даних протягом періоду. У сфері фінансів фактори ризику ринкових змін добре встановлені і є відповідні історичні дані. Тому зусилля були зосереджені на покращенні статистичного розуміння історичних даних та визначенні методів, які найкраще фіксують зміни. Незважаючи на те, що дані збираються з експоненційною швидкістю з точки зору обсягу, різноманітності та швидкості, традиційно оцінки ризиків кібербезпеки враховують лише типи кібератак та мотиви зловмисників (Всесвітній економічний форум і Deloitte, 2015).

Загрози можна моделювати на основі їх ймовірності, конкретних активів, на які вони спрямовані, та наявності суб’єктів загрози з різним потенціалом заподіяння шкоди. На рівні Cy-VaR схема повинна передбачати сценарії, де присутні більше однієї загрози. Нарешті, і в довгостроковій перспективі, схема повинна охоплювати різні страхові продукти і пов’язувати їх з організаціями, щоб

спочатку обґрунтувати системний ризик. Системний ризик виникає, коли катастрофічні події стосуються кількох організацій одночасно. Охоплюючи страхові продукти та пов'язуючи їх з організаціями з конкретними активами, схема дозволяє нам розглянути сценарії, коли одна і та ж політика запускається в кількох організаціях протягом короткого періоду часу. Вхідними є файли даних, які відповідають схемі, а результатом є розподіл Cy-VaR, який розраховується за допомогою моделювання Монте-Карло. Ми вибираємо послідовне виконання моделювання Монте-Карло на всіх рівнях моделі (активи, загрози, засоби контролю та шкоди); відправною точкою є активи організації, і система поступово рухається до шкоди. Такий підхід забезпечує детальність і потенційно може вказувати на події, які призводять до катастрофічних сценаріїв. Спочатку ми вводимо формалізацію цих послідовних обчислень, перш ніж обговорювати використані значення та розподіли.

Cy-VaR для організації ефективно формується шляхом підсумовування Cy-VaR для всіх активів, враховуючи всі загрози інтересу. Даний підхід враховує мінливість ефективності контролю ризиків шляхом абстрагування будь-яких деталей навколишнього середовища (таких як операційні процеси, конфігурації, методи використання тощо) до простої бінарної моделі, в якій контроль є ефективним або неефективним. Ефективний контроль як запобігає завданню шкоди активу, так і запобігає подальшому поширенню шкоди. Неефективний контроль не захищає актив I може дозволити подальше поширення шкоди. Враховуючи відсутність емпіричних даних, створення більш складної або тонкої моделі в цей час здавалося занадто надуманим.

Ми запускаємо ряд симуляцій Монте-Карло, які виконуються послідовно для кожного активу в кортежах. Результати цих симуляцій об'єднуються для обчислення загального Cy-VaR для одного запуску. Цей підхід дає пояснення того, як можуть відбуватися катастрофічні події протягом певного періоду часу. Точніше, перший крок моделювання Монте-Карло тягне за собою визначення того, виникає загроза чи ні. У [23] розглядаємо розподіл Бернуллі, оскільки ми припускаємо, що загрози є незалежними, і ми не спостерігаємо загроз, що

виникають більше одного разу протягом періоду часу (рік) для однієї і тієї ж організації. Розподіли Бернуллі є дискретними розподілами з двома можливими результатами, 1 або 0, з ймовірністюсі 1 - *c*. Наприклад, якщо ймовірність виникнення загрози становить 20% і результат проби Бернуллі успішний, запускається наступний крок моделювання. Якщо загроза реалізується, система перейде на наступний рівень, тобто рівень контролю. Подібно до загроз, розподіли Бернуллі вибираються, щоб визначити, чи можуть наявні засоби контролю зупинити загрозу чи ні. Ефективність контролю — це розподіл ймовірностей (у нашому прикладі ми використовуємо якісні описи «Високий», «Середній» та «Низький»), який визначить, чи буде контроль ефективним у конкретному прогоні чи ні. У випадку, коли контроль неефективний, перша частина системи завершує і готує перехід до наступного рівня, який є рівнем шкоди. Це описано в Алгоритмі 1 (Додаток А)**,** де функція захищає (контролює, загрожує)повертає або «Правда» або «Помилкове значення», залежно від того, чи вдасться будь-якому із засобів контролю зупинити загрозу, що спричиняє пошкодження активу. Функція Бернуллі повертає «Правда» або «Помилкове значення» на основі ймовірності *c*. Для інтерпретації значення *c,* якщо, наприклад, контроль ефективний на 80%, система виробляє а випадкове число від 0 до 100. Якщо число більше 80, контроль не діє в цьому конкретному запуску. В іншому випадку контроль ефективний. Таким чином, загальна кількість симуляцій, заснованих на теоремі про великі числа, буде мати даний розподіл ймовірності для ефективності контролю, оскільки приблизно в 80% запусків буде ефективним. Щоб врахувати випадки, коли один і той самий тип шкоди може існувати в більш ніж одному шляху графіка шкоди, система буде зберігати стан усіх вузлів у графі шкоди, які запускаються. Такий підхід гарантує, що система не додає збитків від одного типу шкоди більше одного разу. Загальний CVaR запуску – це підсумовування значень, отриманих від випадкового вибору випадкових чисел із середніми значеннями відповідної шкоди та активів. Ця частина системи описана в Алгоритм 2 (Додаток А), де *f rontier* містить усі вузли графіка, *a* реалізація шкоди (функція ймовірності) залежить, серед іншого, від ефективності

засобів контролю, які організації застосовують для пом'якшення такої шкоди.

Для моделювання Монте-Карло [23] та випадково згенерованих значень інструмент підтримує ряд різних розподілів ймовірностей: бета, хі-квадрат, експоненціальний, гамма, Гамбель, нормальний (гаусівський), логарифмічний нормальний, трикутний і Вейбулла. Оператор інструменту повинен вибрати розподіл, який краще відповідає втратам для оцінки. Залежно від вибраного розподілу, розподіл CVaR може бути важким (високий ексцес), що призводить до більших втрат. Рисунок 3.1 ілюструє форми різних розподілів із середнім значенням $\mu = 1$ на 10 000 000 зразків.

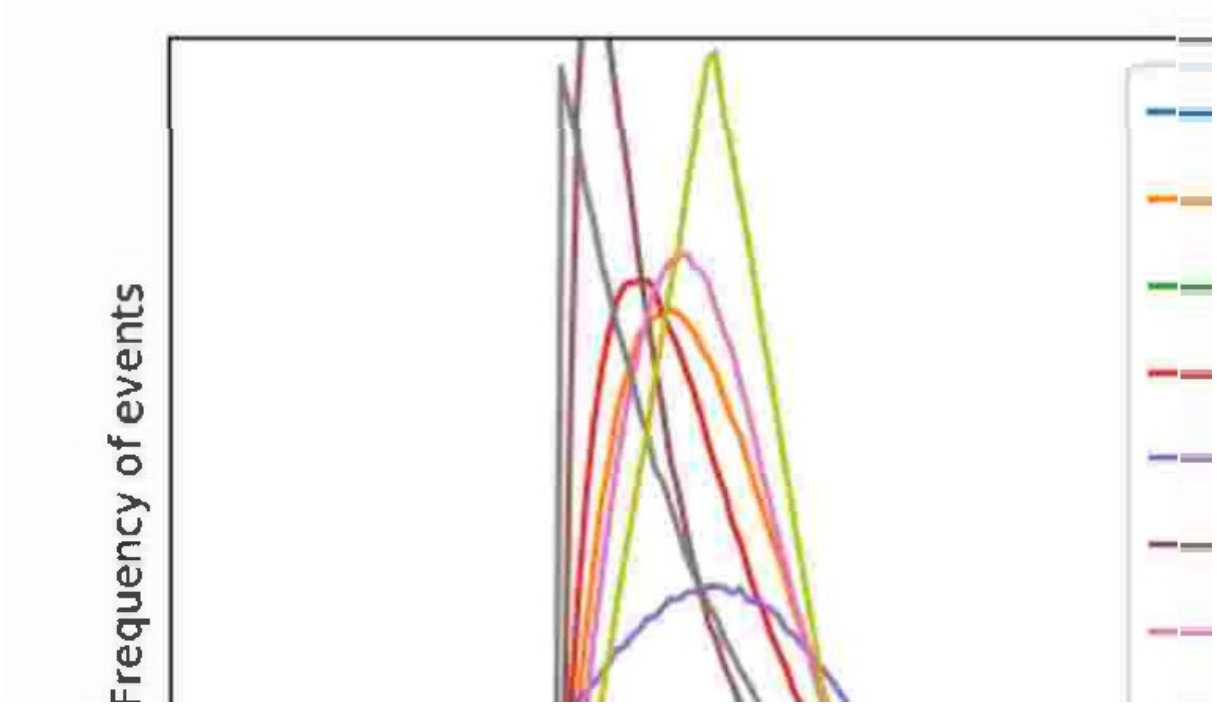

Рисунок 3.1. Ілюстрація моделювання Монте-Карло на основі різних розподілів ймовірностей для випадкового вибору чисел з μ= 1.

Важливо визначити мінімальну кількість пробіжок Монте-Карло *z*. Враховуючи той самий розподіл ймовірностей, велика кількість запусків забезпечить багатший набір значень для створення графіка Cy-VaR, і він, швидше за все, дасть екстремальні значення (тісним чином відповідають хвосту CVaR) [23], ніж невелика кількість запусків. Однак, збільшуючи кількість запусків, ми лінійно збільшуємо час, необхідний для виконання моделювання. Рисунки 3.1 і

3.2 показують графік Q-Q для нормального розподілу, виконуючи моделювання 1000 і 100 000 разів відповідно. За 100 000 запусків результати ближче до розподілу, особливо в хвості. Якщо ми перевіримо асигнування та ексцес даних, ми отримаємо 0,061 і 0,122 для 1000 запусків і 0,006 і 0,012 для 100 000 запусків, що вказує на те, що дані мають кращу симетрію і краще фіксуються в нормі. Подібні результати отримані для інших розподілів. Тому ми вирішуємо проводити моделювання з принаймні 100 000 запусків на одне дослідження.

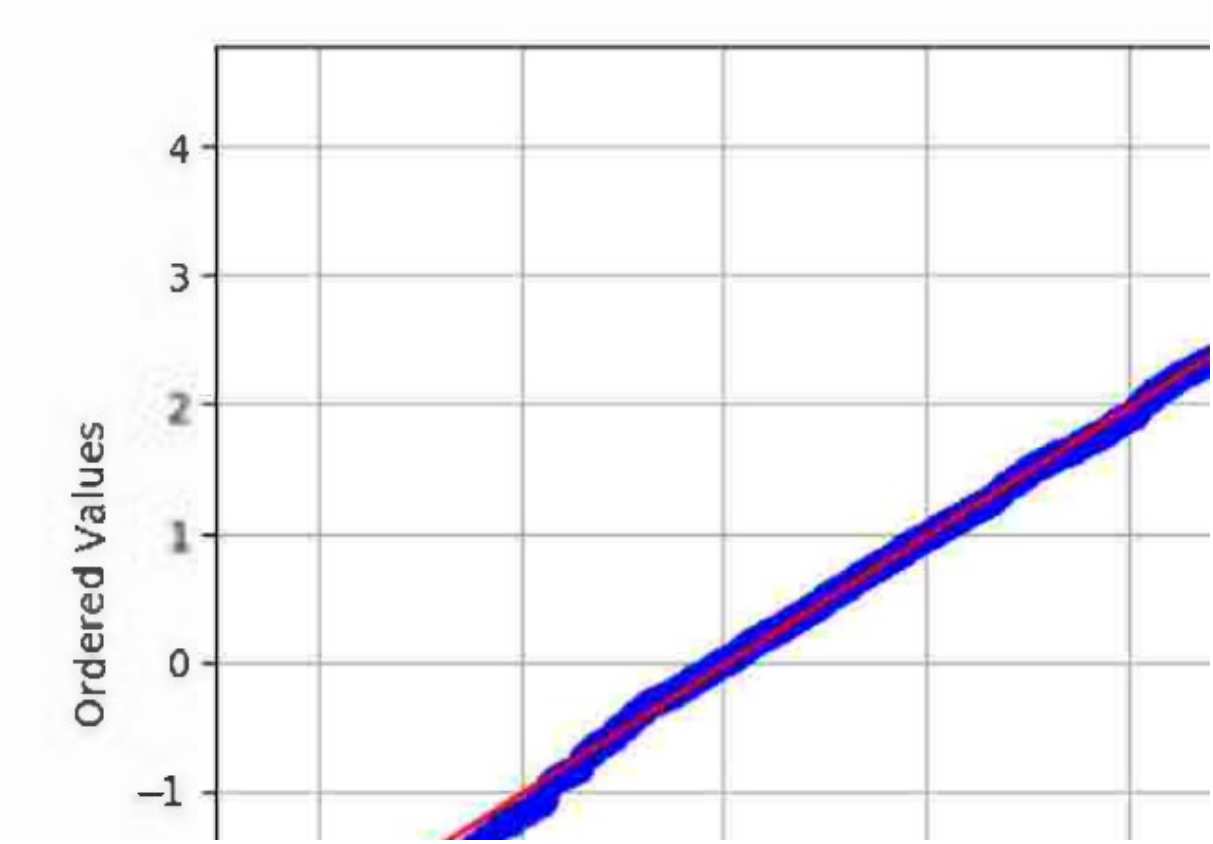

Рисунок 3.2 Графік Q-Q для 1000 запусків із використанням нормального розподілу

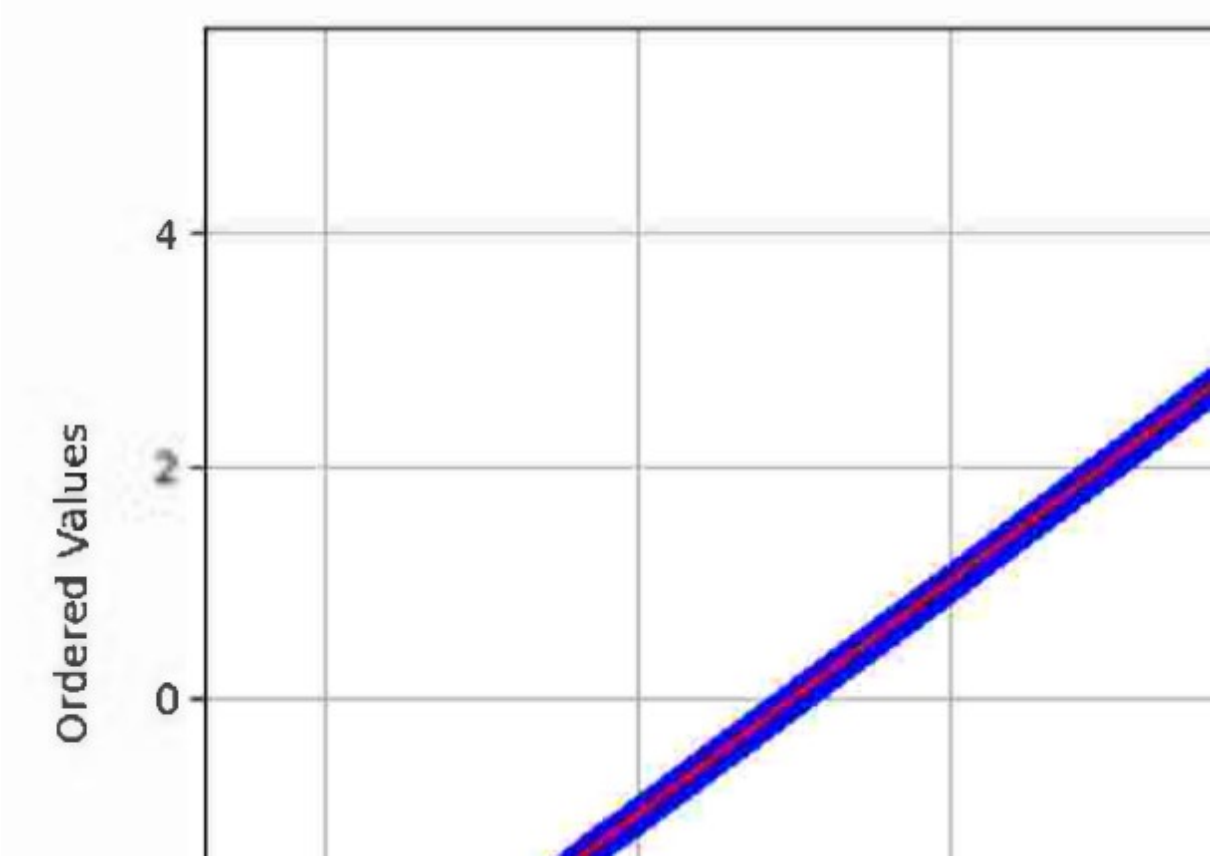

Рисунок 3.3 Графік Q-Q для 100 000 запусків із використанням нормального розподілу

Тим не менш, наша шкода пов’язана не тільки з порушенням даних, а й з багатьма іншими видами втрат. Тому ми не можемо бути впевнені, що дані підійдуть будь-якому із запропонованих розподілів. На жаль, дані, проаналізовані з форм претензій, не надають достатньо деталей для обчислення розподілу втрат, тому ми вирішили запустити моделювання з двома різними розподілами: нормальним і логнормальним. Наше рішення було зумовлено тим, що:

- нормальні розподіли використовуються для представлення випадкових величин, розподіли яких невідомі, а також вони більш помірні при відхиленні від середнього порівняно з іншими розподілами;
- логнормальний використовувався в багатьох дослідженнях, які досягли хороших результатів.

Це дозволить порівняти відмінності результатів, просто використовуючи різні розподіли.

Кількість симуляцій Монте-Карло, які виконує система, визначається кількістю кортежів *k*, що відповідають набору активів A і набору загроз T, що впливають на них. Кількість симуляцій z можна налаштувати в системі, хоча рекомендується мінімум 100 000. Отже, вартість роботи системи дорівнює k * z, що є лінійним для обох змінних.

3.2 Удосконалення оцінки Cy-VaR

Cyber Value-at-Risk (Cy-VaR) розроблено з урахуванням потенційної шкоди, яка може виникнути від кіберзагроз, і змінної ефективності часто використовуваних засобів контролю ризиків. Дане твердження було запантентовано на всесвітньому економічному форумі Deloitte, який відбувася у 2015 році. Зрештою, це спрямовано на розуміння залишкового ризику організацій, шкоди, якій вони можуть зазнати у кіберпросторі, а також наслідків застосування засобів контролю ризиків. Отримання глибокого розуміння ризиків, з якими стикаються організації, може привести до прийняття обґрунтованих рішень щодо контролю ризиків, що може зменшити ймовірність виникнення кіберзагроз або покращити здатність пом’якшувати різні види шкоди. Така інформація має вирішальне значення для нагляду за ризиками та функцій керівництва організації, оскільки вони планують стійкість та встановлюють схильність до ризику, а також для спеціалістів із кібербезпеки, які повинні розуміти залишковий ризик, який може виникнути внаслідок використання засобів контролю ризиків та зміни ландшафту загроз

Подібним чином страхові компанії, які підписують поліси, щоб допомогти організаціям розподіляти та передавати кібер-ризики, зацікавлені в точній оцінці Cy-VaR. На відміну від ринку майнового страхування, де андеррайтинг здійснюється лише на основі покриття, андеррайтери кіберполіс вивчають докази позиції безпеки організацій (Європейське управління страхування та професійних

пенсій, EIOPA). Таким чином, наріжним каменем для оцінки премій у кіберполітиках є ефективність контролю ризиків, які впроваджують організації. Тут дані Cy-VaR можуть містити інформацію про оцінку премій, враховуючи організаційну поведінку щодо контролю ризиків, наслідки, які вони мають для залишкового ризику, і потенційні збитки, з якими організації стикаються в результаті кібератак. Проблема, однак, полягає в тому, що засоби контролю ризиків, які зазвичай вважаються необхідними для професійної та експертної спільноти, як правило, не підкріплюються будь-якою структурою, яка сприяє чіткому обґрунтуванню, кваліфікації або кількісній оцінці переваг, які є результатом їх застосування. Це означає, що реальна цінність відповідності або мінливості відповідності стандартам контролю ризиків не є добре обґрунтованими або виміряними в науковому, однозначному або підданому перевірці сенсі.

Проте, дані методики оцінки Cy-Var є дуже узагальнювальними вілносно переліку загроз, які існують для різних організацій. Альтернативним рішенням даної проблеми являється проведення оцінки ризиків кібербезпеки на основі експертного оцінювання. Оцінка ризиків кібербезпеки допомагає організаціям розуміти, контролювати та пом’якшувати всі форми кіберризиків. Це важливий компонент стратегії управління ризиками та зусиль із захисту даних.

В деяких тлумаченнях кіберризики іноді можна називати загрозами інформаційній безпеці безпеці. Приклади кіберризиків включають:

- Кібер-вимагання
- Ексфільтрація даних
- Помилки IT
- Крадіжка особистих даних/злом цифрових даних
- Промисловий контроль та операції
- Порушення роботи мережі/веб-сайту
- Фішинг, спуфінг, соціальна інженерія
- Конфіденційність – несанкціонований договір або розкриття інформації, несанкціоноване

- Знімання, фізичне втручання
- Відмова в обслуговуванні (DDoS)/Порушення системи

Використовуючи цю просту методологію, можна розробити високорівневий розрахунок кіберризику в IT-інфраструктурі:

$$Cy\text{-}VaR = загроза * вразливість * інформаційна цінність \quad (3.1)$$

У світі існує чимало практичних стратегій, які існують для того, щоб мінімізувати ризик кібербезпеки. Незважаючи на те, що вони зазвичай використовуються як синоніми, кіберризики та вразливості не є однаковими. Уразливість — це слабкість, яка призводить до несанкціонованого доступу до мережі під час експлуатації, а кіберризик — це ймовірність використання вразливості. Кіберризики поділяються на категорії від нульового, низького, середнього та високого. Слід пам'ятати, що існує дуже мало речей з нульовим ризиком для бізнес-процесу чи інформаційної системи, а ризик передбачає невизначеність. Якщо щось станеться гарантовано, це не ризик. Це частина загальних бізнес-операцій.

Основна мета оцінки кіберризиків полягає в тому, щоб інформувати зацікавлені сторони та підтримувати належну відповідь на виявлені ризики. Вони також надають резюме, щоб допомогти керівникам і директорам приймати обґрунтовані рішення щодо безпеки.

Якщо ви зможете відповісти на ці запитання, ви зможете визначити, що захищати. Це означає, що ви можете розробити засоби контролю IT-безпеки та стратегії безпеки даних для усунення ризиків. Але перш ніж це зробити, вам потрібно відповісти на такі запитання:

- Який ризик я зменшую?
- Це найбільш пріоритетний ризик безпеки?
- Чи знижу я ризик найбільш рентабельним способом?

Це допоможе вам зрозуміти інформаційну цінність даних, які ви намагаєтеся захистити, і дозволить вам краще зрозуміти процес управління інформаційними ризиками в рамках захисту бізнес-потреб.

Хто має проводити оцінку кіберризиків? В ідеалі організації повинні мати спеціальні внутрішні команди, які обробляють оцінки ризиків. Це означає, що IT-персонал має розуміння того, як працює ваша цифрова та мережева інфраструктура, керівників, які розуміють, як передається інформація, і будь-які власні організаційні знання, які можуть бути корисними під час оцінювання.

Організаційна прозорість є ключем до ретельної оцінки кіберризиків. Малі підприємства можуть не мати потрібних співробітників для ретельної роботи, і їм доведеться передати оцінку третій стороні. Організації також звертаються до програмного забезпечення для кібербезпеки , щоб контролювати свою оцінку кібербезпеки, запобігати порушенням , надсилати анкети безпеки та зменшувати ризики третіх сторін. Для більш ретельної оцінки кіберризиків було розроблено шаблон, відносно якого можна якісно дати оцінку кіберризикам:

Крок 1. Визначення цінності інформації. Більшість організацій не мають необмеженого бюджету для управління інформаційними ризиками, тому краще обмежити свою сферу діяльності найбільш важливими для бізнесу активами.

Щоб заощадити час і гроші пізніше, витратите деякий час на визначення стандарту для визначення важливості активу. Більшість організацій включають вартість активів, юридичний статус та ділову важливість. Після того, як стандарт буде офіційно включено в політику управління інформаційними ризиками організації, використовуйте його для класифікації кожного активу як критичного, основного або другорядного. Для визначення цінності інформації, можна застосовувати такі питання, а саме:

- Чи існують фінансові або юридичні санкції, пов’язані з розкриттям або втратою цієї інформації?
- Наскільки ця інформація цінна для конкурента?

- Чи можемо ми відтворити цю інформацію з нуля? Скільки часу це займе і які будуть пов’язані з цим витрати?
- Чи вплине втрата цієї інформації на дохід або прибутковість?
- Чи вплине втрата цих даних на повсякденні бізнес-операції? Чи могли б наші співробітники працювати без нього?
- Яку шкоду репутації завдасть витік даних ?

Крок 2. Визначення пріоритетів активів. Першим кроком є визначення активів для оцінки та визначення обсягу оцінки. Це дозволить визначити пріоритетність активів для оцінки. У цій ситуації потрібно працювати з бізнес-користувачами та керівництвом, щоб створити список усіх цінних активів. Для кожного активу зберіть таку інформацію, якщо це можливо:

- програмне забезпечення
- Апаратне забезпечення
- Дані
- Інтерфейс
- Кінцеві користувачі
- Особиста підтримка
- Мета
- Критичність
- Функціональні вимоги
- Політики безпеки IT
- Архітектура безпеки IT
- Топологія мережі
- Захист зберігання інформації
- Інформаційний потік
- Технічний контроль безпеки
- Контроль фізичної безпеки
- Екологічна безпека

Крок 3. Визначення кіберзагрози. Кіберзагроза — це будь-яка вразливість,

яка може бути використана для порушення безпеки , щоб заподіяти шкоду або вкрасти дані вашої організації. Хоча хакери, зловмисне програмне забезпечення та інші ризики IT-безпеки нагадують, існує багато інших загроз:

- Стихійні лиха : повені, урагани, землетруси, блискавки та пожежі можуть знищити стільки ж, скільки будь-який кібер-зловмисник. Ви можете втратити не тільки дані, але й сервери. Вибираючи між локальними і хмарними серверами, подумайте про ймовірність стихійних лих.
- Збій системи : Ваші найкритичніші системи працюють на високоякісному обладнанні? Чи мають вони хорошу підтримку?
- Людська помилка : чи правильно налаштовано ваші сегменти S3, що містять конфіденційну інформацію ? Чи має ваша організація належну освіту щодо шкідливого програмного забезпечення, фішингу та соціальної інженерії ? Будь-хто може випадково натиснути посилання на шкідливе програмне забезпечення або ввести свої облікові дані для фішингового шахрайства. Вам потрібно мати надійні засоби контролю IT-безпеки, включаючи регулярне резервне копіювання даних, менеджери паролів тощо.
- Змагальні загрози : сторонні постачальники , інсайдери, довірені інсайдери, привілейовані інсайдери, встановлені колективи хакерів, спеціальні групи, корпоративне шпигунство , постачальники, національні держави

Існують деякі поширені загрози, які впливають на кожну організацію, включають:

- Несанкціонований доступ: як зловмисники, так і зловмисне програмне забезпечення, помилка співробітника
- Зловживання інформацією авторизованими користувачами: зазвичай це інсайдерська загроза, коли дані змінюються, видаляються або використовуються без схвалення

- Витоки даних: персональна інформація та інші конфіденційні дані зловмисниками або через погану конфігурацію хмарних служб
- Втрата даних: організація втрачає або випадково видаляє дані внаслідок поганого резервного копіювання або реплікації
- Порушення обслуговування: втрата доходу або пошкодження репутації через простої

Крок 4. Визначення вразливих місць. Тепер настав час перейти від того, що «може» статися, до того, що має шанси статися. Уразливість — це слабкість, яку загроза може використати, щоб порушити безпеку, завдати шкоди вашій організації або вкрасти конфіденційні дані. Уразливості можна знайти за допомогою аналізу вразливостей, звітів аудиту, бази даних уразливостей Національного інституту стандартів і технологій (NIST), даних постачальників, груп реагування на інциденти та аналізу безпеки програмного забезпечення .

Існує можливість зменшити вразливості організаційного програмного забезпечення за допомогою належного керування виправленнями за допомогою автоматичних примусових оновлень. Але варто не забувати про фізичні вразливості, ймовірність того, що хтось отримає доступ до комп'ютерної системи організації, зменшується завдяки доступу з карткою ключів.

Крок 5. Аналіз елементів керування та запровадження нових елементів керування. Необхідно виконати аналіз наявних засобів контролю, щоб мінімізувати або виключити ймовірність загрози чи вразливості. Контроль можна реалізувати за допомогою технічних засобів, таких як апаратне чи програмне забезпечення, шифрування, механізми виявлення вторгнень, двофакторна автентифікація, автоматичне оновлення, безперервне виявлення витоку даних або за допомогою нетехнічних засобів, таких як політики безпеки та фізичні механізми, як-от замки чи доступ з картки ключів.

Контроль слід класифікувати як превентивний або детективний контроль. Запобіжні засоби контролю намагаються зупинити такі атаки, як шифрування, антивірус або безперервний моніторинг безпеки , детективні засоби контролю

намагаються виявити, коли сталася атака, як-от безперервне виявлення доступу до даних.

Крок 6. Розрахунок ймовірності та впливу різних сценаріїв на річній основі. Тепер маючи знання відносно цінності інформації, загроз, вразливостей та засобів контролю, це дає можливість не тільки в тому, чи у майбутньому вдасться зіткнутися з однією з цих подій у якийсь момент, але і в тому, який потенціал для успіху може бути. Дану інформацію можна використовувати, щоб визначити, скільки витратити на пом’якшення кожного з визначених кіберризиків.

Крок 7. Розставлення пріоритетів кіберризиків на основі вартості профілактики та цінності інформації. Використовуючи рівень ризику як основу (високий, середній, низький), це дасть змогу визначити дії дії для вищого керівництва чи інших відповідальних осіб для зменшення ризику.

Проте слід обов'язково пам'ятати, що якщо захист активу коштує більше, ніж коштують сам актив, можливо, не має сенсу використовувати превентивний контроль для його захисту. Також це може мати великий вплив на репутацію, а не лише на фінансовий вплив, тому важливо враховувати наступне:

- Організаційна політика
- Репутаційна шкода
- Доцільність
- Положення
- Ефективність контролю
- Безпека
- Надійність
- Організаційне ставлення до ризику
- Толерантність до невизначеності щодо факторів ризику
- Організаційне зважування факторів ризику

Крок 8. Документування та аналіз результатів звітів про оцінку кіберризиків. Цей крок дає змогу розробити результат звітів про оцінку ризиків для підтримки керівництва у прийнятті рішень щодо бюджету, політики та

процедур. Для кожної загрози звіт повинен описувати ризик, уразливі місця та цінність. Поряд з впливом і ймовірністю виникнення і рекомендації щодо контролю.

На основі даного шаблону було виконано дослідженя на конкретній виробничій інфраструктурі. За допомогою експертного опитування, в якому брали участь 6 працівників, які мали повний об'єм інформації відносно бізнес процесів. Таблиця 3.1 показує зібраний аналіз кіберризику одного працівника відносно 7 обраних загроз на конкретній виробничій організації.

Таблиця 3.1 Кіберризики одного працівника відносно 7 обраних загроз

	Загроза	Вразливість	Інформаційна цінність	Cy-VaR
Соціальна інженерія	0.8	0.8	0.9	0.576
Промисловий контроль та операції	0.23	0.32	0.46	0.3174
Крадіжка особистих даних/злом цифрових даних	0.3	0.61	0.91	0.16653
Знімання, фізичне втручання	0.9	0.8	0.55	0.396
Порушення роботи мережі/веб-сайту	0.27	0.35	0.4	0.378
Конфіденційність	0.8	0.85	0.9	0.612
Помилки IT	0.18	0.81	0.19	0.27702

Виконавши процедуру з кожним з 6 експертів було визначено список пріоритетних загроз для конкретної виробничої організації (Таблиця 3.2)

Таблиця 3.2 Сумарний Cy-Var

Cy-Val № есперта	1	2	3	4	5	6	μ
Знімання, фізичне втручання	0.576	0.625	0.851	0.691	0.401	0.702	0.641
Промисловий контроль та операції	0.317	0.432	0.601	0.568	0.32	0.443	0.447
Крадіжка особистих даних/злом цифрових даних	0.166	0.278	0.543	0.571	0.374	0.199	0.355
Соціальна інженерія	0.396	0.498	0.515	0.731	0.781	0.765	0.613
Порушення роботи мережі/веб-сайту	0.378	0.221	0.351	0.201	0.3	0.3	0.292
Конфіденційність	0.612	0.731	0.591	0.672	0.567	0.912	0.68
Помилки IT	0.277	0.175	0.355	0.320	0.2	0.3	0.271

Даний набір загроз визначає найбільшу небезпеку для організації:

1. Конфіденційність – несанкціонований договір або розкриття інформації
2. Знімання, фізичне втручання

3. Соціальна інженерія
4. Крадіжка особистих даних/злом цифрових даних
5. Промисловий контроль та операції
6. Порушення роботи мережі/веб-сайту
7. Помилки IT

Обравши пріоритетні загрози, це дасть змогу отримати достовірну оцінку Cy-VaR для пріоритетної загрози на конкретній виробничій організації. Важке завдання для компаній – визначити, скільки ресурсів інвестувати в різні бізнес-проекти. Труднощі є особливо великими, якщо ці проекти, замість того, щоб принести негайну економічну віддачу, мають своєю основною метою запобігання майбутніх втрат.

Також, зі списку вище було обрано загрози, які мали пріоритет високий, а саме:

1. Конфіденційність – несанкціонований договір або розкриття інформації
2. Знімання, фізичне втручання
3. Соціальна інженерія

3.3 Обрахування на конкретному прикладі

На основі проведеного дослідження виконаємо апробацію розрахунків кіберцінності під ризиком при оцінці інвестицій в інформаційну безпеку. Були саме обраховані загрози які мають пріоритет високий.

Конфіденційність. Виробнича організація останніми роками постраждала від зростаючих порушень безпеки, тому власники вирішили інвестувати гроші в рішення безпеки. Виходячи з минулих успішних кібератак, очікується щорічна втрата даних, штрафів і продуктивності в 1 375 000 українськийх гривень Більше

того, 2 850 000 ₴ – це розрахункова максимальна очікувана втрата з рівнем довіри 5%. Вартість захисного рішення становить 485 000 ₴ на рік. Очікуваним ефектом пом'якшення від інвестицій є щорічне зниження збитків до 85%.

Спочатку порахуємо рентабельність інвестицій у безпеку (ROSI)

$$\text{ROSI} = \frac{1168750 - 485000}{485000} = 1.409 \qquad (3.2)$$

Тепер порахуємо рентабельність інвестицій у безпеку (ROSI) з поправкою на ризик (RaROSI)

$$\text{RaROSI} = \frac{947500 - 485000}{485000} = 0.953 \qquad (3.3)$$

Обрахуємо рентабельність капіталу з поправкою на ризик у кібербезпеку

$$\text{CyRAROC} = \frac{1168750 - 48500 \quad 0.15 * 2850000}{2850000} = 0.389 \qquad (3.4)$$

На основі рівнянь (5), (7) і (9) обчислюються ROSI, RaROSI та CyRAROC. Ми можемо помітити, що розрахунковий ROSI для компанії становить 140.9%. Інвестиції, які в цьому прикладі становлять 485 000 ₴ на рік, заощадить організації приблизно 679 000 українських гривень на рік, що визначається різницею між очікуваним зменшенням збитків ΔE[L] та інвестиційною вартістю l_0. Як наслідок, заощадження, отримані від інвестиції, дасть 140.9% окупності інвестицій у безпеку. Тим не менш, враховуючи найгірший випадок втрати з рівнем довіри 5%, RaROSI становить 95,3%, нижче, ніж ROSI. Дійсно, в цьому випадку компанія заощаджує приблизно 947 500 ₴, що визначається різницею ΔU[L] - l_0, знаменником рівняння (7). Це нижче значення пояснюється тим, що ефект пом’якшення від інвестицій обчислюється у відсотках від CyVAR, тобто ΔU[L] = E[L] - mCyVaR(a). CyRAROC становить 38,9%, встановлюючи i = 15% у рівнянні (9).

Знімання та фізичне втручання. Компанія. останніми роками постраждав від зростаючих порушень безпеки, і вирішив інвестувати гроші в рішення безпеки. Виходячи з минулих успішних кібератак, очікується щорічна втрата даних, штрафів і продуктивності в 200 000 українських гривень. Більше того, 350 000 ₴ – це розрахункова максимальна очікувана втрата з рівнем довіри 5%. Вартість захисного рішення становить 74 000 ₴ на рік. Очікуваним ефектом пом'якшення

від інвестицій є щорічне зниження збитків до 90%.

На основі рівнянь (5), (7) і (9) обчислюються ROSI, RaROSI та CyRAROC. Ми можемо помітити, що розрахунковий ROSI для становить 143%. Інвестиції, які в цьому прикладі становлять 74 000 На основі рівнянь (5), (7) і (9) обчислюються ROSI, RaROSI та CyRAROC. Ми можемо помітити, що розрахунковий ROSI для організації становить 143%. Інвестиції, які в цьому прикладі становлять 74 000 ₴ на рік, заощадить організації приблизно 106 000 українських гривень на рік, що визначається різницею між очікуваним зменшенням збитків ΔE[L] та інвестиційною вартістю l_0. Як наслідок, заощадження, отримані від інвестиції, дасть 143% окупності інвестицій у безпеку. Тим не менш, враховуючи найгірший випадок втрати з рівнем довіри 5%, RaROSI становить 122,9%, нижче, ніж ROSI. Дійсно, в цьому випадку компанія заощаджує приблизно 91 000 ₴, що визначається різницеюΔ [L] - l_0, знаменником рівняння (7). Це нижче значення пояснюється тим, що ефект пом'якшення від інвестицій обчислюється у відсотках від CyVAR, тобто ΔU[L] = E[L] - mCyVaR(a). CyRAROC становить 45,28%, встановлюючи i = 15% у рівнянні (9).

Третьою загрозою пріоритету високий є соціальна інженерія. Дані обрахунки показують оцінку ROSI у 233%, що є дуже високим показником. У цьому випадку інвестиції в розмірі 60 000 ₴ на рік заощадили б приблизно 140 000 ₴ на рік. Таким чином, оцінка ROSI, скоригована на ризик, є негативною (-225%) і говорить нам, що при рівні довіри 5% компанія може втратити 125 000 українських гривень за один рік із дуже високою негативною окупністю -225%. CyRAROC становить 29,7%, що дуже низький у порівнянні з попередніми загрозами описані вище.

Таблиця 3.3. Результати метрики інвестицій у безпеку

	Конфіденційність	Знімання та фізичне втручання	Соціальна інженерія
Інвестування у	485 000	-74 000	-60 000

безпеку			
ΔE[L]	1 168 750	180 000	200 000
ΔU[L]	947500	165 000	-75 000
ROSI	140.9%	143%	233%
RaROSi	95.3%	122.9%	-225%
CyRAROC	38.9	45.28	29.7%

На основі даних результатів, було створено таблицю (таблиця 3.3) результатів метрики у безпеку[23]. У всіх трьох обрахунках прикладах ROSI дає дуже хороші результати, проте RaROSI нижчий в всіх тьох випадках випадках. Справді, він враховує ризик виникнення хвостової події. Насправді, його значення сильно залежить від обраного рівня довіри, що відображає ступінь неприйняття ризику особи, яка приймає рішення. Обраховуючи загрозу соціальної інженерії ми помічаємо, що навіть якщо ROSI є дуже високим порівняно з передніми, його значення з поправкою на ризик (RaROSI) є глибоко негативним, при цьому CyVaR дуже високий порівняно з очікуваними збитками E[L]. Більше інформації надає CyRAROC, який може допомогти особам, які приймають рішення, порівняти різні інвестиції. Ці результати показують, що Cy-VaR пропонує додаткову інформацію, яка підтримує інвестиційні рішення. Справді, при ефективному виборі інвестицій слід враховувати показники ризику, включаючи втрати в найгіршому випадку.

Висновок до 3 розділу

За допомогою створенного шаблону було виконане дослідження на конкретній виробничій організації та упорядковано обрано загрози, які притаманні даній організації. Також відносно перших трьох загроз, які мають пріритет високий бупо проведено математичні розрахунки по оцінці Cy-VaR. НА

основі обрахунків можемо зробити висновок, що майбутніх дослідженнях може бути цікаво оцінити запропоновані метрики, що моделюють агрегований розподіл втрат, беручи до уваги залежність між фактичними кібервтратами. Крім того, емпіричні результати покращать майбутні дослідження.

ВИСНОВКИ

У цій дисертації ми провели аналіз стандартів інформаційної, проаналізували моделі формування ризику, проаналізували модель інвестування в інформаційну безпеку.

У даній роботі було проаналізовано вибір метрик у безпеку. Основна мета метрики - порівняти альтернативи. Хоча порівняння в часі або між організаційними підрозділами можна проводити з конкретними технічними показниками рівня безпеки, порівняння між заходами захисту або варіантами розподілу бюджету вимагають, щоб основні показники були в одному масштабі. Також було проаналізовано методику ролі кібер-цінності ризику. Дана методика дозволяє оцінити Cy-VaR на основі інвестиції в кібербезпеку.
У результаті аналізів було визначено альтернативний розрахунок розподілу – моделювання Монте-Карло.

За допомогою створенного шаблону було виконане дослідження на конкретній виробничій організації та упорядковано обрано загрози, які притаманні даній організації. Також відносно перших трьох загроз, які мають пріритет високий бупо проведено математичні розрахунки по оцінці Cy-VaR. На основі обрахунків можемо зробити висновок, що майбутніх дослідженнях може бути цікаво оцінити запропоновані метрики, що моделюють агрегований розподіл втрат, беручи до уваги залежність між фактичними кібервтратами. Крім того, емпіричні результати покращать майбутні дослідження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. State standards of ukraine (Електронний ресерс) - Режим доступу до ресурсу: https://ukrpatent.org/en/articles/dstu

2. ISO (International Organization for Standardization) - Режим доступу до ресурсу: https://www.techtarget.com/searchdatacenter/definition/ISO

3. Архипов О.Є., Архіпова С.А. КОНЦЕПТУАЛІЗАЦІЯ МОДЕЛЕЙ РИЗИКІВ // НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ» №4 //2011

4. Шегда А.В. Ризики в підприємництві: оцінювання та управління: навч. посіб. / А.В. Шегда, М.В. Голованенко; за ред. А.В. Шегди. К.: Знання, 2008. – 271с.

5. Івченко І.Ю. Моделювання економічних ризиків і ризикових ситуацій / І.Ю. Івченко. – К.: Центр учбової літератури. 2007. – 344 с.

6. Архипов О.Є. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації / О. Є. Архипов, І. П. Касперський // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. – 2007. – Вип.2 (15). – С.13–19.

7. Архипов О.Є., Носок С.О. Основи документаційного забезпечення діяльності організації. Навчальний посібник. К.: НТУУ "КПІ", 2010.-НМУ № Е 10/11-084.

8. FIPS (2004). Publication 199 Federal Information Processing Standards

(FIPS), Categorization of Security of Federal Information and Information Systems.

9. NIST (2004). National Institute of Standards and Technology (NIST) Special Publication 800-60 Workshops, Displaying Information Types and Information Systems to the Security Category

10. CSI (2007). CSI Survey 2007. 12th Annual Computer Crime and Security Survey. Retrieved October 10, 2007, from http://www.gocsi.com/forms/csi_survey.jhtml.

11. O. Milov , M. Kostyak , S. Milevskyi , H. N. Rzaev Information security investment model: resource representation and organizational training, In: Advanced Information Systems. 2019. Vol. 3, No. 4

12. Weishaupl, E., Yasasin, E., and Schiyen, G. (2015), "IT Security Investments through the Lens of the Resource-based View: A new theoretical Model and Literature Review," ECIS 2015 Completed Research Papers.

13. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004), "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," International Journal of Electronic Commerce (9:1), pp. 70-104.

14. Demirhan, D. (2005), "Factors Affecting Investment in IT: A Critical Review," Journal of Information Technology Theory and Application (JITTA) (6:4), pp. 1-13.

15. Beautement, A., Sasse, M. A., and Wonham, M. (2008), "The Compliance Budget: Managing Security Behaviour in Organisations," in Proceedings of the 2008 Workshop on New Security Paradigms, pp. 47-58.

16. Argyris, C., Putnam, R., and Smith, D. M. (1985), "Action Science: Concepts, Methods, and Skills for Research and Intervention,",Jossey-Bass San Francisco, CA.

17. Rok Boyanch, Strategies for minimizing risks through economic modeling of ICT, Jozef Stefan Institute and Faculty of Economics, Slovenia

18. Allianz Global Corporate & Specialty. 2021. Allianz Risk Barometer 2021:

Top Business Risks for 2021. Report. Available online: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html (accessed on 10 February 2021).

19. Rainer Bohme, Security Metrics and Security Investment Models In: International Computer Science Institute, Berkeley, California, USA

20. Orlando, Albina. 2021. Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. Risks 9: 184. https:// doi.org/10.3390/risks9100184

21. Christian Locher, Methodologies for Evaluating Information Security Investments - What Basel II Can Change in the Financial Industry, Association for Information Systems AIS Electronic Library (AISeL), 2005

22. Arnau Erolaa,∗ , Ioannis Agrafiotis a , Jason R.C. Nurse b , Louise Axona , Michael Goldsmitha , Sadie Creesea A system to calculate cyber-value-at-risk In: Computers & Security 113 2022

23. Урсол О. І., Гальчинський Л.Ю. Оцінювання ризику кіберзагроз підприємства з метою визначення необхідних витрат для певного рівня кібрезбезпеки, II International Scientific and Theoretical Conference «CURRENT ISSUES OF SCIENCE, PROSPECTS AND CHALLENGES», June10. 2022; Sydney, Australia

ДОДАТОК А

Алгоритм 1 Одна ітерація Монте-Карло

```
losses = 0
triggered = []
for each Ai ∈ A
for all Tuples containing Ai
if Bernoulli(ti)
## the threat is triggered
if protects(Ci, Ti)
## the asset is protected
continue
if Ai ∈/ triggered
losses += ai ∗ random()
triggered.append(ai)
losses += F_HARMS(Ci, Hi)
return losses
```

Алгоритм 2 Алгоритм поширення шкоди

```
function f_harms(Ci, Hi)
f rontier ← Hi
total_harm = 0
triggered = []
while f rontier do
```

```
6: harm ← f rontier.pop()
7: if Bernoulli(harm.hi) then
8: all f ailed ← True
9: for controls ∈ Ci do
10: if not Bernoulli(control.ci) then
11: all f ailed ← False
12: if all f ailed then
13: ## the harm is triggered
14: if not harm in triggered then
15: total_harm += harm.v ∗ random()
16: triggered.append(harm)
17: for successor ∈ harm.successors do
18: f rontier.append(successor)
19: return total_harm
```