**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Західноукраїнський національний університет**
**Факультет комп'ютерних інформаційних технологій**
Кафедра кібербезпеки

**Якименко Назар Ярославович**

# Модель визначення кіберризиків на основі ймовірнісного аналізу/ Cyber Risk Identification Model Based on Probabilistic Analysis

спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи
КБм -21
Н. Я. Якименко

Науковий керівник
д.т.н., професор М.М.Касянчук

Кваліфікаційну роботу
допущено до захисту:

«____» _____ ___2025 р.

Завідувач кафедри
_____ **В.В.Яцків**

**ТЕРНОПІЛЬ - 2025**

**Факультет комп'ютерних інформаційних технологій**

Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
**Якименко Назара Ярославовича**
(прізвище, ім'я, по батькові)

**1. Тема кваліфікаційної роботи:**
**Модель визначення кіберризиків на основі ймовірнісного аналізу/ Cyber Risk Identification Model Based on Probabilistic Analysis**
керівник роботи: д.т.н., професор М.М.Касянчук
затверджені наказом по університету від 29 листопада 2024 року № 938

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
- провести огляд сучасних підходів до класифікації кіберризиків;
- дослідити міжнародні стандарти управління ризиками інформаційної безпеки (ISO 27005, NIST, COBIT);
- розглянути методології оцінки ризиків у кібер-системах;
- проаналізувати типові вразливості та загрози сучасних інформаційних систем;

провести аналіз ризиків конкретної кібер-системи та розробити рекомендації щодо їх мінімізації.

5. Перелік графічного матеріалу у роботі:
– Діаграма впливу для сценаріїв у Space Corp
– Послідовність атаки на мережу супутників
– Діаграма прийняття рішень щодо кібербезпеки
– Модифікована діаграма рішень
– Моделювання методом Монте-Карло

6. Консультанти розділів кваліфікаційної роботи

| | Прізвище, ініціали та посада Консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |
| | | | |
| | | | |
| | | | |

7. Дата видачі завдання 29 листопада 2024 р.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строки виконання етапів кваліфікаційної роботи | Примітка |
|---|---|---|---|
| 1 | Теоретичні основи та сучасний стан проблеми кількісної оцінки кіберризиків | 12.2024 р. – 03.2025 р. | |
| 2 | Методологія моделювання та кількісної оцінки кіберризиків | 03.2025 р. – 06.2025 р. | |
| 3 | Практичне застосування моделей кількісної оцінки кіберризиків | 06.2025 р. – 11.2025 р. | |

Студент _____ Якименко Н. Я.
( підпис )

Керівник роботи _____ д.т.н., професор М.М.Касянчук

# АНОТАЦІЯ

Якименко Н. Я. Модель визначення кіберризиків на основі ймовірнісного аналізу. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека та захист інформації», освітньо-професійна програма «Кібербезпека». – Західноукраїнський національний університет, Тернопіль, 2025.

У роботі були сформульовані та вирішені такі завдання: проведено огляд сучасних підходів до класифікації кіберризиків, досліджено міжнародні стандарти управління ризиками інформаційної безпеки (ISO 27005, NIST, COBIT), розглянуто методології оцінки ризиків у кіберсистемах, проаналізовано типові вразливості та загрози сучасних інформаційних систем, проведено аналіз ризиків конкретної кіберсистеми та розроблено рекомендації щодо їх мінімізації.

Результати дослідження: розроблена методика оцінки ризиків апробована на реальній/модельній кібер-системі, що підтверджує її практичну застосовність. Результати дослідження можуть бути використані фахівцями з інформаційної безпеки для проведення аудиту ризиків та розробки стратегії їх управління.

Ключові слова: КІБЕРРИЗИКИ, АЛГОРИТМИ, БЕЗПЕКА, СЦЕНАРІЇ, ЗАХИСТ ДАНИХ

ABSTRACT

Yakymenko N. Ya. Cyber Risk Identification Model Based on Probabilistic Analysis – Рукопис.

Research for the degree of "Master" in specialty 125 "Cybersecurity and Information Protection", educational and professional program "Cybersecurity". - Western Ukrainian National University, Ternopil, 2025.

The following tasks were formulated and solved in the work: a review of modern approaches to the classification of cyber risks was conducted, international standards for information security risk management (ISO 27005, NIST, COBIT) were studied, methodologies for assessing risks in cyber systems were considered, typical vulnerabilities and threats of modern information systems were analyzed, risks of a specific cyber system were analyzed and recommendations for their minimization were developed.

Research results: the developed risk assessment methodology was tested on a real/model cyber system, which confirms its practical applicability. The research results can be used by information security specialists to conduct a risk audit and develop a risk management strategy.

Keywords: CYBERRISKS, ALGORITHMS, SECURITY, SCENARIOS, DATA PROTECTION.

ЗМІСТ

# ВСТУП

**Актуальність теми.** Кількісна оцінка кіберризиків залишається однією з найбільш складних і актуальних проблем сучасних організацій. Незважаючи на зростання обізнаності щодо загроз інформаційній безпеці, керівники служб інформаційної безпеки (CISO) часто стикаються з труднощами у визначенні пріоритетних напрямів захисту. Зокрема, виникають сумніви щодо того, які ризики становлять більшу небезпеку — фізичні інциденти, пов’язані з втратою пристроїв, чи соціоінженерні атаки, як-от фішинг.

Сучасний ринок пропонує широкий спектр рішень для забезпечення кібербезпеки, однак постачальники цих рішень рідко надають кількісні оцінки впливу своїх технологій на загальний рівень ризику організації. Унаслідок цього спостерігається тенденція до неефективного розподілу ресурсів та здійснення інвестицій у безпеку без належного обґрунтування. Типовим прикладом є ситуація, коли аналітики з безпеки переоцінюють внутрішні загрози, тоді як фактичні дані свідчать про значно більшу частоту атак, наприклад, на веб-сайти та веб-додатки. Аналіз інцидентів упродовж п’ятирічного періоду в окремих організаціях показав, що реальні ризики, пов’язані з кібератаками на вебресурси, значно перевищують загрозу від інсайдерських дій, хоча інтуїтивно може здаватися навпаки.

Відсутність достовірних методів кількісного вимірювання ефективності заходів кібербезпеки ускладнює прийняття стратегічних рішень щодо оптимізації витрат і розподілу бюджету. Інвестиції у шифрування даних, навчання персоналу з протидії фішингу або модернізацію мережевого обладнання часто здійснюються без порівняльної оцінки потенційного зниження ризику. Це призводить до низької ефективності витрат і нераціонального використання обмежених ресурсів.

З огляду на зазначене, актуальним є розроблення методів, які дозволяють здійснювати кількісне оцінювання кіберризиків на основі достовірних статистичних імовірнісних моделей. Поєднання історичних даних про інциденти з аналітичними підходами, зокрема байєсівським моделюванням, відкриває

можливість підвищення точності оцінок ризику навіть у випадках, коли емпіричні дані є неповними або застарілими.

Таким чином, організації, які впроваджують кількісні методи оцінювання кіберризиків, отримують змогу обґрунтовано визначати пріоритети безпеки, підвищувати ефективність інвестицій, а також забезпечувати баланс між рівнем захисту, зручністю використання систем та економічною доцільністю. Представлений у цій роботі підхід спрямований на підвищення об’єктивності процесу прийняття рішень у сфері кібербезпеки шляхом формалізованого аналізу ризиків та економічної оцінки заходів захисту.

**Метою кваліфікаційрої роботи** є аналіз та оцінка ризиків у кібер-системах, розробка методології їх ідентифікації та впровадження заходів щодо мінімізації потенційних загроз інформаційній безпеці організації.

Для досягнення поставленої мети необхідно вирішити низку взаємопов’язаних задач:

- провести огляд сучасних підходів до класифікації кіберризиків;
- дослідити міжнародні стандарти управління ризиками інформаційної безпеки (ISO 27005, NIST, COBIT);
- розглянути методології оцінки ризиків у кібер-системах;
- проаналізувати типові вразливості та загрози сучасних інформаційних систем;
- провести аналіз ризиків конкретної кібер-системи та розробити рекомендації щодо їх мінімізації.

**Об’єктом дослідження** кваліфікаційної роботи є процеси виявлення, оцінки та управління ризиками в кібер-системах.

**Предметом дослідження** методи, моделі та інструменти аналізу ризиків інформаційної безпеки в кібер-системах.

**Методи досліджень.** Для вирішення поставлених наукових завдань використовувався математичний апарат теорії ймовірностей та математичної статистики, методи системного аналізу, методології оцінки ризиків (FAIR,

OCTAVE, CVSS), а також методи моделювання загроз та вразливостей інформаційних систем.

Достовірність та обґрунтованість отриманих у кваліфікаційній роботі результатів та сформульованих на їх основі висновків забезпечуються:

– використанням визнаних міжнародних стандартів управління ризиками (ISO/IEC 27005, NIST SP 800-30);

– строгістю виконаних аналітичних розрахунків та коректним використанням методологічного апарату досліджень;

– застосуванням перевірених методик кількісної та якісної оцінки ризиків.

Справедливість висновків щодо ефективності запропонованих заходів з мінімізації ризиків підтверджена практичним аналізом реальної/модельної кібер-системи, результатами оцінки вразливостей та порівняльним аналізом рівня ризиків до та після впровадження рекомендованих контрольних заходів.

**Наукова новизна.** Удосконалено методику оцінки ризиків інформаційної безпеки кібер-систем шляхом інтеграції кількісних та якісних підходів, що дозволяє підвищити точність ідентифікації критичних вразливостей та пріоритезації заходів захисту. Розроблено комплексну модель оцінки ризиків для кібер-систем, яка враховує специфіку сучасних загроз та динаміку зміни ландшафту кібербезпеки.

**Практичне значення отриманих результатів.**

Розроблена методика оцінки ризиків апробована на реальній/модельній кібер-системі, що підтверджує її практичну застосовність. Результати дослідження можуть бути використані фахівцями з інформаційної безпеки для проведення аудиту ризиків та розробки стратегії їх управління.

**Публікації та апробація ВКР.**

1. Якименко Н., Слободян В., Якименко Ю., Хомяк Р., Метод кількісної оцінки кіберризиків на достовірних статистичних імовірнісних моделей – Тернопіль, 2025. – С.46-49

2. Якименко Н., Слободян В., Якименко Ю., Хомяк Р. Методологія кількісного моделювання кіберризикків для підтримки управлінських ріщень в організаціях – Тернопіль, 2025. – С.112-114

# 1. ТЕОРЕТИЧНІ ОСНОВИ ТА СУЧАСНИЙ СТАН ПРОБЛЕМИ КІЛЬКІСНОЇ ОЦІНКИ КІБЕРРИЗИКІВ

## 1.1. Актуальність та потреба у ймовірнісних методах оцінки кіберризиків

Кіберризики є серйозною проблемою для організацій. Кіберсистеми зараз переповнені злочинцями, хакерами-аматорами, урядовими структурами та іншими супротивниками. Протягом останніх кількох років, увага ЗМІ до питань кібербезпеки також значно зросла. Під час святкового сезону 2013 року з терміналів торговельної мережі Target було викрадено понад 40 мільйонів кредитних карток [1]. Наступного року в результаті подібної атаки з мережі Home Depot було викрадено дані 56 мільйонів кредитних карток. У лютому 2015 року особисті дані майже 80 мільйонів людей були викрадені з медичної компанії Anthem [28]. Спочатку малі підприємства могли розраховувати на те, що їх не помітять, і уникнути кібератак, але в 2014 і 2015 роках злочинці перейшли до банківського шахрайства та атак з використанням програм-вимагачів6, націлених на малі організації [35]. Також почали з’являтися нові категорії злочинців, зокрема самоорганізовані групи активістів та групи, які толеруються державою. Навіть підприємства, що спеціалізуються на хакерстві, стали жертвами; наприклад, у 2015 році Hacking Team зазнала збиткового витоку даних, який викрив діяльність компанії [4].

Поряд із значним зростанням уваги ЗМІ, кібератаки, як було доведено, впливають на підприємства та приватних осіб у унікальний і несподіваний спосіб. Моніторинг кредитів та повідомлення про порушення є основними чинниками витрат, пов’язаних із порушенням безпеки даних; атаки типу «розподілена відмова в обслуговуванні» (DDoS) призводять до переривання діяльності підприємств, а кібератаки — до знищення фізичних компонентів. Кібербезпека зараз визнається суттєвою загрозою для організацій та національної безпеки в цілому.

Більшість рішень щодо інвестицій в безпеку в організаціях приймаються на основі евристики. Керівник служби інформаційної безпеки може покладатися на

інтуїцію, галузеві звіти або рекомендації продавців продуктів безпеки, щоб визначити, які технології впроваджувати. Якщо існує фактичний процес оцінки кіберризиків, то найчастіше він є якісним. Наприклад, для оцінки ймовірності та впливу певного сценарію або класу ризиків може використовуватися матриця ризиків, яка представлена на рисунку 1.1.

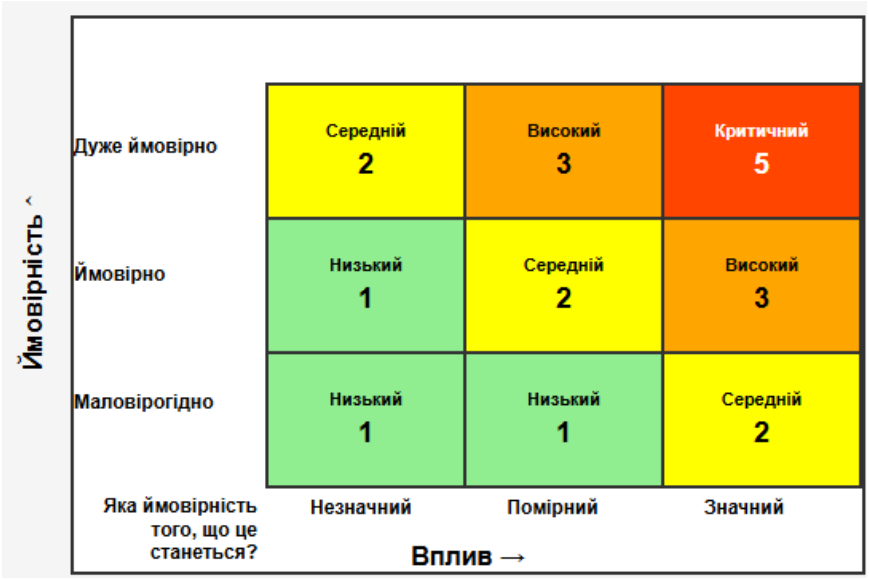



Рисунок 1.1 – Типова матриця ризиків, що використовується для оцінки ризиків

Матриці ризиків мають важливі обмеження і не є достатніми для проведення аналізу ризиків кіберсистем, але можуть бути ефективними інструментами для зацікавлених сторін для обговорення різних ризиків, мають важливі обмеження [36]. Вони не враховують комбінації ризиків або залежності між ними. Крім того, багатий набір інструментів, пов’язаний з імовірнісним аналізом ризиків, не може бути використаний в якісній системі оцінки ризиків. Аналіз чутливості, оптимізація та багато інших потужних методів не можуть бути застосовані до матриці ризиків.

Якісні інструменти також можуть призвести до значної плутанини. Терміни, що використовуються в матриці ризиків, такі як «малоймовірний», є неоднозначними і можуть по-різному тлумачитися різними людьми. У 2018 році дослідники провели опитування інженерів-нафтовиків, щоб вивчити сприйняття різних термінів, таких як «досить впевнений» і «доведений» [6]. Не дивно, що вони виявили, що інженери по-різному тлумачили багато з цих слів. Наприклад, деякі

інженери стверджували, що нафта буде знайдена у 100% родовищ із доведеними запасами, тоді як інші говорили, що нафта буде знайдена лише на 25% родовищ. Така значна розбіжність у тлумаченні суб'єктивних слів несумісна з ретельним аналізом ризику. Насправді існує значна література, яка демонструє упередження та евристику у людей, що призводять до неоптимального прийняття рішень [7]. Навіть такі, здавалося б, прості деталі, як формулювання питання, можуть призвести до значних упереджень.

Якісні методи оцінки ризиків особливо схильні до упередженості і можуть призвести до прийняття неправильних рішень. Кібербезпека особливо схильна до таких упереджень, зважаючи на непропорційну увагу ЗМІ до певних інцидентів, рідкість певних типів подій та велику кількість невизначеності. Наприклад, керівник служби інформаційної безпеки однієї організації обговорював інвестиції в безпеку з аналітиком. Організація нещодавно впровадила повне шифрування диска та програму резервного копіювання даних і розглядала можливість впровадження програми відновлення активів. Аналітик провів швидкий аналіз, щоб визначити, чи є програмне забезпечення для відновлення активів вигідною інвестицією. Програмне забезпечення для відновлення активів було відносно дорогим, його ліцензія коштувала близько 150 000 доларів на рік. Однак, виходячи з кількості ноутбуків, викрадених за останні п'ять років, і припускаючи, що технологія може відновити 100% викрадених пристроїв, аналітик визначив, що організація відновить лише близько 50 000 доларів викраденого обладнання на рік. Отже, відновлення активів було невигідним для організації, оскільки відновлення втрачених активів на суму 50 000 доларів коштувало б 150 000 доларів.

Ймовірнісний аналіз ризиків (PRA) використовується для управління ризиками в ряді інших галузей, включаючи ядерну безпеку, космічні системи та медичні пристрої [8]. Однак багато потужних інструментів та технік PRA ще не застосовуються у кіберсфері, особливо для усунення упереджень, розрахунку співвідношення вигод і витрат та усунення невизначеності щодо подій, які ще не відбулися.

Як зазначалося раніше, упередження пронизують кібербезпеку. Зростання уваги ЗМІ створило враження, що порушення безпеки даних стають все частішими, хоча факти свідчать про протилежне [9]. Деякі вектори атак, які трапляються рідко, є предметом пильної уваги ЗМІ, тоді як більш часті та шкідливі вектори привертають менше уваги. PRA забезпечує суворий спосіб оцінки кіберризику та може усунути багато хибних уявлень, які можуть мати аналітики про кібербезпеку і також забезпечує суворий, повторюваний і точний спосіб оцінки вигод і витрат від інвестицій у кібербезпеку. Кількість постачальників послуг з безпеки різко зросла, але організації не можуть точно оцінити вартість інвестицій у захист за допомогою якісних методів.

PRA також необхідна для усунення поширеної невизначеності в кібербезпеці, що виникає з двох джерел: епістемічної невизначеності, що виникає в першу чергу через ймовірність інцидентів з великим впливом, які ще не відбулися, та збитків, пов'язаних з цими серйозними кіберінцидентами, та алеаторної невизначеності щодо серйозності кібервпливу в випадках, коли дані існують. Багато організацій змушені проводити якісну оцінку через фундаментальну складність оцінки кібервпливу, такого як шкода репутації. Організація може оцінити, що збитки можуть становити від 10 до 50 мільйонів доларів, тому така перспектива просто позначається як «сильний вплив» [7]. Оцінка ймовірності рідкісних, великих інцидентів може бути ще більш складною. Замість того, щоб маскувати невизначеність у якісних категоріях, PRA включає ці невизначені оцінки безпосередньо в аналіз, що часто призводить до інших результатів порівняно з випадком, коли використовуються точкові оцінки витрат. Імовірнісні оцінки призводять до набагато якіснішої дискусії про ризик.

PRA також необхідна для вирішення проблеми невизначеності щодо серйозності наслідків кібератак. Опитування та галузеві звіти переповнені розрахунками «середньої» вартості порушення безпеки даних або «типових» наслідків. Однак деякі наслідки кібератак мають надзвичайно важкі наслідки, що означає, що використання середнього значення є в кращому випадку оманливим, а в гіршому — шкідливим.

На рисунку 1.2 показано розподіл годин розслідування втрачених пристроїв у великій організації, що є одним із багатьох наслідків інциденту. Середній розмір інциденту становить 0,5 години розслідування, але трапляються інциденти, які на три порядки більші.

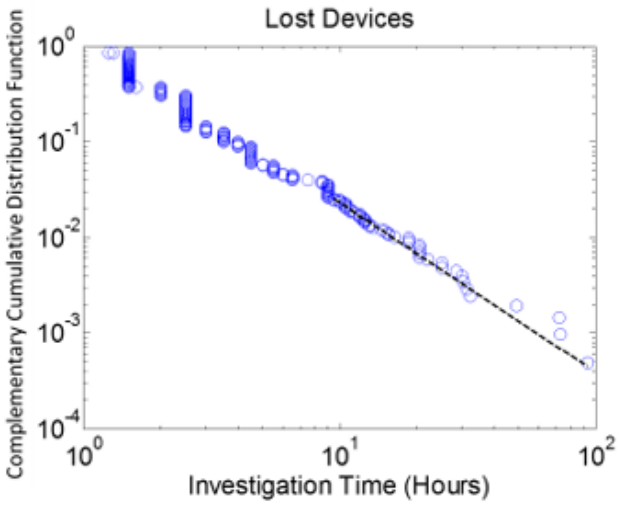



Рисунок 1.2 – Доповнювальна кумулятивна функція розподілу для часу розслідування

Слід зазначити, що розподіл годин розслідування втрачених пристроїв у великій організації є лінійним на логарифмічному графік. Це означає, що розподіл має важкі хвости. Однією з головних переваг імовірнісного аналізу ризиків є можливість розглядати розподіли замість єдиного показника збитків. Явне врахування невизначеності в процесі оцінки кіберризиків дозволяє особам, які приймають рішення, зважувати інциденти з низькою частотою та високим рівнем впливу та інциденти з високою частотою та низьким рівнем впливу. Недостатнє врахування невизначеності в кіберсистемах робить осіб, які приймають рішення, схильними до неправильного розуміння ризиків.

## 1.2. Обсяг та структура дослідження.

У цій роботі представлено метод проведення кількісної оцінки ризиків кіберсистем у вигаданій, але реалістичній організації під назвою Space Corp. Space

Corp займається дослідженнями та розробками різних технологій. Це приватна організація, яка отримує замовлення від державних і приватних клієнтів. Space Corp працевлаштовує приблизно 20 000 осіб у Сполучених Штатах. Мета полягає в розрахунку повної кривої ризику, щоб можна було визначити пріоритетність різних заходів безпеки.

Повна крива ризику складається з різних режимів, а саме: частини, що складається з частих інцидентів з незначним впливом, та частини, що складається з більш масштабних, але рідкісних інцидентів. Хоча деякі організації можуть мати великі обсяги історичних даних, ці минулі статистичні дані обмежуються інцидентами, що вже відбулися, і можуть не враховувати інциденти, які є або рідкісними, або новими типами інциденти, які ще не відбулися.

Для оцінки загального ризику крива ризику поділяється на три різні режими (рис. 1.3):

1. Модель на основі даних походить від історичних інцидентів, якщо дані існують і є стабільними в часі;

2. Модель на основі сценаріїв використовується для моделювання інцидентів, які ще не відбулися;

3. Режим перекриття поєднує модель на основі даних і модель на основі сценаріїв шляхом перекриття кривих ризику, щоб уникнути подвійного підрахунку інцидентів.

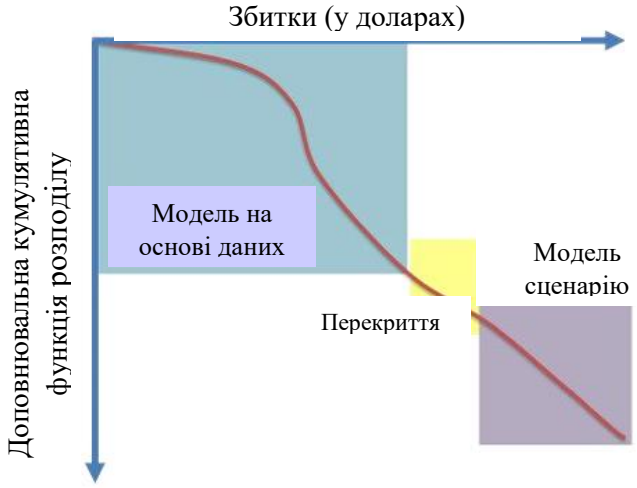



Рисунок 1.3 - Три режими кривої ризику

Фактична крива ризику генерується за допомогою симуляції Монте-Карло та імовірнісної моделі, яка ініціалізується на основі інформації, зібраної з даних, від експертів та байєсівського аналізу певних сценаріїв. Ці частини об'єднуються в загальну модель для оцінки кіберризику в організації.

Моделювання кібербезпеки вимагає системного аналізу, що включає інформацію про зловмисників, засоби захисту, систему та наслідки. Інформація про зловмисників є корисною для визначення найкращого способу захисту організації, тобто аналітики можуть визначити, хто вони, що вони знають і чого хочуть. Крім того, багато організацій мають обмежену інформацію про те, як працюють їхні системи і що потребує захисту. Модель витрат формулюється для кількісної оцінки наслідків кіберінцидентів. Це робиться в доларовому еквіваленті, оскільки для порівняння кіберризику з іншими видами бізнес-ризику необхідні грошові наслідки. Нарешті, економічна ефективність різних інвестицій у безпеку оцінюється шляхом моделювання зниження ризику, пов'язаного з кожним заходом захисту.

Хоча кібербезпека є актуальною для багатьох зацікавлених сторін на різних рівнях, основна увага в цій роботі приділяється оцінці кібербезпеки на організаційному рівні, а не на індивідуальному чи урядовому рівні. Модель, представлена в цій роботі, не дуже підходить для урядів, які стикаються зі стратегічними рішеннями в галузі кібербезпеки, що взаємодіють зі складним економічним і політичним ландшафтом. Представлений тут метод найкраще підходить для організацій або навіть менших масштабів, включаючи управління ризиками на рівні проектів.

Важливим аспектом моделювання кібербезпеки є врахування динамічної природи загроз. Кіберзагрози постійно еволюціонують: зловмисники розробляють нові методи атак, використовують раніше невідомі вразливості (zero-day exploits) та адаптуються до впроваджених засобів захисту. Тому ефективна модель оцінки ризиків повинна передбачати механізми регулярного оновлення та перегляду, що дозволяє організаціям своєчасно реагувати на зміни в ландшафті загроз.

Додатково, сучасні підходи до моделювання кібербезпеки все частіше інтегрують методи машинного навчання та штучного інтелекту для прогнозування потенційних атак та автоматизації процесів виявлення аномалій. Використання історичних даних про інциденти безпеки дозволяє будувати предиктивні моделі, які оцінюють ймовірність реалізації конкретних загроз для даної організації з урахуванням її специфіки, галузі діяльності та наявних засобів захисту.

Не менш важливим є врахування людського фактору в моделях кібербезпеки. Статистика свідчить, що значна частина успішних кібератак відбувається через помилки персоналу, соціальну інженерію або недостатню обізнаність співробітників про загрози. Тому комплексна модель повинна включати оцінку організаційних ризиків, пов’язаних з культурою безпеки, рівнем підготовки персоналу та ефективністю політик інформаційної безпеки.

На організаційному рівні модель дозволяє керівництву приймати обґрунтовані рішення щодо розподілу бюджету на інформаційну безпеку, балансуючи між інвестиціями в превентивні заходи та потенційними втратами від реалізації загроз.

## 1.3 Огляд літератури та існуючі підходи до аналізу кіберризиків.

Інформаційні технології (ІТ) кардинально змінили спосіб функціонування організацій. З поширенням ІТ до мереж підключалося все більше систем, що призводить до збільшення кількості вразливостей. Ранні атаки були здебільшого концептуальними і розроблялися комп’ютерними експертами або були результатом експериментів, що пішли не так [11]. З часом змінювалися як зловмисники, так і методи атак. Зараз Інтернет переповнений скриптовими хакерами, злочинними організаціями, хактивістами та державами, які намагаються зламати комп’ютери на різних рівнях. Напади на організації тепер включають вандалізм, вимагання, організовану злочинність та цілеспрямовані атаки з метою викрадення комерційної таємниці. Незважаючи на ці загрози, деякі організації донедавна не визнавали кібербезпеку важливою проблемою. Відповідальність за

кібербезпеку покладається на різних осіб в різних організаціях, серед яких можуть бути директор з управління ризиками, директор з безпеки, директор з інформаційних технологій, директор з технологій або інші посадові особи. Незважаючи на високий статус, директор з інформаційних технологій часто не має значних повноважень і змушений виконувати складне завдання із забезпечення безпеки організації з обмеженими ресурсами, одночасно інформуючи про ризики генерального директора та членів правління, які можуть не розуміти суті кібербезпеки.

Отримання достатніх ресурсів для забезпечення безпеки організації завжди було складним завданням, оскільки безпека вимагає інвестицій для уникнення збитків, але ніколи не приносить прибутку. Виправдати витрати на безпеку складно, коли доводиться конкурувати з іншими бізнес-можливостями, що мають позитивну віддачу від інвестицій. Тому в багатьох організаціях часто спостерігається типова послідовність подій:

1. Організація має слабку інформаційну безпеку, а ресурси розподіляються неефективно.

2. Організація зазнає хакерської атаки.

3. Для вирішення проблеми в безпеку вкладаються великі інвестиції.

Попередній сценарій є неоптимальним, оскільки рішення є реакційними і приймаються на основі минулих результатів, а не ризиків. У 2014 році JPMorgan Chase оголосив, що їхній бюджет на кібербезпеку становить 250 мільйонів доларів на рік [9]. Кілька місяців по тому вони були зламані хакерами, що призвело до чергового оголошення про те, що бюджет на безпеку тепер становитиме 500 мільйонів доларів на рік. Однак не зрозуміло, на чому базується ця цифра, тобто чому інвестиції становлять 500 мільйонів доларів, а не, скажімо, 450 або 550 мільйонів доларів. Хоча ці перші зусилля можуть здаватися ситуативними, організації тепер визнають, що безпекою необхідно керувати, і шукають інструменти для оцінки кіберризиків [13].

Кібербезпека є широкою галуззю, і велика кількість робіт присвячена дослідженню інших аспектів кіберсистем, включаючи міжнародне

кіберзаконодавство, кіберконфлікти та сильне шифрування [14]. Хоча існують деякі роботи з кількісної оцінки ризику в обмежених сферах [15], прикладів оцінки кіберризику на організаційному рівні набагато менше. Наприклад, багато робіт присвячено застосуванню методів машинного навчання до систем виявлення вторгнень (IDS) для поліпшення виявлення зловмисної діяльності в організації, але це принципово інша сфера, ніж кількісна оцінка кіберризику в більш широкому масштабі [16]. Однак багато з цих чудових технічних аналізів можуть бути використані як вхідні дані для загальної моделі ризику.

Дослідники та аналітики з IT-безпеки працювали над розробкою суворих інструментів для оцінки кіберризиків в організаціях вже більше десяти років. Однак брак даних у відкритому доступі перешкоджає публікації валідації моделей кіберризиків, що обмежує обсяг роботи, виконаної в академічних колах. Приватні консультанти, можливо, насправді найбільше просувають цю сферу, використовуючи дані про інциденти, моделювання за методом Монте-Карло та аналіз чутливості для кількісної оцінки ризиків у компаніях, але ці компанії, як правило, не публікують деталі своєї роботи зі зрозумілих причин.

Ранні спроби оцінити кіберризики використовували підхід, заснований на очікуваннях, для оцінки ймовірності події та її наслідків. Наприклад, однією з перших метрик для вимірювання кіберризику була річна очікувана величина збитків (ALE), де $O_i$ - результат і, $I(O_i)$ - вплив результату і, а $P_i$- частота події $i$.

$$ALE = \sum_{i=1}^{N} I\,(O_i)\,P_i. \qquad (1.1)$$

Однак ризик не дорівнює очікуванню, і з роками були запропоновані більш досконалі методи. У дисертаційній роботі Су Ху використовувався аналіз рішень і ймовірнісний аналіз ризиків для оцінки розподілу збитків, пов’язаних з різними заходами кібербезпеки [5]. Метод, який запропонував Су Ху передбачав оцінку частоти атак на організацію, ймовірності успіху цих атак та грошових втрат. Потім він отримав оцінки ефективності різних заходів безпеки, щоб кількісно змоделювати економічну ефективність кожного заходу. Модель включає кілька

потужних технік, зокрема аналіз чутливості, розрахунок вартості інформації та ймовірнісну домінантність.

З огляду на відсутність публічних даних, більша частина досліджень була зосереджена на економічних моделях кібербезпеки або емпіричних дослідженнях, спрямованих на встановлення об'єктивних фактів. У 2002 році Гордон і Лоб опублікували економічну модель оптимальних інвестицій у безпеку [18]. Модель зосереджена на оцінках загроз, вразливостей та наслідків і використовує припущення, що інвестиції в безпеку мають зменшувану граничну віддачу, для розрахунку верхньої межі інвестицій в безпеку. Гордон і Лоб дійшли висновку, що особи, які приймають рішення, не повинні інвестувати більше 37 % від очікуваних збитків у разі порушення безпеки.

Багато інших визнали необхідність створення кращих моделей кіберризиків. Томас та ін. розробили модель розгалуженої діяльності, яка описувала різні сценарії атак і їх наслідків [10]. У цій статті автори надають огляд труднощів оцінки наслідків кіберризиків, включаючи фактори, що стримують організації від розкриття даних, значну невизначеність та людські упередження.

Сонненрайх у [20] ще раніше описали проблеми, пов'язані з розподілами з важким хвостом, але їхній аналіз рентабельності інвестицій у безпеку обмежений відсутністю високоякісних даних. Міністерство оборони США використовує іншу модель ризику, яка називається Інструмент оцінки мережевих ризиків (NRAT) і була розроблена для оцінки операційних ризиків [21].

Одним з найпопулярніших методів оцінки кіберризиків в організаціях є факторний аналіз інформаційних ризиків (FAIR) [22]. FAIR розкладає кіберризики на складові, оцінюючи частоту втрат і масштаб збитків. Обидва ці фактори можна розділити на більш дрібні складові, що дозволяє керівникам і аналітикам легше проводити оцінку. На рисунку 1.4 показано, як різні оцінки функціонально об'єднуються в загальний ризик. Після оцінки кожного компонента він об'єднується з частотою втрат і масштабом втрат, що в сукупності утворюють загальний ризик.


Рисунок 1.4 - Підхід FAIR до кіберризиків

Також NIST опублікував багато документів у рамках спеціальної серії публікацій (SP-800), які охоплюють широкий спектр тем — від дуже детальних і конкретних стандартів шифрування до загальних рамок управління ризиками в кіберсистемах. Ці публікації стали важливим джерелом інформації для осіб, що приймають рішення, але є недостатнім керівництвом для аналітиків, які проводять кількісну оцінку ризиків. Оригінальна версія Посібника NIST з проведення оцінки ризиків (SP 800-30) була опублікована у 2002 році [23].

У 2012 році була випущена нова версія, яка замінила версію 2002 року [24]. На жаль, кількісні методи знову майже не обговорюються, а деякі рекомендації щодо оцінки ризиків не враховують відповідні інструменти та методи. Хоча в документі не висловлюється явна перевага якісних методів над кількісними, наводяться лише якісні та напівкількісні приклади. Крім того, є проблеми з прикладами, наведеними в додатку (табл. 1.1, 1.2).

У 2014 році NIST опублікував новий документ під назвою «Концепція поліпшення кібербезпеки критичної інфраструктури» [25]. У цій концепції перераховано п’ять функцій для досягнення результатів у сфері кібербезпеки: ідентифікація, захист, виявлення, реагування та відновлення. Кожна функція має категорії та підкатегорії, що визначають засоби контролю, процеси та управління, які підтримують цю функцію. У документі також розглядається цикл аналізу ризиків. Концепція кібербезпеки NIST була підтримана урядом США та іншими

організаціями. У лютому 2015 року на саміті з кібербезпеки в Білому домі, що відбувся в Стенфордському університеті, президент США виступив перед лідерами галузі, урядом, науковцями та громадськістю з промовою про важливість кібербезпеки. На саміті кілька бізнес-лідерів оголосили про прийняття структури NIST, серед них Apple, Bank of America, U.S. Bank, Pacific Gas & Electric, AIG, Walgreens та Kaiser Permanente.

Таблиця 1.1

Шкала оцінки – ймовірність настання події, загрози (несуперечна)

| Якісні значення | Напівкількісні значення | | Опис |
|---|---|---|---|
| Дуже високий | 96-100 | 10 | Помилка, аварія або стихійне лихо ймовірно трапляється або трапляється більше 100 разів на рік |
| Високий | 80-95 | 8 | Помилка, аварія або стихійне лихо дуже ймовірно трапляється або трапляється від 10 до 100 разів на рік |
| Помірний | 21-79 | 5 | Помилка, аварія або стихійне лихо досить ймовірно трапляється або трапляється від 1 до 10 разів на рік |
| Низький | 5-20 | 2 | Помилка, аварія або стихійне лихо навряд чи трапляється або трапляється рідше одного разу на рік, але частіше одного разу на 10 років |
| Дуже низький | 0-4 | 0 | Помилка, аварія або стихійне лихо малоймовірні або трапляються рідше, ніж раз на 10 років |

Таблиця 1.2

Шкала оцінки – рівень ризику (поєднання ймовірності та впливу)

| Ймовірність настання загрозливої події та її негативний вплив | Рівень впливу | | | | |
|---|---|---|---|---|---|
| | Дуже низький | Низький | Помірний | Високий | Дуже високий |
| Дуже висока | Дуже низький | Низький | Помірний | Високий | Дуже високий |
| Висока | Дуже низький | Низький | Помірний | Високий | Дуже високий |
| Помірна | Дуже низький | Низький | Помірний | Помірний | Високий |
| Низька | Дуже низький | Низький | Низький | Низький | Помірний |
| Дуже низька | Дуже низький | Дуже низький | Дуже низький | Низький | Низький |

Основна цінність багатьох документів NIST щодо кіберризиків полягає в їхній здатності підкреслити важливість кіберризиків в організаціях. Хоча в конкретних методах, запропонованих у цих документах, є недоліки, ця концепція, ймовірно, додасть значної цінності, розпочавши дискусію. Також важливо визнати, що документи NIST мають обмеження в технічній складності. Організаціям буде складно впровадити структуру з детальними математичними формулюваннями, тому важливо наголошувати на простоті. Однак документи NIST повинні містити більш детальне обговорення кількісних методів і посилання на існуючі складні методи.

Існують також інші якісні рамки для оцінки ризиків у кіберсистемах. Катсікас представляє комплексний огляд методів управління ризиками [26]. COBIT (Control Objectives for Information and Related Technology) — це система управління, яка іноді використовується в IT. OCTAVE — це інший метод, розроблений спільно з US-CERT [38] в Університеті Карнегі-Меллон [22].

Всі ці методи мають обмежену застосовність через їх якісний характер. Нестача публічних даних є основним фактором, що обмежує загальне вивчення кіберризиків. Організації можуть мати власні передові технології, але вони не є загальнодоступними. Проте емпіричні дослідження поступово накопичуються, що дає важливі відомості для осіб, які приймають рішення, та аналітиків [29].

Необхідно проводити більше наукових досліджень у сфері кібербезпеки. Постачальники регулярно публікують офіційні документи з оманливими або неправильними висновками. У 2014 році інститут Понемона опублікував звіт про глобальні витрати на кіберзлочинність, який містив помилки та іноді оманливі результати [8]. Інші публікації містять оманливі висновки, наприклад, використовують середнє значення для опису сильно викривлених даних [12]. Дані також регулярно базуються на невеликих вибірках з добровільних опитувань. Флоренсіо та Херлі написали цікаву статтю про добре відомі проблеми з опитуваннями щодо кіберзлочинності [32]. На жаль, багато дослідників використовують ці звіти, оскільки інших даних немає, що надає галузевим

опитуванням набагато більшої надійності, ніж вони заслуговують [18]. Невелика кількість звітів, спонсорованих галуззю, є корисною.

Академічні дослідження важливі для встановлення об'єктивної істини та запобігання хибним уявленням про кібербезпеку. Компанія McAfee, постачальник антивірусного програмного забезпечення, зазнала жорсткої критики за твердження, що кіберзлочинність коштує світовій економіці 1 трильйон доларів на рік, хоча ця цифра практично не має під собою жодних підстав [34]. Дослідники спростували цю оцінку в статті, присвяченій вивченню вартості кіберзлочинності [4]. Бінер, Елінг і Вірфс дослідили кіберзбитки на основі бази даних операційних ризиків і обговорили наслідки для страхових ринків, запропонувавши більш обґрунтовані оцінками фактичного впливу кіберзлочинності [31].

Іншою темою, яка викликає значні дискусії, є вплив кіберзлочинів на репутацію організації. Дослідження показують розбіжності між тим, що говорять про порушення безпеки даних, та фактичним впливом на ціну акцій [13]. Не дивно, що споживачі можуть дуже голосно висловлюватися про порушення безпеки даних, але як це перетворюється на матеріальний вплив, залишається неясним. З точки зору бізнесу, репутація є цінною для забезпечення майбутніх прибутків. Тому багато дослідників використовували ціну акцій як показник шкоди репутації, а в декількох статтях було проаналізовано дохідність фондового ринку після оголошення про порушення безпеки даних. Дослідження послідовно показують дуже слабкий вплив порушення безпеки даних на ціни акцій; наприклад, як Campbell et al., так і Cavusoglu et al. виявили докази зниження цін на акції протягом двох днів після оголошення про порушення, але не довше. Gordon, Loeb і Zhou виявили докази того, що негативний вплив порушень безпеки даних з часом зменшується, що свідчить про те, що інвестори звикають до порушень безпеки даних. Насправді, переривання бізнесу може бути набагато більш витратним ризиком для організацій, ніж порушення безпеки даних [38].

Публічно доступні кібербази даних стають все більш поширеними, але на даний момент існують лише в обмежених режимах. Наприклад, дані про зараження ботнетами, спам-листи та шкідливі фрагменти коду збираються та підтримуються

організаціями та дослідниками. Однак дані про інциденти кібербезпеки є дуже обмеженими. Privacy Rights Clearinghouse веде відкрите, створене за допомогою краудсорсингу сховище даних про порушення безпеки даних. Ці інциденти схильні до подій, які привертають увагу ЗМІ, але база даних все одно є корисним ресурсом. У кількох статтях було проаналізовано частоту та серйозність порушень безпеки даних з використанням цього джерела даних [39]. VERIS (Vocabulary for Event Recording and Incident Sharing) — ще одна добре задокументована система для повідомлення про інциденти. Дані VERIS містять демографічні дані жертв, описи інцидентів, інформацію про виявлення та реагування, оцінку впливу та багато інших полів. Одним із недоліків VERIS є те, що велика кількість полів може спричинити втому від даних для слідчих, які неодноразово вводять одну й ту саму інформацію для інцидентів з низьким рівнем впливу. Однак загалом ці відкриті бази даних є надзвичайно цінними, оскільки дають уявлення про стан кібербезпеки в різних компаніях.

Хоча дані про кіберінциденти рідко оприлюднюються, багато організацій насправді мають у своєму розпорядженні високоякісні дані, які можна використовувати для аналізу кіберризиків у динаміці. Організації часто реєструють інциденти кібербезпеки, щоб відстежувати навантаження на співробітників, задовольняти вимоги аудиторів, виконувати вимоги щодо звітності або аналізувати кіберризики. Хоча внутрішні бази даних про інциденти безпеки часто ігноруються, вони містять безцінну інформацію, яку можна використовувати для оцінки загроз, вразливостей та наслідків кібератак, надаючи детальний огляд кіберризиків в організації.

Імовірнісний аналіз ризиків та аналіз класів сценаріїв використовуються для оцінки ризиків з високим рівнем впливу в інших сферах. Конкретні сценарії також аналізуються в кіберпросторі. Дослідницька група з Кембриджського університету провела детальний аналіз атаки на енергосистему США [40]. Дослідники вивчили, як шкідливе програмне забезпечення може спричинити відключення електромережі, та кількісно оцінили економічний вплив на підприємства, уряд та страхувальників, створивши кількісні моделі на основі реальних інцидентів. Такий

тип аналізу дає змогу особам, які приймають рішення, проводити якісні обговорення припущень та результатів сценарію моделі.

Ще одним викликом у моделюванні кібербезпеки стає питання, як інтегрувати аналіз сценаріїв з історичними даними. На щастя, ця проблема була вирішена за допомогою декількох технік у ряді галузей. Один із підходів полягає у параметризації оцінок ймовірності, отриманих від експертів, і розгляді їх як попереднього розподілу, який потім можна оновлювати за допомогою історичних даних. Подібна проблема зустрічається в кліматології та фінансовому моделюванні. В обох випадках історичні дані існують, але можуть бути недостатніми, оскільки базова система змінюється. У кліматології підвищення рівня $CO_2$ вимагає поєднання історичних даних з детальними моделями хімічного та фізичного складу атмосфери. У цій магістерській роботі сценарійні моделі інтегровані з моделями, що базуються на даних, шляхом розробки області перекриття кривої ризику. Історичні події, що траплялися рідко, можуть бути використані для порівняння результатів сценарійної моделі та дослідження різних можливих варіантів майбутнього.

# 2. МЕТОДОЛОГІЯ МОДЕЛЮВАННЯ ТА КІЛЬКІСНОЇ ОЦІНКИ КІБЕРРИЗИКІВ

## 2.1. Концептуальні основи моделювання кіберризиків на основі даних про інциденти

Кіберризик складається з поширених інцидентів з невеликим впливом у поєднанні з рідшими інцидентами, що мають більший вплив. Необхідно оцінити всю криву ризику, щоб особи, які приймають рішення, могли зрозуміти обидва типи ризику: історичні інциденти, які вже трапилися, а також нові сценарії, які, можливо, ще не траплялися.

У випадку кібербезпеки аналітики можуть використовувати експертні думки або моделі сценаріїв, які ще не відбулися, щоб отримати більш повну оцінку всієї кривої ризику. Використовуючи цю структуру, кіберризик можна моделювати в трьох режимах:

– модель на основі даних базується на історичних подіях, якщо дані існують і є стабільними у часі;

– модель на основі сценаріїв використовується для моделювання інцидентів, які ще не відбулися (зазвичай інциденти з великим впливом);

– режим перекриття поєднує модель на основі даних та модель на основі сценаріїв шляхом перекриття кривих ризику, щоб уникнути подвійного підрахунку інцидентів.

Після об’єднання цих трьох режимів особа, яка приймає рішення, отримує повну характеристику кіберризику, з яким стикається організація (рис. 2.1).

Деякі організації можуть мати власні історичні дані про кіберінциденти, які були записані протягом часу. Хоча статистичні дані самі по собі не є достатніми для оцінки кіберризику, деякі висновки можна отримати, проаналізувавши ці дані та використавши їх для створення моделі кіберризику на основі даних. Організації, які не мають офіційної системи відстеження інцидентів, все одно можуть отримати дані з інших джерел. Поширені випадки зараження шкідливим програмним забезпеченням часто реєструються в системі квитків служби підтримки.

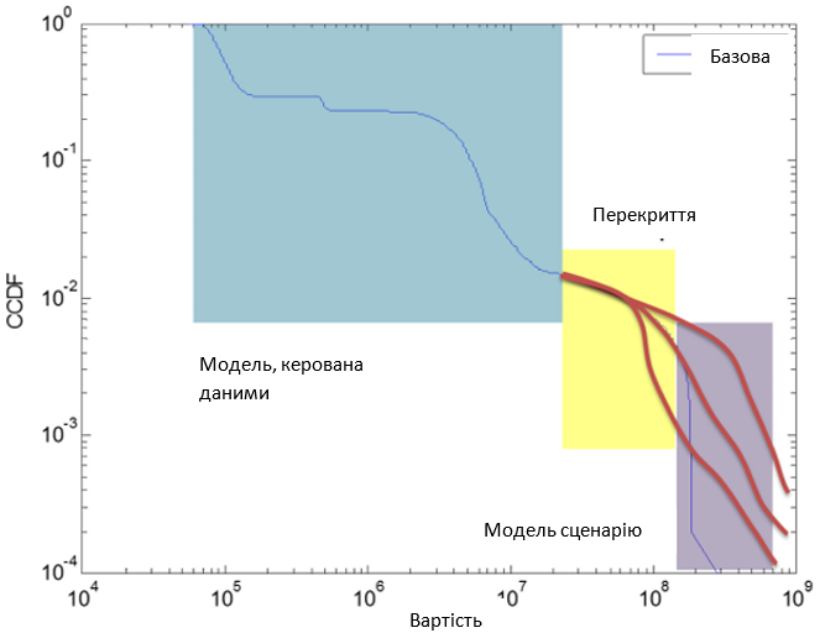



Рисунок 2.1 – Три режими кривої ризику

Інформація з тестів на проникнення, аудитів третіх сторін та від команди безпеки може надати дані, що вказують на рівень вразливості та виправлення.

Поєднання цих джерел інформації часто є достатнім для отримання приблизної оцінки рівня та наслідків різних атак. Крім того, використання розподілів ймовірностей замість точкових оцінок дозволяє особі, яка приймає рішення, врахувати невизначеність щодо цих даних.

Після отримання даних їх необхідно проаналізувати таким чином, щоб можна було розрахувати різні криві ризику в організації. Дуже важливо вибрати відповідний рівень деталізації для моделі кібербезпеки. Існує велика кількість таксономій і фреймворків для кібербезпеки, які фокусуються на зловмисниках, захисниках, векторах, експлойтах або жертвах. Найважливішою особливістю моделі є вибір характеристики, яка є корисною для особи, що приймає рішення.

У роботі для оцінки кібербезпеки в організації використовується модель, що базується на інцидентах. У цій моделі фінансові наслідки кібербезпеки в організації розраховуються як сукупність наслідків багатьох окремих інцидентів кібербезпеки.

Інциденти кібербезпеки в цьому контексті визначаються як події, що документуються аналітиком центру операцій з безпеки. Зауважте, що ці інциденти не обов’язково є кібератаками. Втрата ноутбуків та інциденти витоку даних не

спричинені зловмисними діями, але класифікуються як інциденти кібербезпеки. Це визначення також допомагає прояснити неоднозначний характер сканування портів, яке може бути наслідком розвідки мережі зловмисником або законних дослідницьких проектів, що картографують Інтернет.

Щоб зробити аналіз більш значущим, представлена тут модель базується на інцидентах кібербезпеки, які передбачають певну форму взаємодії з боку захисника. Інциденти кібербезпеки зазвичай реєструються в системах управління інцидентами (IMS). IMS можуть бути офіційно розробленими системами, такими як RSA Archer або Demisto, власними базами даних або навіть інцидентами, випадково зареєстрованими в електронній поштовій скриньці людини.

Системи управління інцидентами відстежують події, що перевищують мінімальний рівень впливу, що робить аналіз набагато кориснішим, ніж шумні дані журналів. Наприклад, про втрату пристрою буде повідомлено, і аналітик проведе опитування співробітника, щоб з'ясувати, як було втрачено пристрій, переконатися, що дані були зашифровані, або розпочати процес повідомлення про розкриття даних. Про інциденти із зловмисними електронними листами повідомляється аналітику з безпеки, який видаляє електронний лист, налаштовує фільтри електронної пошти, щоб запобігти зараженню інших комп'ютерів тим самим електронним листом, і вживає заходів для усунення наслідків у вигляді видалення шкідливого програмного забезпечення з пристрою користувача або перезавантаження паролів.

Інциденти, зареєстровані в IMS, зазвичай вимагають певного розслідування або виправлення. Наприклад, шкідливий електронний лист, який блокується фільтром електронної пошти, може не спричинити створення інциденту, тоді як спроба пошкодження веб-сайту може вимагати ідентифікації IP-адреси зловмисника та додавання її до чорного списку. Визначення того, які події реєструються як інциденти, є суб'єктивним, але протягом тривалого періоду часу зареєстровані інциденти є чудовим показником того, як центр безпеки використовує свій час.

Організації стикаються з багатьма різними загрозами, але часто не можуть розрізнити різних супротивників. Наприклад, важко визначити, чи порт-сканування здійснюється державою чи групою науковців. В інших випадках організації можуть отримати інформацію про зловмисника. Унікальне шкідливе програмне забезпечення, яке раніше не зустрічалося, є ознакою цілеспрямованого зловмисника з розвиненими ресурсами, тоді як фішингові листи, що намагаються викрасти облікові дані веб-пошти, часто надходять від звичайних спамерів. Деяким організаціям може бути корисно розпочати аналіз із складання списку можливих зловмисників. Наприклад, організації, що займаються державною діяльністю, можуть бути більш схильні до атак хактивістів.

Однією з причин, чому кількісні моделі кібербезпеки досі не набули широкого поширення, може бути те, що ці моделі часто є надто деталізованими. Аналітик може швидко заплутатися, моделюючи технічні атаки на веб-сайти, включаючи атаки на перехід по каталогах, SQL-ін’єкції, міжсайтовий скриптинг або спроби брут-форсу . Такий рівень деталізації часто працює проти аналітика, оскільки невизначеність дуже швидко зростає.

На рисунку 2.2 показані різні вектори, використані в цьому аналізі. Необхідно звернути увагу на те, що модель включає інциденти, які не є атаками, але, як правило, підпадають під відповідальність центру безпеки.

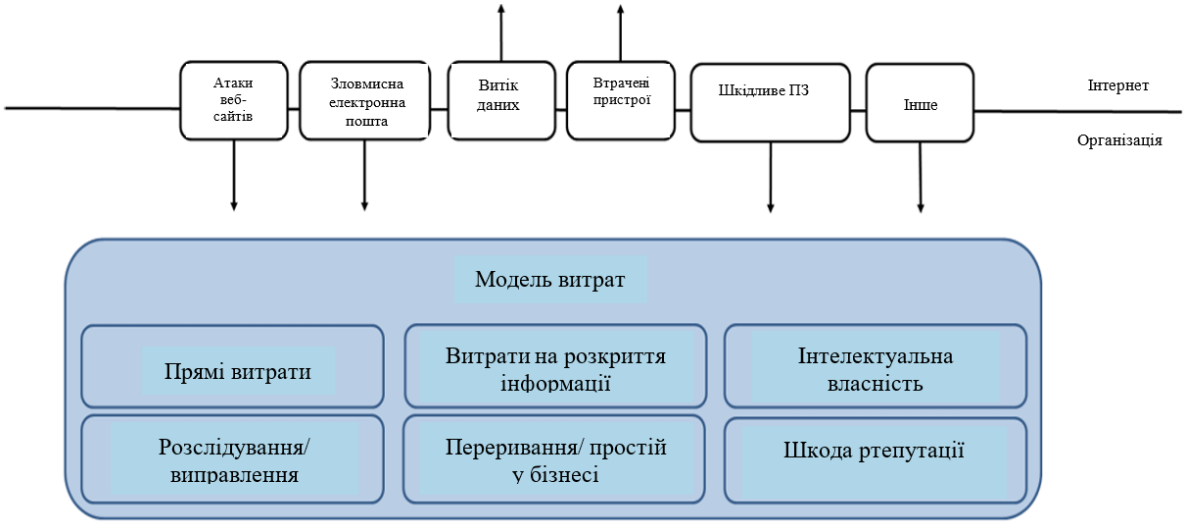



Рисунок 2.2 – Категорії інцидентів кібербезпеки

Зловмисники можуть отримати доступ до мережі через атаки на веб-сайти, шкідливі електронні листи, інциденти з шкідливим програмним забезпеченням та інші вектори атак. Витік даних і втрата пристроїв можуть призвести до витоку даних, хоча зловмисники не отримують доступ до організації через ці вектори. Кожен вектор може спричинити збитки за шістьма типами витрат, кожен з яких моделюється з використанням історичних даних та думок експертів.

У роботі моделюються шість векторів атак:

- витік даних;
- зловмисні електронні листи;
- втрачені або викрадені пристрої;
- інциденти з веб-сайтами;
- інциденти з веб-браузерами та USB;
- інше.

Вимірювання наслідків інцидентів кібербезпеки історично було серйозним викликом. У цій моделі розрізняється серйозність інциденту вимірюється в людино-годинах розслідування та грошові витрати, пов’язані з інцидентом. Наведений тут набір даних містить показник серйозності кожного інциденту, що описує кількість годин, витрачених на розслідування та усунення інциденту.

У моделі використовуються індикаторні функції, щоб інциденти могли спричиняти додаткові грошові витрати, якщо перевищено певний поріг часу розслідування. Це передбачає, що інциденти з низьким рівнем серйозності не спричиняють значних грошових витрат, що відповідає спостереженням за діяльністю організації. Хоча існує ймовірність, що простий штам шкідливого програмного забезпечення, розслідування якого займає п’ять годин, може призвести до мільйонних збитків, такий сценарій не зустрічається в даних. Інциденти, що спричиняють грошові збитки, як правило, розслідуються більш ретельно, іноді з метою підготовки юридичної або аудиторської документації, або через загальний консенсус, що дорогі інциденти заслуговують на більшу увагу.

Фінансові наслідки для організації оцінюються за шістьма типами витрат:

– витрати на розслідування;
– прямі витрати;
– переривання бізнесу;
– пошкодження репутації;
– моніторинг кредитів/повідомлення про порушення;
– втрата інтелектуальної власності.

Організації, які несуть унікальні витрати внаслідок кібератак, можуть вирішити моделювати більше наслідків, що просто передбачає створення нової моделі наслідків. Наприклад, можна додати ще одну категорію, яка кількісно оцінює наслідки втрати стратегічних державних таємниць. Втрата креслень нового винищувача вплине на організацію через цей вектор витрат. Наслідки втрати державних таємниць виходять за межі цієї магістерської роботи.

Для кожного з цих типів впливу створюється підмодель для розрахунку відповідного впливу інциденту. Кожен інцидент завжди спричиняє витрати через час, витрачений на його розслідування. Інші наслідки можуть виникнути залежно від типу інциденту та його тяжкості.

Після моделювання розподілу різних типів атак, їх частоти та впливу, криву ризику на основі даних можна обчислити за допомогою моделювання методом Монте-Карло. Крім того, розподіл вхідних даних може базуватися на історичних даних або сценаріях. Тому інциденти, що моделюються, могли відбутися в минулому, але також можуть бути новими сценаріями, які ще не спостерігалися. Іншими словами, модель Монте-Карло узагальнюється в метод моделювання навіть для інцидентів, які ще не відбулися. Інциденти моделюються із заданою частотою, і кожен інцидент має відповідний вплив, взятий з розподілу. Модель моделює один рік кіберінцидентів, хоча це можна легко змінити. На основі великої кількості прогонів ($n$=10 000) розраховується доповнювальна кумулятивна функція розподілу.

Більш формально визначено наступні терміни для використання в моделюванні:

| *Символ* | *Значення* |
|---|---|
| $C$ | Вартість |
| $I$ | Позначення інциденту |
| $J$ | Позначення типу інциденту (веб-сайт, ел. пошта, шкідливе ПЗ, тощо) |
| $H$ | Години |
| $V$ | Ф-ції індикатора |
| $P_i$ | Ймовірність втрати для інциденту типу і |
| $DC_i$ | Прямі витрати для інциденту типу і |
| $PI_i$ | Втрата конфіденційної $i$-ції для інциденту типу $i$ |
| $RD_i$ | Втрата репутації для інциденту типу $i$ |
| $IP_i$ | Втрата інтелектуальної власності для інциденту типу $i$ |
| $BI_i$ | Втрати від переривання бізнесу для інциденту типу $i$ |

Загальна вартість кіберінцидентів в організації за рік — це просто сума вартості кожного інциденту, що стався.

$$\text{Річна вартість} = \sum_i C_i. \tag{2.1}$$

Загальна вартість кожного інциденту визначається шляхом підсумовування кожної категорії впливу, а саме: витрати на розслідування, прямі витрати, переривання діяльності, шкода репутації, моніторинг кредитоспроможності та втрата інтелектуальної власності. Припускається, що кожна година розслідування коштує 100 доларів, тому кількість годин, витрачених на розслідування інциденту, множиться на 100. У цій моделі робиться спрощене припущення, що витрати є умовно нерелевантними, враховуючи години розслідування. Можуть виникнути певні ситуації, в яких це припущення не спрацьовує, наприклад, коли втрата інтелектуальної власності збільшує ймовірність шкоди репутації. Загальна вартість визначається:

$$C_i = H_i * \$100 + DC_i + BI_i + RD_i + PI_i + IP_i. \tag{2.2}$$

Категорії впливу можуть залежати від типу j інциденту, а вартість інциденту і типу j є функцією годин розслідування інциденту і, розподілу впливу, функцій індикаторів та умовних ймовірностей. Наприклад, вартість інциденту і типу «витік даних» можна записати наступним чином:

$$C_i = H_i * \$100 + RD_i + PI_i. \quad (2.3)$$

В результаті інциденту з витоком даних можуть виникнути лише витрати часу на розслідування, шкода репутації та розкриття конфіденційної інформації. Витрати можна додатково розбити на такі складові:

$$C_i = H_i * \$100 + V(H_i) * (RD_i + PI_i). \quad (2.4)$$

$$V(H_i) = \begin{Bmatrix} 1 \; if \; H_i \geq 500 \\ 0 \quad else \end{Bmatrix}. \quad (2.5)$$

$$PI_i = \{Uniform\ (60k\ to\ 5M)\}. \quad (2.6)$$

$$RD_i = \begin{Bmatrix} Uniform\ (1M\ to\ 2M), & \text{з ймовірністю } 0{,}45 \\ Beta\ Dist\ (100M\ to\ 160), & \text{з ймовірністю } 0{,}05 \\ 0, & \text{з ймовірністю } 0{,}5 \end{Bmatrix}. \quad (2.7)$$

Іншими словами, збитки від шкоди репутації та витрати на інформацію про приватність виникають лише в тому випадку, якщо час розслідування перевищує 500 годин, звідси і походить функція індикатора $V(H_i)$. Якщо це відбувається, з розподілу вибирається випадкова змінна, щоб отримати рівень збитків від інциденту.

Втрати конфіденційної інформації вибираються з рівномірного розподілу, а шкода репутації з кускового, що представляє три типи результатів. Після того як вартість кожного інциденту вибрана з розподілів і обчислена, криву ризику можна отримати шляхом багаторазового моделювання та формування функції розподілу або, в даному випадку, додаткової кумулятивної функції розподілу.

На рисунку 2.3 показано діаграму рішень щодо кібербезпеки в організації та те, як частота, вплив і тип інциденту впливають на загальну вартість.

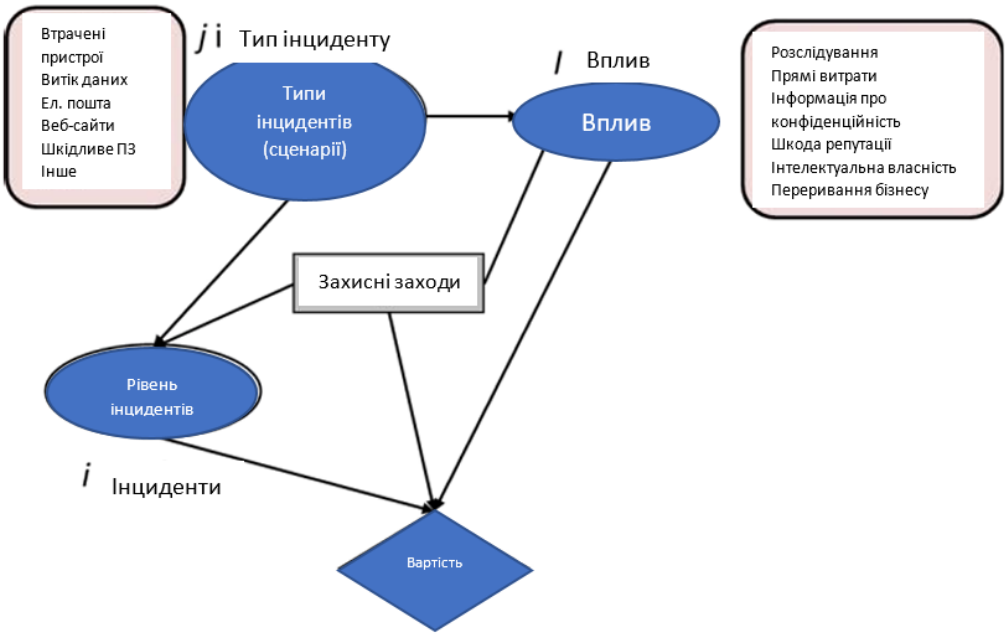



Рисунок 2.3 – Моделювання методом Монте-Карло

Використання моделі, заснованої на інцидентах, є зручним, оскільки деякі невизначеності стають умовно нерелевантними для вартості, враховуючи інформацію про частоту, тип і вплив атак.

## 2.2 Сценарний підхід до моделювання кіберризиків

Важливо підкреслити, що модель, заснована на даних, не обмежується використанням історичних даних про частоту або вплив. Насправді в даних часто трапляються артефакти, які потрібно виявляти, очищати та видаляти. Наприклад, одна організація зафіксувала значне зростання кількості втрачених пристроїв протягом одного місяця, що спотворило очікувану кількість втрачених пристроїв на наступний рік. Після подальшого розслідування було встановлено, що різке збільшення кількості втрачених пристроїв було пов’язане з аудитом, який виявив велику кількість пристроїв, які зникли протягом тривалого періоду часу, але були зареєстровані як втрачені одночасно.

З огляду на цю інформацію, аналітик зміг видалити ці винятки та скласти більш точну оцінку частоти втрати пристроїв. Аналогічно, та сама організація спостерігала постійне зменшення кількості інцидентів із шкідливим програмним

забезпеченням з року в рік. Після обговорення цього питання з CISO аналітик змоделював 10% зниження кількості інцидентів із шкідливим програмним забезпеченням. Аналітик також включив атаки програм-вимагачів, хоча в організації було зареєстровано дуже мало таких атак. На основі галузевих звітів та розмов з іншими компаніями CISO вважав, що атаки програм-вимагачів зростають і будуть відбуватися частіше в наступному році.

Включення зовнішніх знань може бути суб'єктивним, але все одно залишається дуже ретельним. Байєсівські моделі можуть бути побудовані таким чином, щоб ретельно кодувати нові загрози, нові сигнали та докази в симуляції. Особи, що приймають рішення, мають широкий вибір альтернативних джерел даних, що дозволяє побудувати детальну модель, яка базується як на статистичних даних, так і на суб'єктивних джерелах інформації.

Значна частина нашої здатності моделювати кібербезпеку є прямим результатом стабільності інцидентів кібербезпеки, які, як правило, відбуваються з постійною частотою протягом часу і мають розподіл за ступенем серйозності, який еволюціонує в часовому масштабі років. Завдяки цьому багато аспектів кіберсистем можна досить легко моделювати. Наприклад, прості статистичні інструменти можна використовувати для перевірки того, що частота інцидентів витоку даних в одній організації була досить стабільною протягом останніх шести років. Звичайно, це може змінитися, але для певних типів інцидентів може бути доцільним виходити з базової частоти історичних інцидентів.

Після ідентифікації даних їх необхідно включити в модель. Аналітик може використовувати два загальні підходи. Аналітики можуть використовувати історичні дані для отримання параметризованого розподілу або вибірки безпосередньо з історичних інцидентів (бутстрепінг). Кожна техніка має свої переваги та недоліки, але обидві можуть бути корисними залежно від особливостей моделі. У представленій тут моделі я використовую комбінацію параметричного та бутстрепінг-підходів. Наприклад, частота інцидентів аналізується параметрично, тоді як серйозність інцидентів, як правило, моделюється за допомогою бутстрепінгу.

Одним із корисних методів отримання ймовірнісних вхідних даних є пристосування даних до математичної функції, яка використовується як ймовірнісний вхідний параметр моделі. Наприклад, розподіл годин розслідування певних векторів добре моделюється як розподіл за степеневим законом. Тому аналітик може отримати найкраще пристосування і зробити висновок на основі цього розподілу. Аналогічно, частота інцидентів може бути змодельована як пуассонівський процес і характеризуватися одним параметром (лямбда).

Підхід на основі параметризації та моделювання є корисним, оскільки дозволяє особі, яка приймає рішення, моделювати різні заходи безпеки на рівні процесів. Наприклад, частота випадків зловмисних електронних листів може зменшитися завдяки кращій системі фільтрування електронної пошти, тим самим коригуючи частоту випадків (зазначену $\lambda$) до $\lambda(1 - r)$, де r — додаткова частка виявлених випадків. Аналогічно, розподіл за ступенем тяжкості може змінитися з розподілу за степеневим законом з α = 1,2 до α = 1,4, якщо організація впровадить вдосконалені засоби виявлення. Це також дозволяє аналітику відбирати зразки з інцидентів, які є більшими за найбільші інциденти, що були зафіксовані. Це корисно для доповнення аналізу сценаріїв, який використовується для вивчення великих або рідкісних інцидентів, які ще не відбулися.

Параметризація працює дуже добре, якщо явище є відносно простим, але в деяких випадках може давати збій. На рисунку 2.4 показано розподіл часу розслідування інцидентів, пов’язаних із шкідливим програмним забезпеченням.

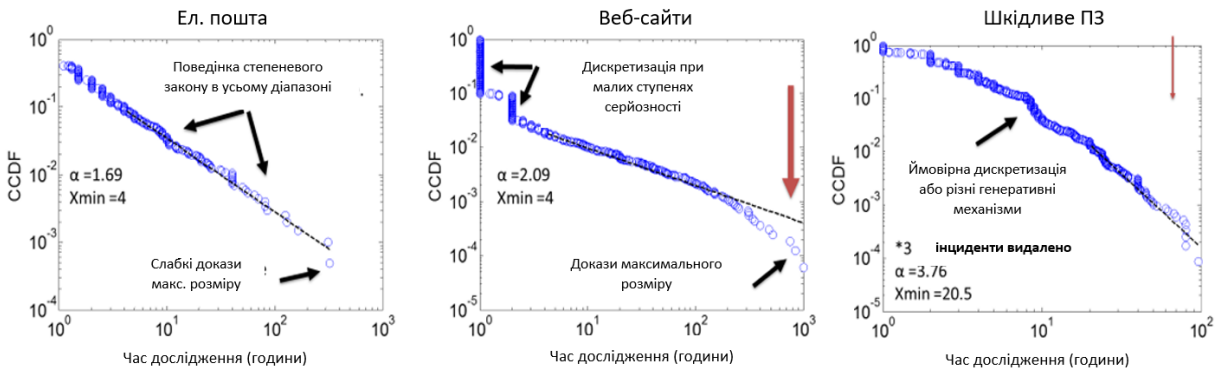



Рисунок 2.4 - Апроксимація кривої даних про кібербезпеку

Важливо, що певні типи інцидентів мають чітку тенденцію (а), тоді як інші типи інцидентів вимагають більш складного моделювання (б). Інші дані можуть призвести до поганої апроксимації через наявність декількох генеративних механізмів, які неможливо розрізнити (в). З графіків (а) і (в) видалено винятки, щоб поліпшити загальну апроксимацію моделі.

Загалом, параметризація вхідних даних забезпечує більш рівномірний розподіл вибірки, дозволяє створювати більш досконалі моделі захисту та екстраполювати дані на інциденти, які ще не відбулися, але також може значно ускладнити модель.

Підхід на основі бутстрепінгу передбачає використання бутстрепінгу, або безпосереднього відбору зразків з інцидентів. Цей метод значно простіший у використанні, оскільки не вимагає підгонки кривої. Історичні дані все одно можна скоригувати за допомогою простого правила або за допомогою аналізу.

Недоліком підходу бутстрепінгу є те, що можуть мати місце деякі ефекти дискретизації, особливо у випадку інцидентів високої тяжкості. У моделюванні можна відбирати лише інциденти, що відбулися в минулому, а інциденти високої тяжкості часто трапляються рідко.

Бутстрепінг дозволяє уникнути більш складних моделей, що виникають при параметричному підході, але призводить до нечисленних зразків інцидентів великої тяжкості.

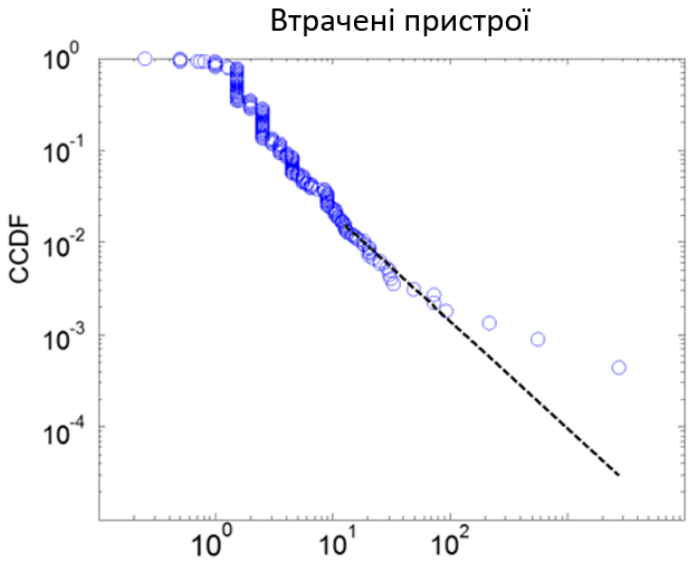



Рисунок 2.5 - Бутстрепінг даних про кіберінциденти

Загалом, бутстрепінг є дуже простим методом і може бути більш точним, якщо розподіл розслідувань є складним. Однак він має обмеження в тому сенсі, що може враховувати лише історично зафіксовані інциденти.

Включення моделі витрат є ще одним важливим завданням. Витрати можуть просто нараховуватися пропорційно до кількості годин розслідування або включати індикаторну функцію для врахування інших факторів. Таким чином, витрати можуть бути пов'язані або роз'єднані в тому сенсі, що вони можуть бути обмежені для включення інших факторів, таких як шкода репутації та витрати на переривання бізнесу, або включати тільки одне або інше.

У будь-якому випадку доцільно розділити інциденти на низький рівень, де час розслідування є єдиною грошовою вартістю, та високий рівень, де можуть виникнути додаткові грошові витрати. Бажано, щоб додаткові витрати відповідали високому часу розслідування, оскільки це підтверджується емпіричними спостереженнями. Було б несподівано, якби розслідування інциденту зайняло лише 10 годин, але коштувало мільйони. Тому перевагу слід надавати індикаторній функції. Наприклад, особа, яка приймає рішення, може вирішити включити шкоду репутації з індикаторною функцією I як функцію часу розслідування V таким чином, що $I(V) = \begin{cases} 1 & if \quad V \geq 200 \\ 0 & else \end{cases}$, це означає, що репутація пошкоджується лише в тому випадку, якщо час розслідування досягає 200 годин.

Історичних даних недостатньо для оцінки всієї кривої ризику, оскільки певні інциденти можуть ще не відбутися, або через те, що не минуло достатньо часу, або через те, що кібербезпека є сферою, яка постійно розвивається, з адаптивним супротивником. У таких випадках можна моделювати та оцінювати різні класи сценаріїв, використовуючи експертні оцінки ймовірностей, інженерні дані, випадки, що ледь не призвели до аварій, та інші джерела інформації. Мета цього розділу - описати, як можна обчислити частоту та наслідки для кожного сценарію, які потім використовуються як вхідні дані для моделювання за методом Монте-Карло з метою отримання сценарієвої моделі загальної кривої ризику. У деяких випадках вхідні дані можуть бути повністю засновані на даних, тоді як в інших

випадках, коли даних немає, використовуються виключно сценарії. Деталі моделі сценарію також залежать від того, який сценарій розглядається, і залежно від того, як оцінюється сценарій, можуть бути замінені різні інструменти моделювання. У цьому розділі представлено модель сценарію для вирішення проблеми ризику проникнення представників національних держав в організацію та викрадення інтелектуальної власності або порушення діяльності.

Кожен сценарій має вплив на організацію. Ці впливи належать до тих самих категорій впливу, що описані в моделі на основі даних, але можуть вимагати додаткового спеціального підходу. Деякі сценарії можуть виходити за межі звичайних кібервпливів, що означає необхідність ретельного аналізу серйозних наслідків. Іншим важливим аспектом є часовий характер виявлення вторгнення. Багато вторгнень у мережу виявляються лише через кілька тижнів або місяців після того, як зловмисник отримав доступ до системи. Ця добре відома статистика підкреслює важливість швидкого виявлення, оскільки організації іноді можуть вжити швидких заходів, що обмежують серйозність інциденту.

Загальна структура моделі для сценаріїв складається з трьох частин: ймовірності, функції втрат та ставки дисконту, заснованої на часі виявлення. Ймовірність розраховується шляхом моделювання кожного сценарію як послідовності дискретних кроків, які повинні відбутися, щоб супротивник досяг певної мети. Кожен сценарій починається з події-ініціатора, такої як зловмисний електронний лист, атака на веб-сайт або клік на зловмисну веб-сторінку. Атака може прогресувати, стаючи все більш серйозною, якщо захисник не в змозі заблокувати, виявити або виправити зловмисну дію. Кожен крок у прогресії атаки має умовні ймовірності, пов’язані з шляхом атакуючого, який може включати успіх або виявлення. Тому ймовірність кожного сценарію і можна записати як:

$$p(outcome_i) = P(IE_i) * P(A_i|IE_i) * P\left(B_i\middle|A_{i,}\, IE_i\right) \dots * P\left(Z_i\middle|A_{i,}B_{i,} \dots Y_{i,}IE_i\right), \quad (2.8)$$

де $IE_i$ є початковою подією сценарію $i$,

$A_i,\ B_i, Z_i\ldots$ позначають додаткові кроки, які супротивник повинен виконати для досягнення своєї мети.

Функція втрат для кожного сценарію має ту саму форму, що й функція втрат, яка використовується в моделюванні Монте-Карло для моделі, що базується на даних, і складається з витрат на розслідування, прямих витрат, переривання діяльності, шкоди репутації, моніторингу кредитоспроможності та втрати інтелектуальної власності. Використовуючи ту саму нотацію:

$$C_i = H_i * \$100 + DC_i + BI_i + RD_i + PI_i + IP_i. \qquad (2.9)$$

Тут функції витрат знову вважаються умовно незалежними, враховуючи час розслідування, хоча в деяких ситуаціях можуть бути залежності. Наприклад, перебої в роботі бізнесу можуть збільшити ймовірність шкоди репутації.

Виявлення супротивника також потрібно моделювати, оскільки швидке виявлення може обмежити вплив певних сценаріїв. З цією метою вводиться функція коефіцієнта виявлення $Di(t)$, яка задається як:

$$D_i(t) = (1 - e^{-t}). \qquad (2.10)$$

Коефіцієнт виявлення позначає момент виявлення атаки, який множиться на вартість інциденту, щоб зменшити його вплив. Якщо атака виявлена негайно, то вартість стає рівною 0, оскільки $D_i(t = 0) = 0$. Якщо атака не виявляється протягом багатьох років, то виникають повні витрати, оскільки $D_i$(t = ∞) =0. На практиці для коефіцієнта виявлення можна використовувати більш складні функції, але експоненціальний аргумент демонструє метод для цього випадку. Поєднання функції втрат і коефіцієнта виявлення дає загальне рівняння для втрат, пов’язаних зі сценарієм *i*.

$$C_i(t) = (H_i * \$100 + DC_i + BI_i + RD_i + PI_i + IP_i) * D_i(t). \qquad (2.11)$$

На цьому етапі ймовірність і вартість сценарію і можуть бути введені в симуляцію Монте-Карло для отримання режиму кривої ризику на основі сценарію.

Спочатку необхідно змоделювати систему. Згідно з оцінками експертів, атаки з боку національних держав найчастіше здійснюються за допомогою електронної пошти або мережі. Інші події, що можуть стати причиною атаки, можна змоделювати окремо, а деякі події не можуть призвести до певних сценаріїв. Після визначення подій, що ініціюють, систему необхідно змоделювати, щоб визначити послідовність кроків, які противник повинен виконати для досягнення своєї мети. Це включає моделювання існуючих системних заходів безпеки.

Отримавши доступ до основної мережі, зловмисник може або шукати інтелектуальну власність, або намагатися отримати доступ до інфраструктури місії. Бічне переміщення відбувається в процесі, під час якого зловмисник намагається дізнатися про внутрішню структуру мережі, включаючи те, як підключені пристрої та які з них мають вразливі місця, які можна використати. Зловмисник може провести сканування, щоб побачити, які пристрої відкриті, або зробити запит до каталогів, щоб отримати список доступних файлів (рисунок 2.6).


Рисунок 2.6 - Бутстрепінг даних про кіберінциденти

Ці дії пов’язані з ризиком виявлення, залежно від рівня кваліфікації захисника. Зловмисник також може зіткнутися із застоєм. Іншими словами, можливо, що зловмисник не може проникнути глибше в систему, але ще не був виявлений. У таких випадках він може продовжувати перебувати в мережі і

повторити спробу вторгнення в майбутньому, або просто відмовитися від спроби злому.

Хоча конфіденційні дані можуть зберігатися в основній мережі, отримати доступ до комунікаційних серверів, які підключаються до космічного апарата, набагато складніше. Щоб отримати доступ до цієї частини мережі, зловмиснику, ймовірно, доведеться викрасти облікові дані. Отримавши доступ до цих машин, зловмисник повинен буде встановити зв'язок із космічним апаратом, відправити команди та переконатися, що ці команди були успішно отримані та виконані.

На рисунку 2.7 показано серію кроків, які супротивник повинен виконати, щоб досягти різних результатів.

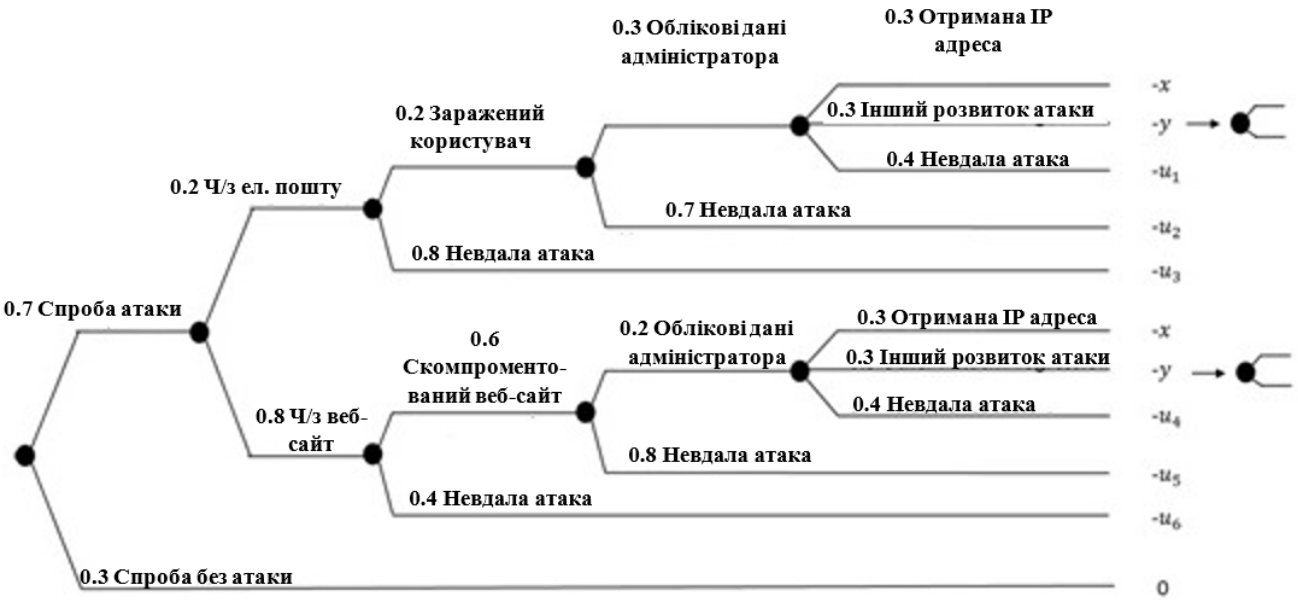



Рисунок 2.7 - Послідовність атак на Space Corp

Імовірності, показані в дереві подій, є реалістичними цифрами, але не походять з експертних джерел або даних. Потрібно звернути увагу, що ця послідовність атак надає кілька можливостей для перевірки моделі. Наприклад, розраховану швидкість проміжного кроку компрометації користувача або веб-сайту можна порівняти з історичними даними. Ці спостереження можна використовувати для калібрування загальної ймовірності атаки, оскільки кілька кроків на цьому шляху вже виконано, навіть якщо остаточні кроки ще не виконано. Іншими словами, результат цієї моделі дає не тільки ймовірність крадіжки

інтелектуальної власності або збою супутникової мережі, але й ймовірність інцидентів, що ледь не призвели до збою, наприклад, ймовірність отримання доступу до мережі місії за одиницю часу (у цьому випадку за тиждень).

На основі рисунка 2.7 можна обчислити ймовірність кожного сценарію. Наприклад, ймовірність крадіжки інтелектуальної власності становить:

$$P(\text{отримана IP адреса}) = P(\text{спроба атаки}) * [P(\text{через ел. пошту}) * P(\text{заражений користувач}) P(\text{облікові дані адміністратора} \mid \text{електронна пошта}) * P(\text{отримана IP адреса}) + P(\text{ч/з веб сайт}) * P(\text{компроментований веб-сайт}) * P(\text{облікові дані адміністратора} \mid \text{веб} - \text{сайт}) * P(\text{отримана IP адреса})] = 0{,}0227.$$

Імовірність крадіжки інтелектуальної власності на тиждень становить 0,0227, що приблизно дорівнює одному випадку крадіжки інтелектуальної власності на рік. Це дещо вища частота, ніж та, що спостерігалася в Space Corp в минулому (приблизно один випадок крадіжки інтелектуальної власності кожні шість років).

На рисунку 2.8 показано діаграму впливудля розрахунку ймовірності крадіжки інтелектуальної власності.

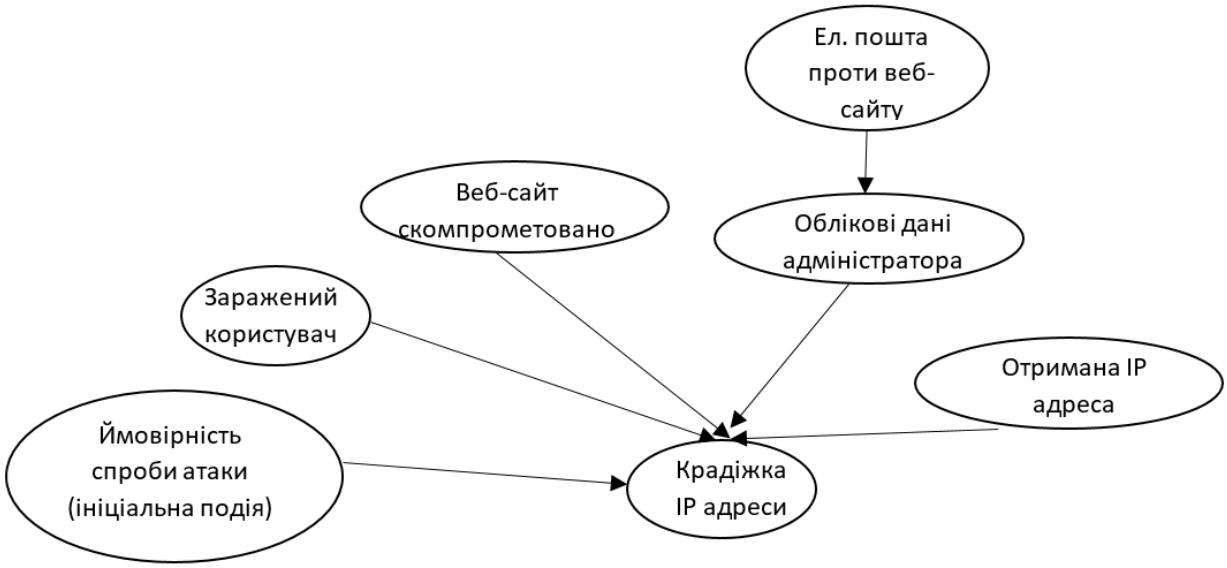



Рисунок 2.8 - Діаграма впливу для сценаріїв у Space Corp

На рисунку 2.9 показано розвиток атаки, який може відбутися, якщо зловмисник продовжить не будучи виявленим.

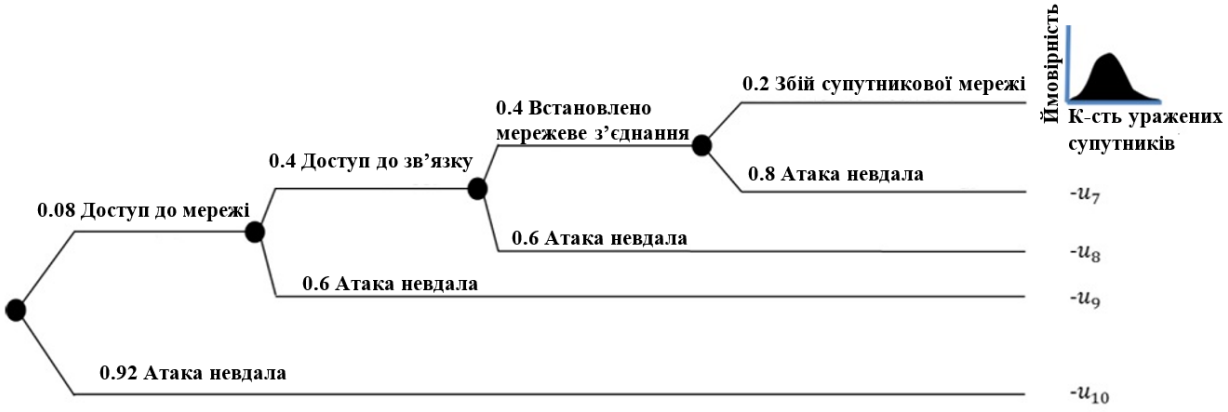



Рисунок 2.9 - Послідовність атаки на мережу супутників

Імовірність виходу з ладу супутникової мережі розрахована як 0,000058, або приблизно раз на триста років. Аналізуючи хід атаки, стає зрозуміло, що ключовим етапом є перехід до мережі місії, враховуючи, що адміністративні облікові дані вже отримано. Така низька ймовірність відповідає заходам безпеки, які застосовує організація і які ускладнюють перехід з однієї мережі до іншої. Додатковий моніторинг безпеки (захист системи), встановлений на вході в мережу місії, може ще більше зменшити ймовірність успішної атаки, що означає, що розвиток атаки залежить як від навичок супротивника, так і від реакції системи.

Нова інформація може змінити ці умовні ймовірності, що призведе до підвищення ймовірності сценарію. Наприклад, якщо відбудеться кілька випадків, коли супротивники отримають доступ до мережі місії після компрометації облікових даних адміністратора, то вхідні дані моделі потрібно буде оновити, щоб відобразити цю нову інформацію.

Основний процес поєднання моделі на основі даних із моделлю на основі сценаріїв передбачає накладення обох кривих впливу в проміжній області. Це, по суті, калібрує модель на основі сценаріїв, пов'язуючи частоту інцидентів, виявлених в організації, з результатами аналізу сценаріїв, і забезпечує орієнтир для інцидентів із великим впливом.

У представленому аналізі розглядається лише один сценарій. При розгляді декількох сценаріїв необхідно змоделювати взаємозалежності між ними. Якщо супротивник здатний отримати інтелектуальну власність, тоді є ймовірність того, що він зможе отримати доступ до інших частин мережі і, отже, заподіяння шкоди бути більшою.

Один із методів накладання цих моделей передбачає ретельне відокремлення історичних випадків крадіжки інтелектуальної власності та порівняння лише цих випадків із сценарієм моделі. У цьому випадку дві криві можна належним чином накласти одна на одну, а для отримання найкращого результату можна використати метод найменших квадратів. Це може передбачати зміщення кривої сценарію моделі, що можна інтерпретувати як застосування коефіцієнта корекції ймовірності, який нормалізує ймовірність інцидентів із великим впливом.

Після накладання двох моделей можна вибрати довільну точку відсікання для переходу між двома моделями. Незначна зміна точки переходу не матиме істотного впливу на розподіл ризиків, оскільки незначна зміна точки переходу призведе до такої самої поведінки, враховуючи, що моделі накладаються одна на одну. На рисунку 2.10 показано остаточну криву ризику для інцидентів з електронною поштою в Space Corp з використанням вищезазначеної умовної моделі сценарію.

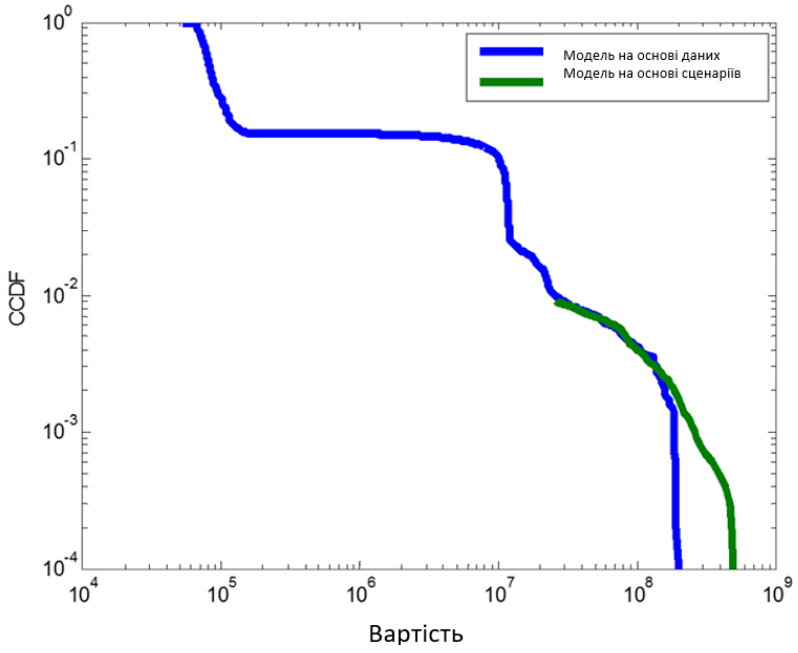



Рисунок 2.10 - Остаточна крива ризику

Після аналізу кожного типу інцидентів можна порівняти результати кожного модельованого року. Нижче показано типовий результат, який відображає щорічні витрати, пов’язані з декількома різними векторами, які сортуються за допомогою додаткової кумулятивної функції розподілу, щоб особа, яка приймає рішення, могла чітко бачити, як часто трапляються збитки певного розміру.

Зауважимо, що втрачені пристрої коштують приблизно однакову суму щороку, тоді як інші типи інцидентів мають великий діапазон збитків. Веб-сайти становлять найбільший ризик для організації та найбільше впливають на криву.

Існує кілька методів порівняння альтернатив. Імовірнісна домінантність є одним з найпростіших. Наприклад, якщо максимальні втрати через втрату пристроїв із повним шифруванням диска менші за мінімальні втрати через втрату пристроїв без повного шифрування диска, то альтернатива з повним шифруванням диска є стохастично домінуючою. Домінування першого порядку виникає, коли CCDF одного вектора завжди менший за інший (наприклад, CCDF витоку даних завжди менший за CCDF веб-сайту на рисунку 2.11).

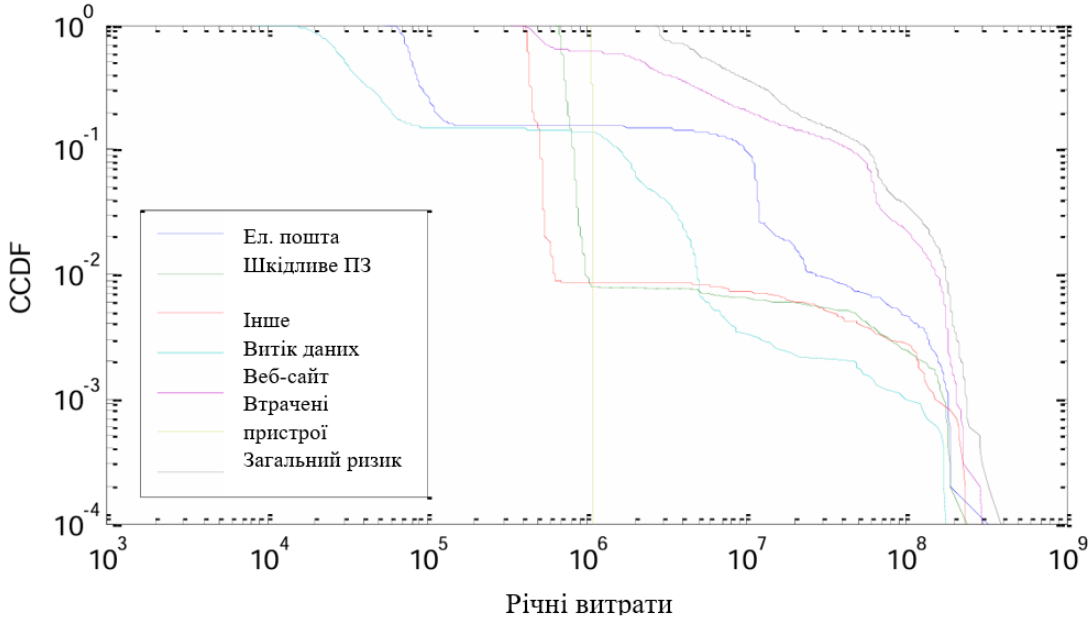



Рисунок 2.11 - Типова крива кіберризиків

Щоб отримати фактичну вартість кожної альтернативи, необхідно з’ясувати ставлення до ризику особи, яка приймає рішення. Ставлення до ризику відображає компроміс між різними втратами та невизначеністю, що означає, що особа, яка приймає рішення і є несхильною до ризику, оцінить невизначену угоду з позитивними вигодами нижче за її очікувану вартість. Оскільки багато розподілів результатів у сфері кібербезпеки мають важкі хвости, особи, які приймають рішення, повинні бути особливо обережними при використанні кривої корисності, яка точно відображає їхні переваги при великих втратах. Оскільки ставлення до ризику є добре розробленою темою, вона не акцентується в цій магістерській. Натомість ця робота зосереджується на інтуїтивних висновках, які можна зробити на основі кривих ризику (CCDF).

Після отримання кривих ризику та значень аналітики можуть вибрати один із декількох способів повідомлення результатів. Деякі організації вважають за краще перевести результати у якісний формат (низький, середній або високий ризик). Інші можуть використовувати медіану або 10-й, 50-й і 90-й процентилі. У будь-якому випадку, розрахунок і представлення розподілу ймовірностей щорічних збитків є важливим, оскільки це дає найбільш повне уявлення про збитки. Якщо особи, що приймають рішення, хочуть спростити аналіз, то перехід від кривої ризику до середнього значення, медіани або іншого показника є тривіальним.

Аналітики повинні бути обережними, щоб спрощення кривої ризику не вплинуло на цілісність результатів. Одним із можливих спрощень є використання вартості під ризиком (VaR). Вартість під ризиком може вводити в оману, оскільки її назва має інше значення, ніж насправді, і вона не дозволяє повною мірою відобразити важкі хвости. Вартість під ризиком часто помилково трактують як максимальний збиток. Наприклад, VaR у розмірі 10 мільйонів доларів інтерпретується як 10 мільйонів доларів, які знаходяться під ризиком і можуть бути втрачені, але не більше. Насправді VaR визначає збитки за певним процентилем (наприклад, 95-м процентилем). Вартість під ризиком у розмірі 10 мільйонів доларів означає, що з імовірністю 0,95 річні збитки будуть меншими за 10 мільйонів доларів.

Інші показники намагаються пом’якшити цю проблему за допомогою використання хвостової вартості ризику. Організації повинні оцінити ці різні показники і вибрати найкращий варіант для своїх потреб, а також подбати про точне донесення значення і результатів аналізу.

## 2.3 Байєсівський підхід до інтеграції факторів кіберризику

Модель, представлена для Space Corp, може бути розширена до загальної моделі для оцінки кіберризиків у будь-якій організації. На рисунку 2.12 показано діаграму прийняття рішень щодо кібербезпеки в організації.

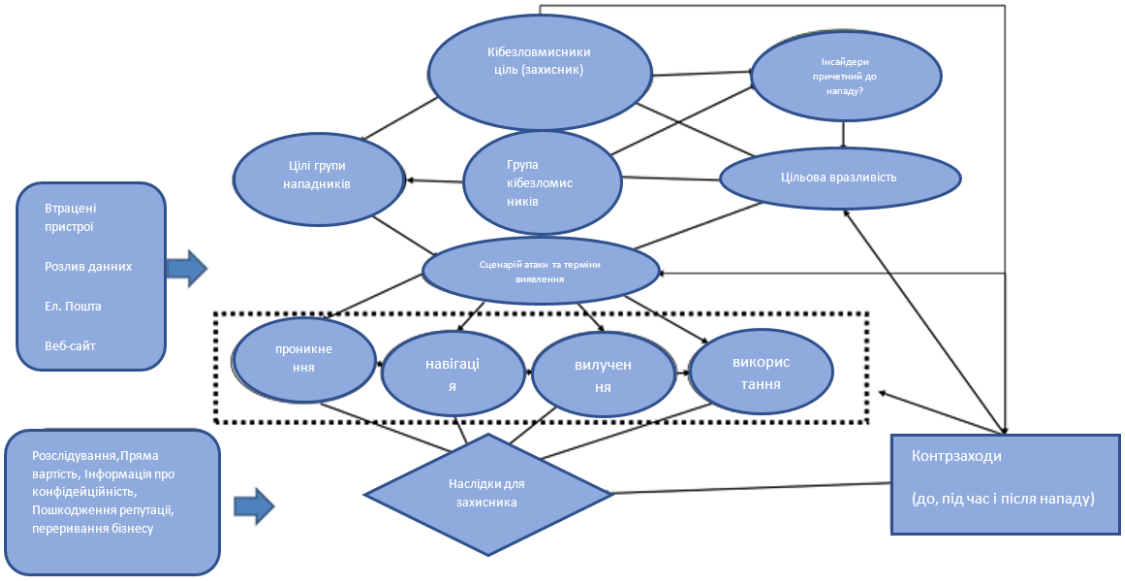



Рисунок 2.12 - Діаграма прийняття рішень щодо кібербезпеки

Конкретні загрози, вразливості та наслідки будуть змінюватися залежно від того, яка організація аналізується, але загальний процес моделювання буде однаковим.

Діаграма містить п’ять груп пов’язаних між собою вузлів, які оцінюють різні аспекти кібербезпеки організації. Перша група стосується супротивників, з якими стикається організація, та деталей оборонних заходів в організації. Друга група

підсумовує різні класи сценаріїв того, як можуть відбуватися атаки або інциденти в організації.

Наприклад, процес атаки моделюється як проникнення в систему, навігація по системі, вилучення інформації та використання даних. Також розглядаються контрзаходи, враховуючи, що організації можуть вживати заходів для обмеження успішності інциденту. Нарешті, наслідки перетворюють ефект атаки на грошові збитки різних типів.

Аналіз проводиться з точки зору організації (захисника). Багато частин моделі залежать від особливостей організації, яка аналізується. Галузь, розмір та місцезнаходження захисника впливатимуть на ймовірність того, що він стане ціллю. Модель також повинна бути адаптована до технічних специфікацій організації. Наприклад, внутрішня структура мережі, вразливість периметра мережі та можливості виявлення впливають на ймовірність успіху кібератаки. Деякі з цих деталей є непевними або невідомими для організації. Точна кількість вразливостей може бути невизначеною через постійне зростання вразливостей програмного забезпечення. Організації також можуть мати вразливості, про які вони не знають, як це часто буває в старих мережах. Організаційні зміни можуть призвести до неправильних налаштувань, які також спричиняють вразливість мережі, яку важко виявити. Одним із перших кроків у моделюванні кіберризиків є збір інформації про ці невизначеності.

Організації також повинні дізнаватися про своїх зловмисників. Великі роздрібні організації стикаються з загрозами з боку злочинців і одиночних хакерів, але рідко стають мішенню для супротивників на рівні національних держав. З іншого боку, виробники можуть стикатися з атаками, спрямованими на крадіжку їх інтелектуальної власності. Широкий спектр витончених методів зловмисників означає, що вивчення загроз, з якими стикається організація, має вирішальне значення для розуміння її загального ризику та визначення найбільш економічно ефективних засобів захисту.

Далі організації повинні зрозуміти можливі сценарії атак. Зловмисники зазвичай дотримуються стандартного процесу високого рівня для отримання

доступу до системи, який включає розвідку мережі, проникнення, латеральне переміщення, підвищення привілеїв, витік даних та використання даних. Організації повинні розуміти ці етапи атак та існуючі засоби захисту, які можуть їх виявити або перешкодити їм. Невизначеність щодо цих дій відображається у вузлі сценарію атаки. Зрештою, особа, яка приймає рішення, в основному стурбована фінансовими втратами, пов'язаними з інцидентами кібербезпеки. Ці втрати включають усі наслідки, спричинені атакою, включаючи переривання бізнесу, шкоду репутації, ремонт або заміну обладнання та інше. Щоб визначити остаточний вплив, особа, яка приймає рішення, повинна знати, які інциденти сталися і скільки коштує кожен з них. У моделі це відображається вузлом наслідків та вузлом частоти. Якщо існують певні типи даних, наведена вище діаграма прийняття рішень може бути ще більше спрощена. На рисунку 2.13 показано модифіковану діаграму для випадку, коли існують деякі історичні дані. У цій ситуації можна спостерігати частоту інцидентів та розподіл наслідків, що означає, що інформація про зловмисника та організацію не має значення для вартості, оскільки частота та наслідки відомі.

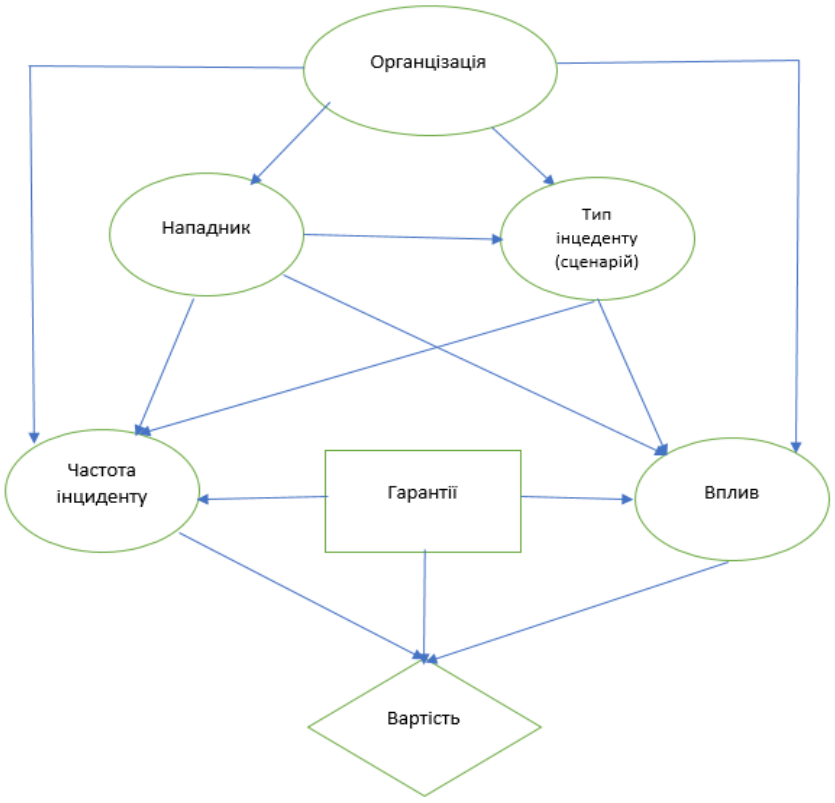



Рисунок 2.13 - Модифікована діаграма рішень

Кількісні моделі ризику вимагають більше вхідних даних і зусиль, ніж інші методи оцінки ризику, але є значно ефективнішими. Аналітики можуть перевірити свої припущення за допомогою аналізу чутливості, який дозволяє визначити, які змінні є найважливішими, оцінюючи надійність остаточного рішення. Розрахунки вартості інформації можуть запобігти надмірним витратам організацій на дорожчі тести на проникнення, які можуть не принести жодної користі. На рівні керівників служб інформаційної безпеки це дозволяє оптимально розподіляти ресурси в умовах невизначеності. Кількісна оцінка кіберризиків також покращує комунікацію щодо ризиків на рівні правління. Кіберризики стають більш переконливими для осіб, що приймають рішення, коли їх можна виразити в грошовому еквіваленті. Багато правлінь розглядають кібербезпеку якісно інакше, ніж інші бізнес-ризики, використовуючи спеціальні інструменти та якісні шкали, що заважають точному порівнянню різних типів бізнес-ризиків. Переклад кіберризику в грошові результати покращує обговорення кіберризику та може забезпечити вирішення цього питання. Нарешті, кількісний кіберризик вже стає критично важливим інструментом для кіберстраховиків. PRA стане важливим інструментом для точної оцінки кіберризиків.

# 3. ПРАКТИЧНЕ ЗАСТОСУВАННЯ МОДЕЛЕЙ КІЛЬКІСНОЇ ОЦІНКИ КІБЕРРИЗИКІВ

## 3.1. Налаштування та адаптація моделі

Щоб продемонструвати, як працює модель, було представлено приклад з практики, адаптований до великої організації.

Кількісна оцінка наслідків інцидентів у сфері кібербезпеки також є складним завданням. Деякі витрати є цілком зрозумілими, наприклад, моніторинг кредитів у разі розкриття конфіденційної інформації. Однак набагато складніше оцінити кількісно такі наслідки, як вихід з ладу космічного апарата внаслідок вторгнення в мережу, втрата конфіденційної інформації, шпигунство за інженерними методами та шкода репутації. Високий рівень ризику космічних місій робить кількісний аналіз ризиків критично важливим інструментом для осіб, що приймають рішення.

Дані про інциденти кібербезпеки, використані в цьому прикладі, походять від великої організації, що базується в США, яка зафіксувала понад 60 000 інцидентів кібербезпеки за шестирічний період. Хоча між фактичним джерелом даних і Space Corp існують значні відмінності, дані використовуються в цьому прикладі для ілюстрації процесу управління ризиками від початку до кінця. Крім того, у всіх прикладах використовуються загальнодоступні дані, а також оцінки експертів. Ці оцінки експертів були отримані за допомогою двох сценаріїв збору інформації. Деяким експертам було надано опис Space Corp і запропоновано надати оцінки, виходячи з припущення, що вони насправді працювали для Space Corp. Інших експертів попросили надати оцінки для їхніх власних організацій. У другому випадку оцінки можуть бути дещо змінені або заплутані перед тим, як їх використовувати як приклади для Space Corp. Результатом цих оцінок є реалістичне моделювання, яке відображає деякі реальні приклади, що були виконані з іншими організаціями.

## 3.2. Комплексна оцінка ризику витоку даних та аналіз наслідків

Першочергово організація поділяє інциденти кібербезпеки на кілька сценаріїв атак. Крім того, моделюється та оцінюється цінність чотирьох основних засобів захисту, а саме запобігання втраті даних, двофакторна автентифікація, демілітаризована зона для веб-сайтів та повне шифрування диска.

Запобігання втраті даних (DLP) – це тип програмного забезпечення, яке контролює дані в мережі. Конфіденційні дані можна ідентифікувати, шукаючи файли, позначені класифікаціями, або контролюючи відповідні формати даних. DLP може бути ефективним захистом від ненавмисного розкриття даних.

На жаль, технологія DLP має кілька недоліків, зокрема, нешкідливі файли можуть бути позначені як конфіденційні, а конфіденційні файли - як нешкідливі. Крім того, зловмисник все одно може досить легко викрасти інформацію, наприклад, зашифрувавши її перед передачею за межі організації.

Двофакторна автентифікація – наразі Space Corp вразлива до зловмисників, які викрадають облікові дані користувачів. Дослідження показують, що рівень успішності фішингу є відносно високим (10–20 %), що означає, що зловмисник може досить легко отримати облікові дані. Ці облікові дані потім можуть бути використані для доступу до електронної пошти або інших додатків, що може призвести до спаму, крадіжки конфіденційної інформації або переходу до інших систем в організації. Двофакторна автентифікація підвищує рівень безпеки, вимагаючи від користувача введення пароля та одноразового токена безпеки для отримання доступу до програми. Наполегливі зловмисники все ще можуть використовувати хитрі атаки для отримання доступу до систем, однак TFA значно підвищує рівень складності.

DMZ для веб-сайтів – атаки на веб-сайти відбуваються часто і мають різний рівень серйозності, що робить їх високим ризиком для Space Corp. У мережі широко використовується застаріле обладнання, а незалежні дослідницькі групи створили незалежні сервери, що призвело до створення гетерогенного середовища. Крім того, багато веб-додатків не підтримуються, оскільки багато проектів не

мають фінансування після їх завершення. Перенесення всіх веб-сайтів до DMZ дозволило б консолідувати ресурси веб-сайтів в одному центральному місці, що значно спростило б управління патчами та моніторинг. Крім того, DMZ знаходиться в сегментованій частині мережі, тому зловмисник не може легко переміститися в інші частини мережі, якщо веб-сервер буде скомпрометований.

Повне шифрування диска – одним з найпоширеніших сценаріїв інцидентів є втрата незашифрованих даних на ноутбуках. У разі втрати або крадіжки ноутбука зловмиснику легко відновити незашифровані дані з пристрою. Повне шифрування диска захищає інформацію на пристрої, вимагаючи введення пароля перед завантаженням ком'ютера. Компанія Space Corp вже впровадила повне шифрування диска, але хотіла б оцінити його ефективність. Також буде оцінено переваги інших засобів захисту від втрати пристроїв, включаючи програмне забезпечення для відновлення активів , навчання з питань запобігання крадіжкам та програми позики ноутбуків.

Щоб визначити цінність кожного з вищезазначених заходів безпеки, необхідно ретельно змоделювати частоту та вплив кібератак, а також ефективність кожного заходу кібербезпеки. У наступних розділах описано цей процес для кожного типу атак.

Кіберзбитки часто виникають через помилки користувачів. Зокрема, інформація може бути ненавмисно розкрита, що призведе до витрат на моніторинг кредитоспроможності або шкоди репутації. Організації класифікують такі інциденти як витік даних. Тип розкритої інформації може включати особисті дані або конфіденційну інформацію, таку як секретна інформація або інтелектуальна власність. Існує кілька причин витоку даних.

Помилка привілеїв: користувачі можуть отримати несанкціонований доступ до матеріалів через неправильну конфігурацію або помилки привілеїв. Наприклад, дослідницькі групи можуть зберігати інформацію на сайті SharePoint, але елементи управління можуть бути неправильно налаштовані, що дає іншим дослідникам доступ до матеріалів.

Необізнаність: користувачі можуть ділитися конфіденційними матеріалами з неавторизованими особами, оскільки вони не знають, що матеріал є конфіденційним або що користувач не має дозволу на роботу з цим матеріалом. Наприклад, працівник відділу кадрів, який намагається зібрати імена, адреси та дати народження співробітників, може надіслати електронною поштою документ Excel великій групі людей із проханням перевірити їхню інформацію.

Помилки: навіть якщо користувачі добре поінформовані про правила, а системи налаштовані належним чином, все одно можуть траплятися випадки витоку даних. Користувачі забувають забрати документи з принтера, або користувач може забути натиснути кнопку «шифрування» під час надсилання електронного листа з номерами соціального страхування.

Інциденти витоку даних мають великі відмінності за масштабами: від надсилання одній особі неправильної податкової форми до надсилання вкладення, що містить 10 000 номерів соціального страхування, на неправильну адресу. Витрати, пов’язані з інцидентами витоку даних, також можуть варіюватися залежно від багатьох потенційних наслідків. Інциденти необхідно розслідувати, щоб визначити масштаби витоку.

Інциденти витоку даних можуть бути дуже складними і складатися з декількох подій, які важко моделювати як ланцюжок подій. На рисунку 3.1 представлено механізми витоку даних, а також витрат і заходів безпеки.

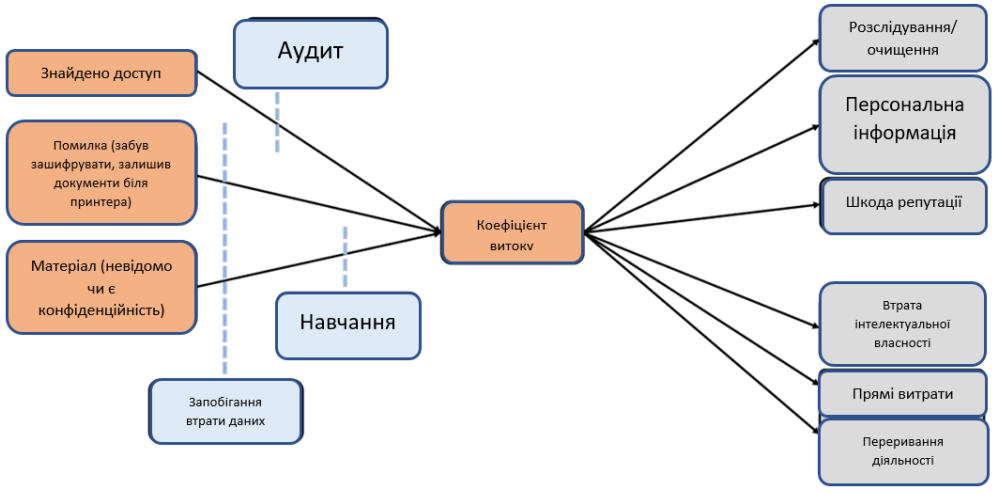



Рисунок 3.1 - Механізми витоку даних, витрат та заходів безпеки

Зауважимо, що втрата інтелектуальної власності, прямі витрати та переривання бізнесу позначені сірим кольором, що означає, що вони не часто трапляються в Space Corp.

Інциденти витоку даних можна умовно розділити на три категорії: A: незначні інциденти, пов'язані виключно з витратами на розслідування; B: середні інциденти, більша частина часу в яких припадає на витрати на розслідування, але частина часу може бути пов'язана з повідомленням зацікавлених сторін або документуванням випадків розкриття невеликих обсягів персональних даних (PII); C: великі інциденти, коли можуть виникнути додаткові витрати, пов'язані з розкриттям PII, які не включені в час розслідування.

На рисунку 3.2 показано розподіл часу розслідування інцидентів витоку даних. Поділ на три категорії є умовним, але корисним для загальної характеристики різних наслідків, пов'язаних з інцидентами витоку даних.

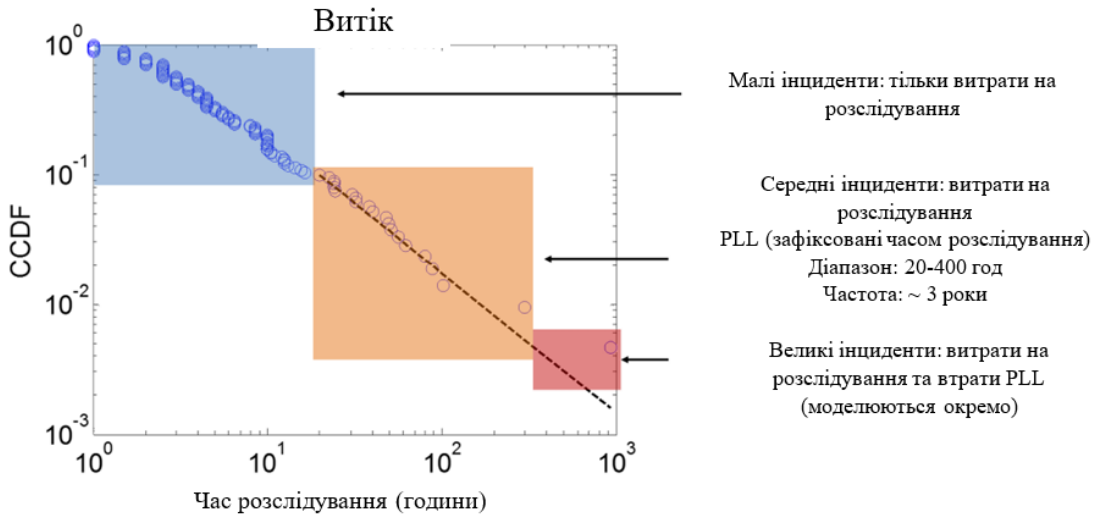



Рисунок 3.2 - Кумулятивна функція розподілу часу розслідування

Важливо, що найбільші інциденти можуть передбачати додаткові витрати, які моделюються окремо. На рисунку 3.3 показано CCDF для годин розслідування витоку даних за роками. Розподіл залишався приблизно постійним у часі, що вказує на те, що розподіл минулих інцидентів є чудовим наближенням до тяжкості майбутніх інцидентів.

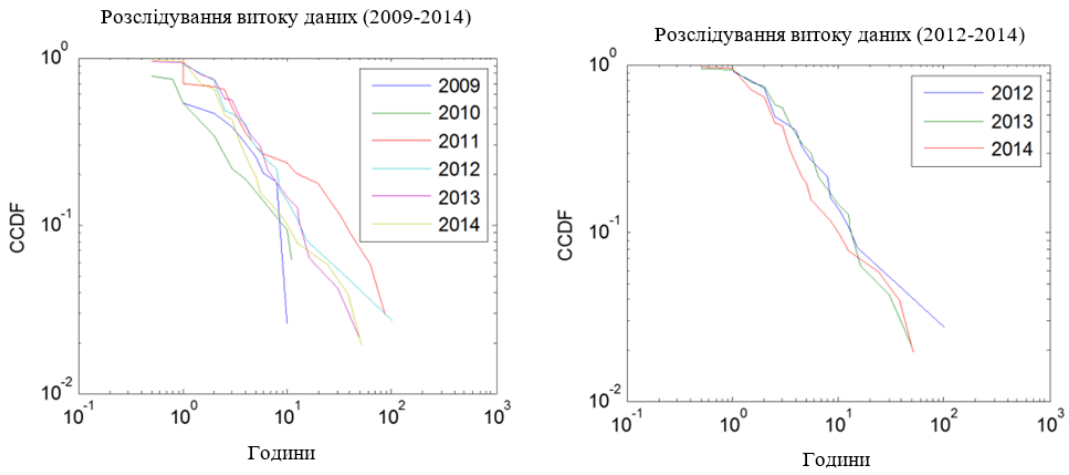



Рисунок 3.3 - Розподіл впливу витоку даних у часі

Випадки витоку даних здебільшого спричинені людською помилкою, що призводить до постійного потоку інцидентів, які відбуваються з часом. Порівняно з іншими категоріями інцидентів, такими як інциденти із шкідливим програмним забезпеченням або атаки на веб-сайти, випадки витоку даних відбуваються з відносно низькою частотою — приблизно 40 випадків на рік у Space Corp.

Більш серйозні інциденти, розслідування яких триває понад 20 годин, відбуваються рідше – приблизно сім випадків на рік. На рисунку 3.4 показано частоту випадків витоку даних різного масштабу з плином часу.

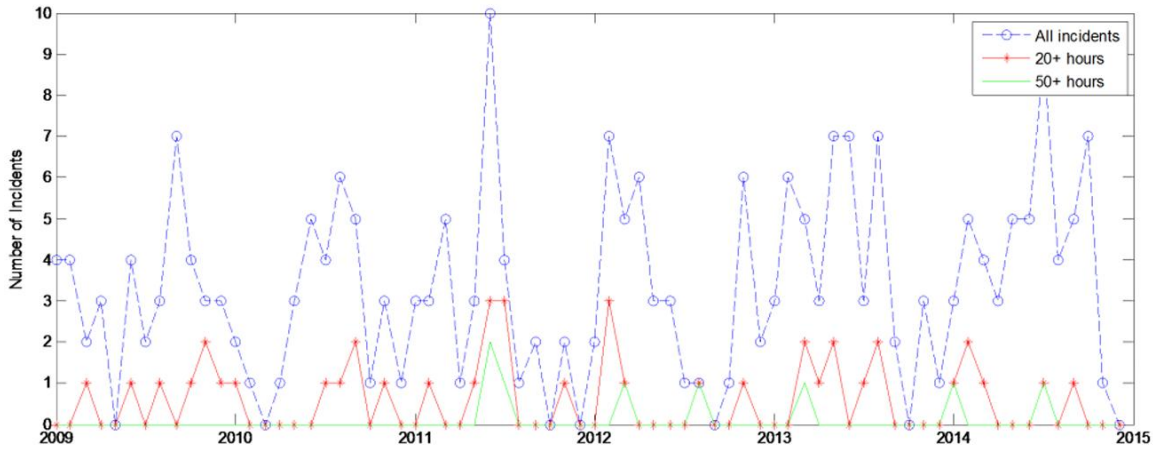



Рисунок 3.4 - Інциденти витоку даних у часі

В цілому, аналіз частоти та серйозності випадків витоку даних свідчить про те, що історичні події можуть бути хорошими індикаторами майбутніх випадків витоку даних. Тому в моделі використовується частота, що дорівнює середній кількості випадків, які відбувалися щороку. Серйозність кожного випадку розраховується за допомогою методу бутстрепінгу, тобто історичні випадки відбираються випадковим чином для отримання серйозності окремого випадку.

Інциденти витоку даних можуть призвести до різних витрат. Для організації ці витрати пов'язані з часом на розслідування, витратами, пов'язаними з втратою особистої інформації, та шкодою репутації. Кожен вплив ретельно моделюється з використанням історичних даних, інформації з відкритих джерел та висновків експертів.

Як зазначалося вище, розподіл часу на розслідування базується на історичних даних (рис. 3.2). Кожна година розслідування є дорогою для організації, враховуючи, що слідчий з питань безпеки має витратити час на розслідування та усунення інцидентів. Фінансовий відділ організації встановлює вартість часу на рівні 100 доларів за годину розслідування. Якщо порушення безпеки даних є результатом грубої недбалості, або є особливо серйозним, це може призвести до шкоди репутації. У цьому випадку організація оцінює, що поріг шкоди репутації настає, коли час розслідування досягає 500 годин або більше, що означає, що шкода репутації може виникнути тільки в разі особливо серйозних інцидентів.

Експерти оцінюють, що для інцидентів, які перевищують цей час розслідування, існує 50% ймовірність, що великий інцидент не приверне уваги, а це означає, що додаткових витрат не буде. Існує 45% ймовірність, що інцидент спричинить додаткові вимоги з боку регуляторних органів, що включають аудити, нові стандарти відповідності та інші перевірки. У минулому зовнішні аудити та вимоги коштували Space Corp від 1 до 2 мільйонів доларів. Тому витрати на аудит моделюються як рівномірний розподіл між 1 і 2 мільйонами доларів. Ці витрати моделюються за допомогою бета-розподілу (рис. 3.5).

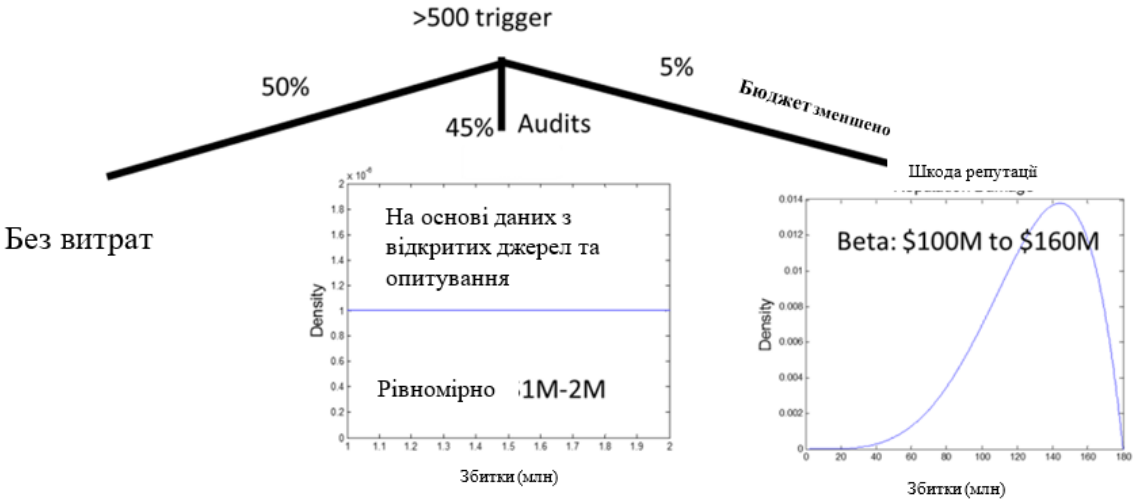



Рисунок 3.5 - Модель шкоди репутації

Інциденти витоку даних часто можуть призвести до розголошення імен, адрес, номерів соціального страхування або іншої особистої інформації. Якщо розголошення особистої інформації стосується значної кількості записів, виникають великі витрати у вигляді зв'язку з постраждалими особами та надання послуг з моніторингу кредитів. Space Corp не обробляє особисту інформацію жодних клієнтів або третіх осіб, крім своїх внутрішніх співробітників. Тому кількість записів, які можуть бути розкриті, обмежена 2000 осіб, плюс 5000 співробітників, які більше не працюють в організації. На основі декількох випадків розкриття PII в Space Corp та висновків експертів, втрати від розкриття PII оцінюються в розмірі від 60 000 до 5 мільйонів доларів.

Інші організації можуть мати значно відмінні розподіли. Наприклад, можуть існувати різні бази даних клієнтів, що містять тисячі, мільйони або десятки мільйонів записів, що призводить до втрат PII, які слід моделювати як розподіл з важким хвостом.

Хоча витік даних може призвести до переривання бізнесу, прямих фінансових витрат або втрати інтелектуальної власності, такі види збитків досі були рідкісними для Space Corp. Інші організації можуть оцінювати ці ризики по-різному. Наприклад, у деяких особливо чутливих бізнес-середовищах будь-яке розкриття інформації може призвести до зупинки діяльності. Space Corp оцінює

ймовірність того, що витік даних призведе до таких втрат, як досить низьку, тому вони не включені до функції витрат.

Після оцінки частоти випадків витоку даних та розподілу їхнього впливу проводиться моделювання за методом Монте-Карло для отримання кривої ризику витоку даних, яка показана на рисунку 3.6.

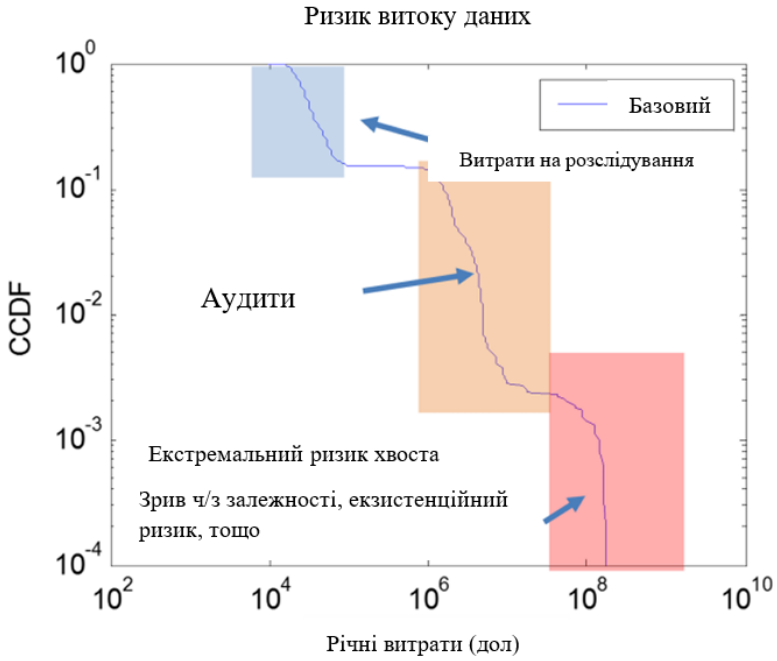



Рисунок 3.6 - Крива ризику інцидентів витоку даних

Аналізуючи розподіл, можна зробити кілька висновків. По-перше, витік даних є порівняно низьким ризиком, з типовими втратами (90-й процентиль) від 10 000 до 100 000 доларів на рік. Ці витрати пов’язані з розслідуванням інцидентів, які не змінюються істотно з року в рік. Додаткові збитки через аудит становлять від 2 до 4 мільйонів доларів і трапляються приблизно в 10 % випадків. Нарешті, в кінці розподілу існує область екстремального ризику, пов’язана з пошкодженням репутації. Зверніть увагу, що в кінці розподілу важливо ретельно враховувати точність моделі. Наприклад, великі інциденти можуть призвести до порушення припущення про незалежність подій, що означає, що один великий інцидент може змінити ймовірність додаткових великих інцидентів. Крім того, ці збитки часто

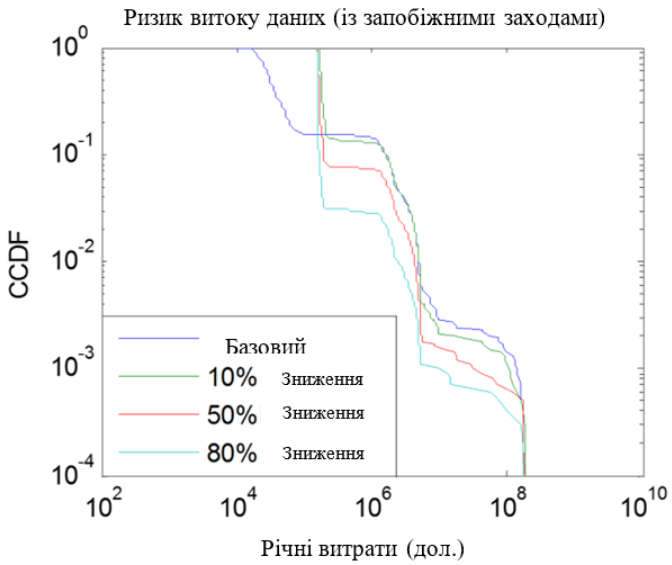
відповідають можливому екзистенційному ризику для організації, який не моделюється на основі історичних даних.

Виток даних, ймовірно, і надалі буде проблемою для багатьох організацій через людські помилки. Питання полягає в тому, як ефективно управляти ризиком, пов'язаним з витоком даних. Існує кілька заходів захисту, які можуть зменшити цей ризик, зокрема аудит для зменшення помилок, пов'язаних з привілеями, навчання для зменшення кількості інцидентів, спричинених недостатньою обізнаністю про мітки конфіденційності даних, та програмне забезпечення для запобігання втраті даних (DLP). Програмне забезпечення DLP призначене для виявлення конфіденційної інформації та захисту її використання, передачі та зберігання. Для ідентифікації конфіденційних даних використовуються різні методи, включаючи явне маркування, розпізнавання шаблонів та пошук за ключовими словами. Наразі все ще існують проблеми з усуненням помилкових спрацьовувань та фіксацією всієї конфіденційної інформації, що підлягає маркуванню. Крім того, DLP все ще має обмеження, а саме втручання у функціональність або пропуск певних типів витоку даних. Наприклад, DLP не може запобігти копіюванню конфіденційної інформації за допомогою знімків екрана або фотографій.

Технології часто є більш ефективними, коли вони орієнтовані на користувачів, які найчастіше припускаються помилок. У Space Corp особиста інформація зберігається на відносно невеликій кількості кінцевих точок, більшість з яких знаходиться у відділах кадрів (HR) та фінансів. Обмежене впровадження засобів запобігання втраті даних для цих кінцевих точок коштувало б приблизно 150 000 доларів на рік на програмне забезпечення та ліцензії. Крім того, розширене впровадження (500 000 доларів на рік) могло б забезпечити встановлення програмного забезпечення DLP на набагато більшій кількості кінцевих точок з метою контролю витоку даних в організації в цілому.

На основі галузевої інформації та випробувань DLP в інших установах, Space Corp оцінює, що обмежена реєстрація програмного забезпечення DLP зменшить кількість випадків витоку даних на 50%. Використовуючи цю інформацію, за

допомогою моделювання Монте-Карло створюється нова серія кривих ризику, які порівнюють збитки, пов'язані з DLP, з DLP і без DLP, що показано на рисунку 3.7.




| Сценарій | Очікуване значення |
|---|---|
| Базовий | $645 тис. |
| 10% зниження | $685 тис. |
| 50% зниження | $458 тис. |
| 80% зниження | $295 тис. |

Рисунок 3.7 - Криві ризику витоку даних для обмеженої ініціативи DLP

Лінії відповідають базовому ризику, а також 10%, 50% і 80% зниженню частоти випадків витоку даних. У таблиці наведено очікуване значення для кожного випадку.

На рисунку 3.7 показано, що щорічні витрати, пов'язані з витоком даних, будуть нижчими більш ніж у 85% випадків, якщо DLP НЕ буде впроваджено. Це пов'язано з тим, що витік даних є низьковитратним вектором у більшості років. Отже, щоб DLP була економічно ефективною, повинен бути особливо важкий рік. Зниження частоти інцидентів на 50% призводить до зниження очікуваної вартості збитків, головним чином за рахунок невеликого зменшення значних наслідків, пов'язаних з аудитом та пошкодженням репутації. Зверніть увагу, що хоча очікувана вартість є меншою у випадку зниження частоти інцидентів на 50%, спостережувані збитки будуть більшими, ніж у базовому випадку, у більшості випадків. Це важливий фактор, який слід враховувати керівництву.

Аналізуючи результати моделювання методом Монте-Карло, можна також помітити обмеження використання очікуваного значення. Кожен сценарій передбачає невелику ймовірність дуже великих втрат, тому очікувані втрати

набагато вищі за втрати, які спостерігатимуться у 90% випадків. Тому можливість проаналізувати повну криву ризику є корисною для особи, яка приймає рішення, оскільки низькі, часті збитки можна чітко порівняти з серйозними, але нечастими збитками.

В цілому, DLP обійдеться організації дорожче, ніж вона заощадить у більшості випадків. Аналіз чутливості може бути використаний для визначення того, що обмежене впровадження DLP буде економічно вигідним, якщо воно зменшить кількість інцидентів на 20% або більше. Враховуючи, що поточна оцінка передбачає 50% зниження кількості інцидентів, обмежене впровадження є вигідною інвестицією. Однак ця рекомендація є дуже чутливою до вартості програмного забезпечення DLP, що означає, що кожне підвищення ціни DLP на 50 000 доларів вимагає додаткового 10% підвищення загальної ефективності для особи, яка приймає рішення без ризику. Тому розширена реєстрація DLP не є економічно вигідною.

При виборі програмного забезпечення DLP слід враховувати велику кількість інших факторів. Наприклад, слід уникати впровадження DLP, яке суттєво порушує робочі процеси. DLP може позначати документи з дев'ятизначними номерами як дані соціального страхування, хоча багато поштових індексів також складаються з дев'яти цифр і не повинні блокуватися. Відомо, що користувачі також можуть йти на обхідні шляхи, якщо заходи безпеки є надто обтяжливими, і можуть не впроваджувати DLP ефективно. Нарешті, слід вивчити, наскільки легко DLP може бути обійдено зловмисним інсайдером або супротивником. Наприклад, злочинці зазвичай шифрують дані перед їх витоком, щоб системи безпеки не могли виявити, що виходить з мережі. З огляду на ці міркування, програмне забезпечення DLP є майже беззбитковим, що означає, що може знадобитися більш детальна модель.

Майже всі аспекти кібербезпеки швидко змінюються, і вимоги до відповідності не є винятком. Компанія Space Corp розглядає сценарій, за якого її основний клієнт вимагає повного впровадження програмного забезпечення для запобігання втраті даних (DLP). Компанія Space Corp вже підрахувала, що розширене впровадження не є економічно вигідним, але хотіла б дослідити, як ця

вимога до безпеки може вплинути на її рішення. Спочатку збиток репутації оцінювався як 50% ймовірність без додаткових витрат, 45% ймовірність витрат на аудит і 5% ймовірність втрати майбутнього бізнесу. Однак нові вимоги до відповідності змінюють ці перспективи, оскільки стає набагато більш імовірним, що будь-які інциденти витоку даних призведуть до аудиту та збитку репутації.

На рисунку 3.8 показано нову криву ризику, розраховану відповідно до вимог до програмного забезпечення DLP, яка відповідає 100% ймовірності шкоди репутації в разі великого інциденту з витоком даних.

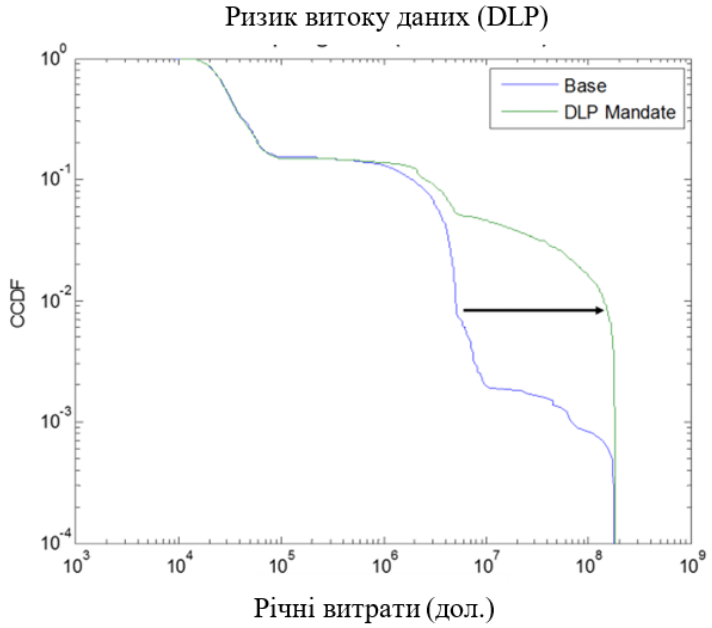



Рисунок 3.8 - Крива ризику з вимогами щодо дотримання нормативних вимог

Базовий ризик витоку даних можна порівняти зі збитками, коли DLP є вимогою дотримання нормативних вимог, що означає, що витрати будуть вищими, якщо трапиться серйозний інцидент.

Аналізуючи криву ризику, особи, які приймають рішення, можуть точно побачити, де виникає додатковий ризик, а саме в кінці розподілу. Інциденти з витоком даних трапляються рідко, а це означає, що збитки будуть однаковими протягом більшості років. Однак, якщо трапиться великий витік даних, а регуляторні органи чекають на це, можуть виникнути великі збитки [42].

Створення кількісної моделі є корисним для організації. Дані чітко показують, що, хоча витік даних є відносно низьким ризиком в цілому, можуть виникнути великі збитки через аудит та шкоду репутації. Крім того, запобігання втраті даних є ефективним для зменшення кількості помилок, але не дуже ефективним для запобігання витоку інформації зловмисними інсайдерами або деякими досвідченими зловмисниками. Повне впровадження DLP не є економічно вигідним, хоча обмежене впровадження стає економічно вигідним, якщо програмне забезпечення може зменшити кількість випадків витоку даних більш ніж на 20%. Нарешті, еволюція вимог до відповідності може змінити оптимальне рішення, оскільки організація понесе додаткові збитки, якщо не буде дотримуватися необхідних стандартів.

Ризик витоку даних відносно простий для аналізу, враховуючи стохастичний характер інцидентів та просту функцію витрат. Інші сценарії атак є більш складними, враховуючи, що супротивники можуть бути адаптивними.

## 3.3 Аналіз та моделювання загроз соціальної інженерії та веб-атак

Деякі з найбільш значних випадків порушення безпеки даних сталися через зловмисні електронні листи, зокрема злом Target, злом університетів та злом RSA. Три поширені типи шкідливих електронних листів включають черв’яки, доставку шкідливого програмного забезпечення та крадіжку облікових даних.

Зловмисники отримують доступ до комп’ютера користувача з кількох причин. Деякі злочинці можуть використовувати зламаний комп’ютер як частину ботнету, мережі комп’ютерів, що використовується для відмови в обслуговуванні, розповсюдження шкідливого програмного забезпечення або майнінгу біткойнів. Інші зловмисники прагнуть отримати доступ до мереж, щоб знайти інформацію про кредитні картки або особисті дані. Багато шкідливих електронних листів, які отримує організація, можуть не стосуватися конкретно цієї організації.

З часом випадки зараження комп’ютерними черв’яками стають все рідшими, оскільки зловмисники переходять до інших форм кібератак. Натомість поширення

шкідливого програмного забезпечення через електронну пошту є дуже поширеним і, здається, є улюбленим методом проникнення для багатьох злочинців. Зловмисники зазвичай досягають високого рівня успішності в тому, щоб спонукати користувачів натискати на шкідливі вкладення або шкідливі посилання.

Зловмисні електронні листи надсилаються різними типами зловмисників, але в основному їх можна віднести до постійних зловмисників, злочинців та спамерів.

На рисунку 3.9 показано CCDF для часу розслідування інцидентів з електронною поштою та поділено інциденти на кілька категорій зловмисників.

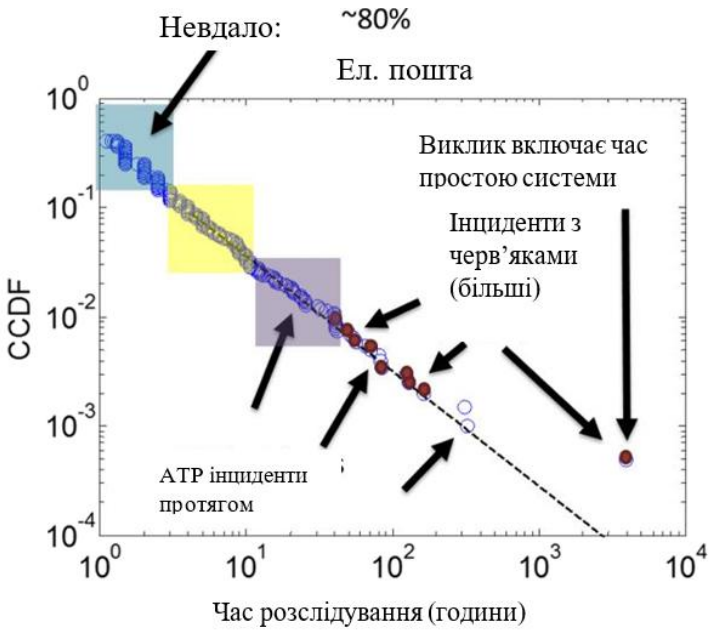



Рисунок 3.9 - CCDF для часу розслідування інцидентів із шкідливими електронними листами

Решта 20% інцидентів стосуються спамерів і злочинців, наполегливих зловмисників та інцидентів із черв'яками. Інциденти з наполегливими зловмисниками охоплюють усі рівні тяжкості, від незначних до серйозних.

Протягом шести років компанія зафіксувала тисячі випадків зловмисних електронних атак. Ці випадки необхідно очистити та класифікувати, щоб отримати більш чітке уявлення про атаки, що відбуваються. Спочатку відокремлюються невдалі спроби зловмисних електронних атак. З усіх зареєстрованих спроб зловмисних електронних листів 81,4% було розслідувано за 1 годину або менше,

що свідчить про те, що електронний лист було позначено як зловмисний і розслідувано, але атака не була успішною. Це добре узгоджується з евристичним правилом, згідно з яким від 10 до 20 % спроб зловмисних електронних листів є успішними.

Далі видаляються черв'яки. Інциденти, пов'язані з черв'яками, становлять дуже невелику частку від загальної кількості інцидентів, але майже виключно мають дуже високий рівень серйозності. Це пов'язано з тим, що інциденти, пов'язані з електронними черв'яками, поширюються дуже швидко і вимагають значних витрат часу на усунення наслідків.

Ці атаки мають різний рівень складності, але можуть бути надзвичайно цілеспрямованими, адаптованими до конкретної цілі. Атаки постійних супротивників також можуть мати різний рівень серйозності, залежно від того, чи є атака успішною. Приблизно 10 % успішних зловмисних електронних листів приписують наполегливим супротивникам. Різні групи зловмисників мають різні стратегії. Наприклад, деякі кампанії атак можуть використовувати цільові електронні листи зі зловмисними вкладеннями, тоді як інші можуть зосередитися на отриманні облікових даних користувача. З огляду на невизначеність щодо корисності отримання облікових даних користувача, спостерігається, що досвідчені зловмисники віддають перевагу зловмисному програмному забезпеченню у своїх атаках.

Нарешті, решту електронних листів можна розрізнити за типом атаки і, часто, за типом зловмисника. Крадіжка облікових даних, коли виманюють пароль користувача, трапляється в 44% випадків, а в решті 56% випадків використовується шкідливе програмне забезпечення. Крадіжка облікових даних зазвичай використовується злочинцями, які використовують зламану електронну пошту для розсилки спаму на інші поштові скриньки. Ці атаки легко виявляються командою безпеки, оскільки зламана поштова скринька часто починає розсилати тисячі електронних листів за хвилину. Тому виявлення є простим з реакційної точки зору, а виправлення передбачає очищення поштової скриньки користувача, скидання облікових даних та виявлення первинного вектора злому (рис. 3.10).

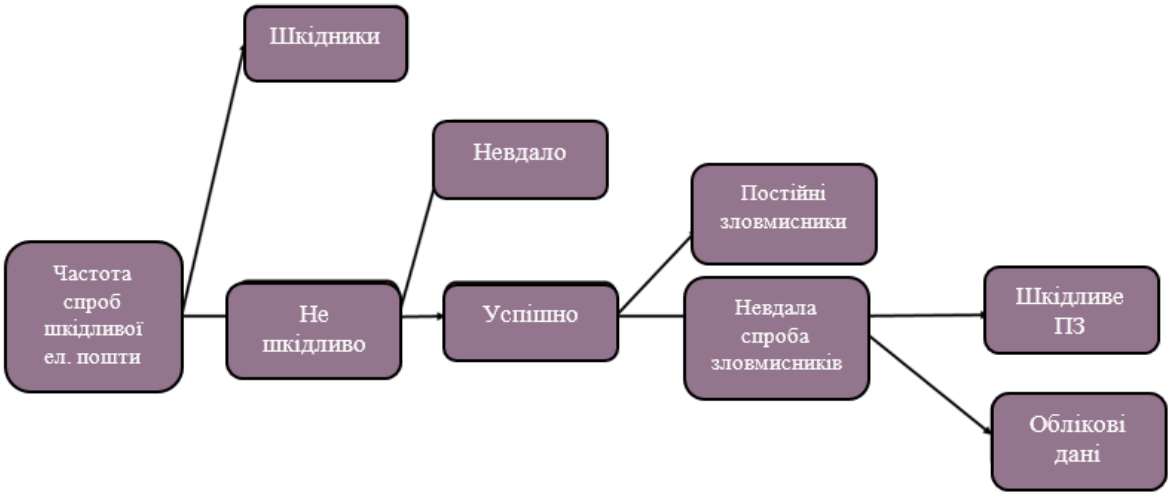



Рисунок 3.10 - Класифікація інцидентів, пов’язаних з електронною поштою

Електронні листи, що містять шкідливе програмне забезпечення, як правило, важче виявити команді безпеки. Зазвичай шкідливе програмне забезпечення завантажується на пристрій, коли користувач відкриває шкідливе вкладення або натискає на шкідливе посилання, яке перенаправляє жертву на скомпрометований веб-сайт. Якщо браузер користувача має вразливість, шкідливе програмне забезпечення може бути завантажене на його комп’ютер. Після цього шкідливий код може деякий час перебувати в неактивному стані, а потім зв’язатися з сервером управління. Це створює «задні двері» до кінцевого пристрою в мережі, що дозволяє зловмиснику отримати вищі привілеї доступу та доступ до більшої частини мережі. Підвищення привілеїв та горизонтальне переміщення в мережі є складним процесом. На високому рівні зловмисник буде повторювати серію інструментів і технік, деякі з яких будуть ефективними, а деякі — ні. Протягом цього процесу відбувається постійна боротьба між експлуатацією та виявленням.

Хоча час розслідування інцидентів, пов’язаних із шкідливими електронними листами, у Space Corp залишався незмінним протягом останніх кількох років, частота інцидентів різко зросла (рис. 3.11). З 2009 по 2015 рік кількість шкідливих електронних листів зросла з приблизно 10 на місяць до майже 150 на місяць. Однак переважна більшість цих додаткових інцидентів не є серйозними, і на їх розслідування витрачається менше 3 годин.

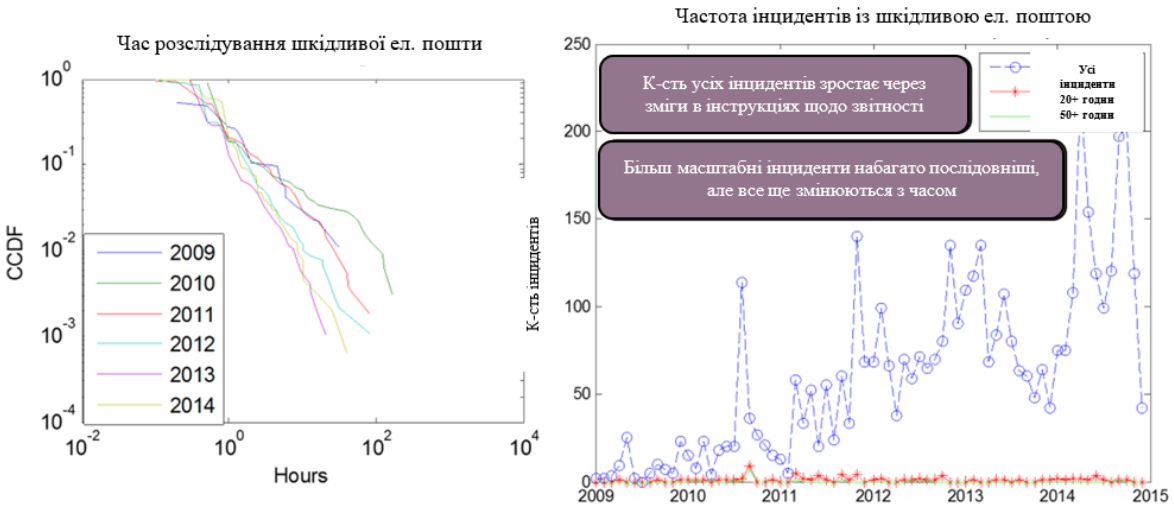



Рисунок 3.11 - Розподіл інцидентів, пов’язаних з електронною поштою

Хоча точний розподіл змінюється з року в рік, зловмисні атаки за допомогою електронної пошти зберігають подібні характеристики за ступенем серйозності. Кількість інцидентів, пов’язаних із зловмисною електронною поштою, що мають незначний вплив, зростає, але великі інциденти все ще відбуваються з постійною частотою. На рисунку 3.12 показано частоту великих інцидентів, пов’язаних із шкідливими електронними листами.

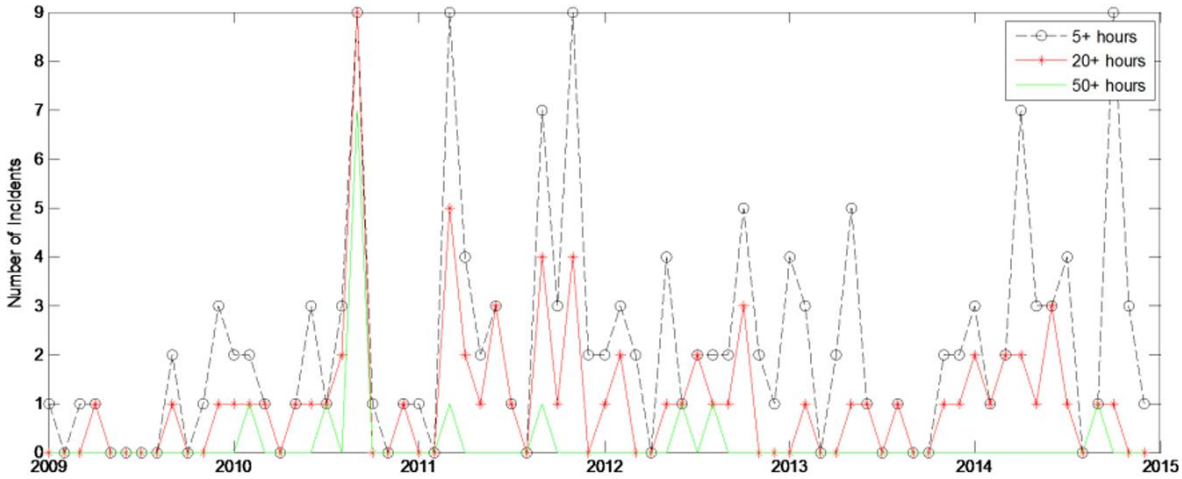



Рисунок 3.12 - Розподіл інцидентів, пов’язаних з електронною поштою

Кількість великих інцидентів залишається стабільною протягом тривалого часу. Такий нюансований погляд на інциденти кібербезпеки ілюструє необхідність

ретельної оцінки тенденцій. Багато галузевих досліджень свідчать про стрімке зростання кількості фішингових інцидентів, які, можливо, є найпоширенішим вектором атак [16]. Хоча загальна кількість зловмисних інцидентів, пов'язаних з електронною поштою, може зростати, важливо також враховувати відповідний рівень їхньої серйозності.

Зловмисні електронні листи можуть бути дуже складними, що пов'язано з великою невизначеністю щодо ймовірності атаки, ймовірності успіху, наявності подальших вразливостей, які дозволяють користувачеві зламати комп'ютер, та наслідків для організації. У ситуаціях з надзвичайною невизначеністю стає ще більш важливим кількісно моделювати процес, а не повертатися до якісних методів. Врахування невизначеностей дозволяє краще зрозуміти відносну важливість різних змінних за допомогою таких інструментів, як аналіз чутливості. Наприклад, важко оцінити важливість кількості шкідливих електронних листів, що надсилаються до організації, порівняно з імовірністю успіху. Кількісне моделювання дозволяє особі, яка приймає рішення, чітко порівняти, як змінюються збитки в обох випадках.

Для моделювання шкідливих електронних листів робиться кілька припущень. По-перше, вважається, що черв'яки є рідкісними і нечасто зустрічаються, оскільки зловмисники, здається, переходять до інших векторів атак. Тому модель передбачає, що інциденти з черв'яками не відбуватимуться протягом наступного року. Крім того, кількість шкідливих електронних листів повільно зростатиме (~5%) протягом наступного року, тоді як частка шкідливих електронних листів, спричинених постійними атаками, спамерами та злочинцями, залишатиметься пропорційною до поточних спостережень 10%, 35% та 45%. Інформація про загрози може доповнити модель, адаптуючи прогнозовану еволюцію зловмисних електронних атак. Наприклад, у 2016 році спостерігалося збільшення кількості зловмисних електронних атак на медичні установи, спрямованих на шифрування медичних даних та вимагання викупу. Організації в галузі охорони здоров'я повинні врахувати цю інформацію у своїх оцінках для отримання більш точних прогнозів [3].

Зловмисні електронні листи передбачають два нових вектори витрат, які необхідно моделювати, а саме: переривання бізнесу та втрата інтелектуальної власності. Переривання бізнесу значною мірою залежить від типу організації. Наприклад, деякі організації є постачальниками послуг і втрачають дохід, коли контент не доставляється. Netflix, постачальники хмарних послуг та засоби масової інформації працюють за цією моделлю витрат. Інші організації можуть мати більш невизначені витрати, пов'язані з перериванням бізнесу. Фінансові установи, що пропонують онлайн-банкінг, потребують високої доступності, оскільки перебої в роботі підривають довіру клієнтів і можуть призвести до втрати продажів, якщо споживач вирішить перейти до іншого постачальника послуг. Навіть у цьому випадку реальні витрати значною мірою залежать від сектору: наприклад, зміна банку є трудомісткою процедурою, і один короткочасний перебій у роботі навряд чи призведе до втрати клієнтів. Однак коротші цикли обслуговування з низькими витратами на перехід більш вразливі до перебоїв, як, наприклад, у випадку бронювання готелів або транспортних послуг (тобто Uber або Lyft).

Отримання розподілу витрат на переривання діяльності вимагає ретельного підходу з боку осіб, що приймають рішення, з урахуванням спостережень за історичними інцидентами та залученням інших експертів у цій галузі. Для Space Corp переривання діяльності проявляється у вигляді порушення надання основних послуг, що призводить до простою працівників (рис. 3.13). Space Corp оцінює, що існує невелика ймовірність затримки, яка призведе до прострочення терміну, і в цьому випадку витрати становитимуть мільйони доларів. Якщо ці витрати будуть реалізовані, ймовірно, це призведе до подальшого пошкодження репутації, яке моделюється окремо. Для моделювання витрат, пов'язаних з перериванням бізнесу, використовується бета-розподіл.

Втрати інтелектуальної власності (ІВ) також повинні бути змодельовані. Наразі існує багато розбіжностей щодо найкращого способу моделювання втрат ІВ. Втрати ІВ фактично стосуються комерційних таємниць або виробничих деталей, які не є загальнодоступними. Порушення патентних прав та авторських прав є окремим питанням, оскільки патенти є загальнодоступною інформацією.

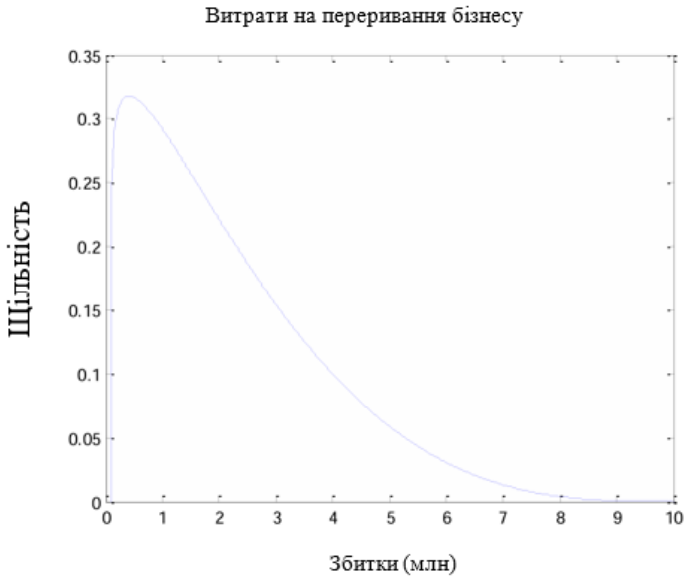



Рисунок 3.13 - Витрати на переривання діяльності компанії Space Corp

Виявлення втрат інтелектуальної власності може бути складним завданням, оскільки ці втрати можуть варіюватися в широких межах. Аналітики повинні бути готові до виявлення збитків на лінійно-лінійному графіку або логарифмічно-логарифмічному графіку, залежно від характеру втрат. Для Space Corp втрати інтелектуальної власності оцінюються на логарифмічно-логарифмічному графіку на основі даних галузі та випадків крадіжки інтелектуальної власності, що спостерігалися в організації. На рисунку 3.14 показано графік виявлення, а також деякі питання, які можна використовувати для орієнтування відповідей.

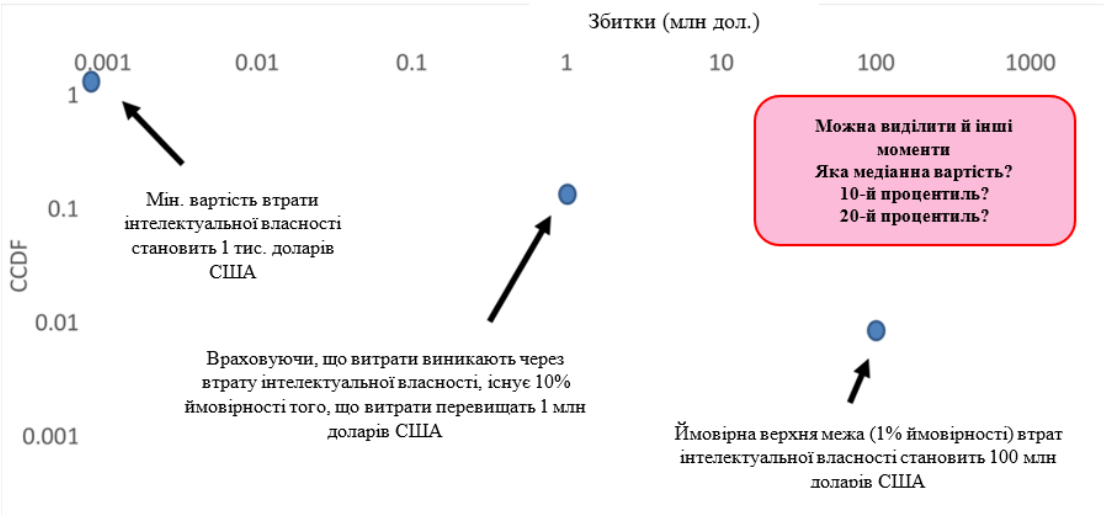



Рисунок 3.14 - Приклад визначення грошових втрат, пов’язаних із втратою інтелектуальної власності

Визначення відбувається в різних порядках величини. Ці визначення використовуються для створення сімейства кривих втрат, з яких можна брати вибірки, а оцінки, що стосуються частоти інцидентів із шкідливими електронними листами та моделей витрат, використовуються для ініціювання ще одного моделювання методом Монте-Карло (рис. 3.15).

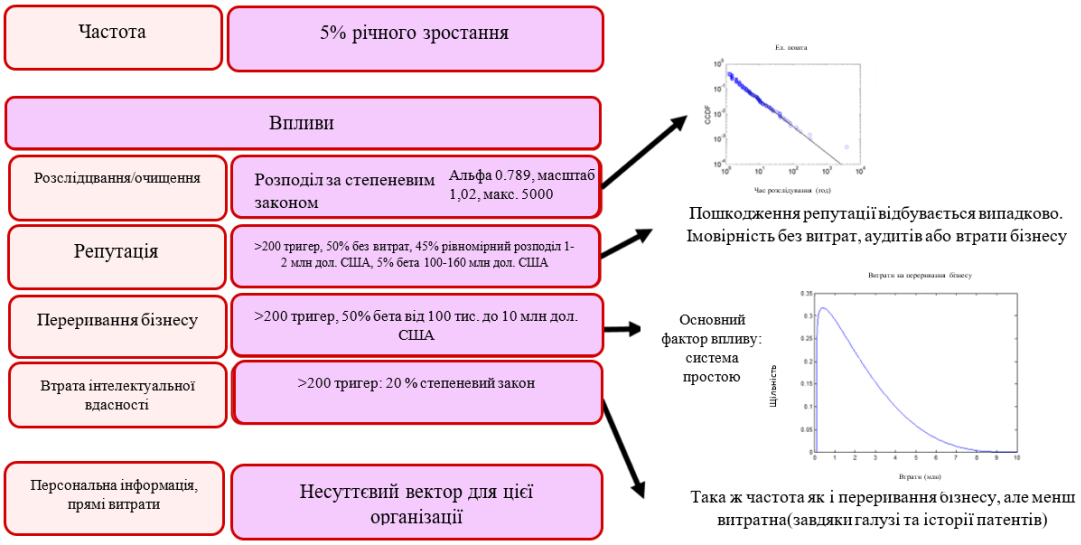



Рисунок 3.15 - Вхідні дані для моделі ризику шкідливих електронних листів

Експерти прогнозують, що протягом наступного року частота інцидентів зросте на 5 %. Час розслідування визначається на основі спостережуваного розподілу історичних інцидентів. Інші витрати виникають із тривалістю розслідування 200 годин.

Переривання бізнесу моделюється з тригером 200 годин і призводить до 50% ймовірності збитків, отриманих з бета-розподілу від 100 000 до 10 мільйонів доларів. Збитки від втрати інтелектуальної власності розраховуються за степеневим законом, отриманим від осіб, що приймають рішення, з максимальним збитком 10 мільйонів доларів.

На рисунку 3.16а показано криву ризику для шкідливих електронних листів. На рисунку 3.16б показано, як змінюються результати, коли до моделювання додаються інциденти з черв'яками; витрати на розслідування зростуть, але ризик хвоста майже не зміниться.

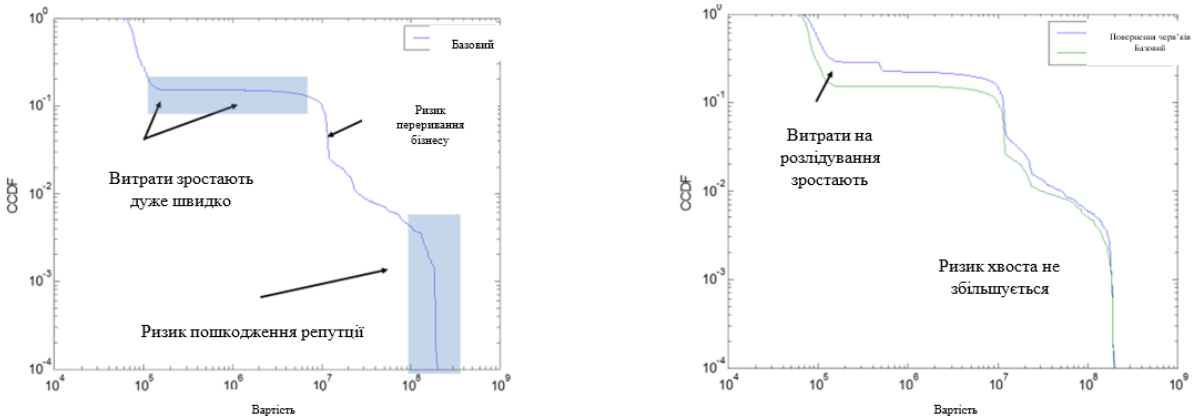



Рисунок 3.16 - Криві ризику для шкідливих електронних листів (а) та аналіз випадків зараження комп'ютерними черв'яками (б)

Одразу видно, що шкідливі електронні листи коштують значно дорожче, ніж інциденти з витоком даних. Хоча лише 20% інцидентів з витоком даних спричиняють збитки на суму понад 20 000 доларів, 20% найсерйозніших інцидентів із шкідливими електронними листами спричиняють збитки на суму 3 мільйони доларів і більше. Це частково пов'язано з різким зростанням витрат, спричиненим пошкодженням репутації та перериванням бізнесу.

Перша лінія захисту від шкідливих електронних листів полягає в їх блокуванні до того, як вони потраплять до користувача. Існує багато корпоративних технологій для фільтрування спаму або шкідливих вкладень. Інші технології захисту не є специфічними для шкідливих електронних листів, але є загальними функціями безпеки, які зменшують ймовірність успішного компрометації з декількох векторів.

Одним з найефективніших засобів захисту від крадіжки облікових даних є двофакторна автентифікація (TFA). Замість простого пароля для доступу до системи, TFA вимагає від користувача іншої форми верифікації.

Двофакторна автентифікація в першу чергу впливає на серйозність інцидентів. Інциденти продовжують відбуватися з тією ж частотою, але їх вплив буде зменшений. Наприклад, якщо користувач розкриває свої облікові дані через фішингове електронне повідомлення, центр безпеки все одно повинен задокументувати інцидент, скинути пароль користувача та перевірити всі

зловмисні невдалі спроби входу. У цьому випадку TFA обмежує потенційно серйозний інцидент дуже невеликим розслідуванням.

З огляду на широкий спектр зловмисників і типів атак за допомогою шкідливих електронних листів, організації можуть вирішити розробити дуже детальні моделі для оцінки ефективності TFA. Для цілей цього тематичного дослідження зроблено кілька спрощених припущень, щоб зробити модель більш зрозумілою. По-перше, експерти компанії оцінюють вартість впровадження TFA у 500 000 доларів на рік. Насправді, для розробки інфраструктури будуть потрібні більші початкові фіксовані витрати, а також додаткові щорічні витрати на ліцензії на програмне забезпечення та підтримку. Однак 500 000 доларів на рік є хорошим приблизним показником для організації.

Зловмисні інциденти з електронною поштою пов’язані з різними типами зловмисників, що означає, що двофакторна автентифікація може мати різну ефективність проти різних типів супротивників. Організація моделює ефективність TFA, спочатку аналізуючи частку зловмисних інцидентів з електронною поштою, пов’язаних з трьома типами зловмисників: спамерами, злочинцями та постійними супротивниками. Далі ефективність TFA оцінюється щодо кожного з цих супротивників. Наприклад, 35% зловмисних інцидентів із електронною поштою пов’язані зі спамерами, а 90% атак спамерів відбиваються за допомогою TFA. Вплив кожного з відбитих інцидентів є обмеженим.

На рисунку 3.17 показано оцінене зниження рівня TFA для кожного типу зловмисників та нову криву ризику після впровадження TFA.

З цих модельних розрахунків можна зробити кілька важливих висновків. По-перше, очевидно, що хоча невелике збільшення кількості зловмисних електронних атак є важливим фактором, який слід враховувати, воно не є основним чинником ризику. Насправді, аналіз чутливості показує, що темпи зростання майже непомітні в короткостроковій перспективі, а це означає, що результати є дуже стійкими до припущень щодо збільшення кількості зловмисних електронних атак. Аналізуючи економічну ефективність TFA, можна зробити кілька інших висновків.

| Зловмисник | Частка поточних інцидентів | Зниження показника TFA |
|---|---|---|
| Спамери | 35% | 90% |
| Злочинці | 45% | 20% |
| Постійні зловмисники | 10% | 20% |

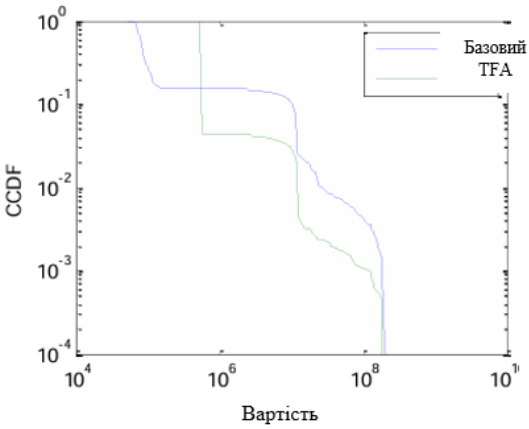



Рисунок 3.17 - Крива ризику для шкідливих електронних листів з різними показниками ефективності TFA

TFA вимагає значних інвестицій і відразу ж зменшує деякі витрати на розслідування, але не настільки, щоб зробити цю технологію економічно ефективною. Однак TFA значно зменшує варіативність витрат на розслідування, а також значно зменшує збитки на суму від 1 до 10 мільйонів доларів. Зниження ризику також значно перевищує вплив DLP на інциденти витоку даних, оскільки зловмисні електронні листи, як правило, пов'язані з більшими фінансовими втратами, ніж інциденти витоку даних. На основі оцінки вартості TFA в 500 000 доларів на рік і ретельного аналізу кривих ризику, Space Corp вважає, що TFA є економічно ефективною технологією. Щорічні витрати дещо обмежуються скороченням часу розслідування, а також покращується ризик хвоста.

З цих модельних розрахунків можна зробити кілька важливих висновків. По-перше, очевидно, що хоча невелике збільшення кількості зловмисних електронних атак є важливим фактором, який слід враховувати, воно не є основним чинником ризику. Насправді, аналіз чутливості показує, що темпи зростання майже непомітні в короткостроковій перспективі, а це означає, що результати є дуже стійкими до припущень щодо збільшення кількості зловмисних електронних атак. Аналізуючи економічну ефективність TFA, можна зробити кілька інших висновків. TFA вимагає значних інвестицій і відразу ж зменшує деякі витрати на розслідування, але не настільки, щоб зробити цю технологію економічно ефективною. Однак TFA

значно зменшує варіативність витрат на розслідування, а також значно зменшує збитки на суму від 1 до 10 мільйонів доларів. Зниження ризику також значно перевищує вплив DLP на інциденти витоку даних, оскільки зловмисні електронні листи, як правило, пов’язані з більшими фінансовими втратами, ніж інциденти витоку даних. На основі оцінки вартості TFA в 500 000 доларів на рік і ретельного аналізу кривих ризику, Space Corp вважає, що TFA є економічно ефективною технологією. Щорічні витрати дещо обмежуються скороченням часу розслідування, а також покращується ризик хвоста.

Хоча аналіз показує, що TFA є економічно ефективним у цьому випадку, важливо підкреслити, що деталі мають значення. TFA може бути реалізовано безперебійно або погано, і досвід користувача може призвести до того, що вся інвестиція буде невдалою.

Важливо також враховувати питання зручності використання. Механізми TFA, що базуються на мобільному пристрої без альтернативного резервного засобу аутентифікації, можуть спричинити серйозні перебої в роботі, якщо працівник загубить свій пристрій або у нього розрядиться батарея. Також необхідно зберегти швидкість аутентифікації, оскільки 30-секундна затримка в отриманні та введенні коду може швидко призвести до незадоволення багатьох користувачів. Нарешті, безпека всієї системи повинна базуватися на найслабшій ланці. Експлойт POODLE полягав у примусовому переведенні з’єднання на слабкий протокол шифрування, який можна було легко зламати. Аналогічно, якщо резервний механізм аутентифікації передбачає дзвінок до служби підтримки та відповіді на прості для вгадування питання безпеки, то вся система аутентифікації TFA стає слабкою та вразливою для багатьох зловмисників.

В організації також можуть існувати емпіричні докази, які безпосередньо ілюструють складність запобігання компрометації користувачів через шкідливі електронні листи. На рисунку 3.18 показано два приклади шкідливих електронних листів у великій організації. Шкідливі електронні листи були розроблені на основі попередніх кампаній атак і надіслані вибірці співробітників організації. Були зібрані дані про частку співробітників, які відкрили підроблений електронний лист

(що в деяких обмежених випадках могло призвести до успішного компрометації), та частку співробітників, які натиснули на вкладення або ввели свої облікові дані.

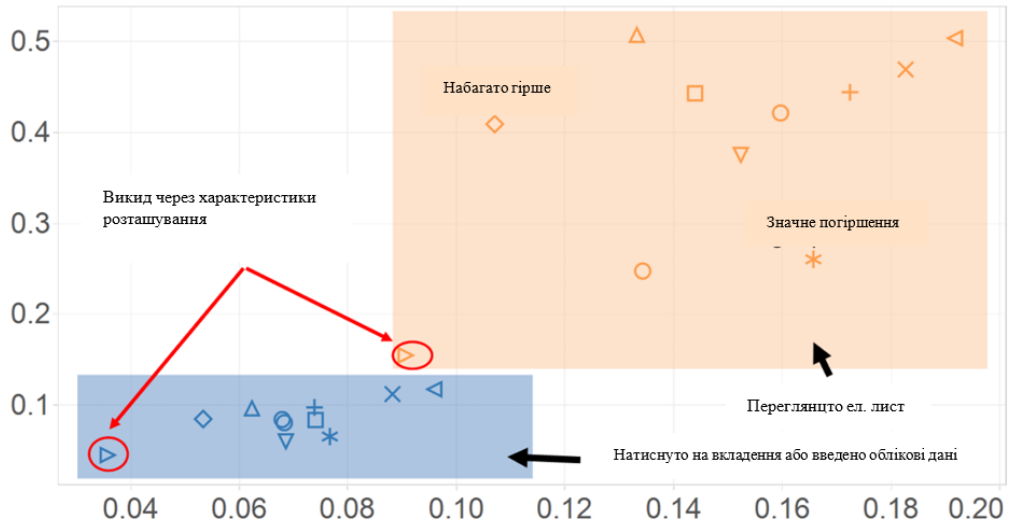



Рисунок 3.18 - Дані з двох зловмисних електронних кампаній

Як зазначалося вище, ефективність фільтрування електронної пошти значною мірою залежить від основної технології та типу електронних листів, що надсилаються до організації. Наприклад, цільові електронні листи набагато складніше фільтрувати, ніж спам, який надсилається великій кількості одержувачів.

Більшість випадків успішного фішингу становлять від 30% до 5%. Навчання користувачів може знизити цей показник, хоча ефект навчання з часом, ймовірно, зникне. Організації повинні збалансувати частоту, ефективність та вартість навчання користувачів.

На рисунку 3.19 показано нову криву ризику за цих припущень.

Навчання користувачів має ті ж самі компроміси, що й інші заходи безпеки, а саме: вищий рівень втрат протягом більшості років, але менший ризик інцидентів із великим впливом. Точна ефективність навчання користувачів є дуже невизначеною, але навіть 5-відсоткове зниження рівня успішності фішингу призводить до помірного зниження ризику. Зловмисні атаки за допомогою електронної пошти в основному базуються на кількості.

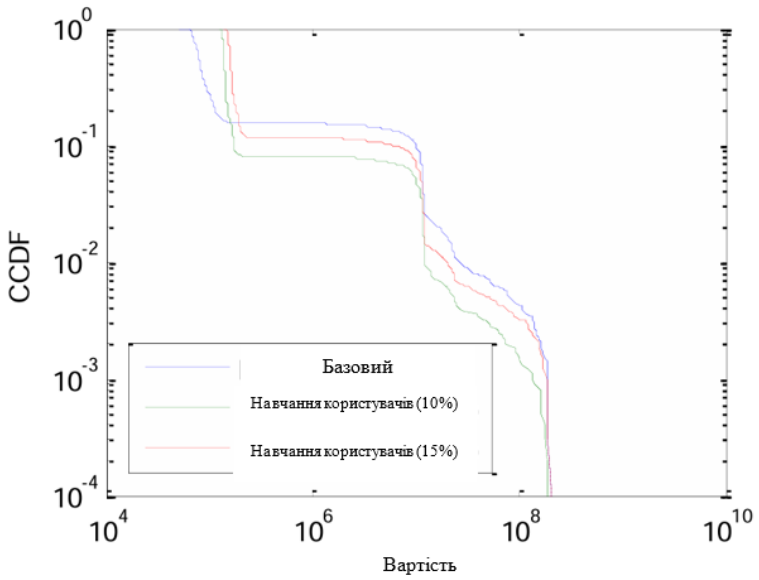



Рисунок 3.19 - Економічна ефективність навчання користувачів

Одна з технік спирається на те, що певна частина населення в будь-який момент очікує на результати обстеження від медичного закладу і відкриє електронний лист, не замислюючись про безпеку, оскільки з нетерпінням чекає на медичні результати.

Зловмисники також можуть досягти успіху, створюючи спеціальні цільові електронні листи. В одній організації зловмисники змогли встановити, що група співробітників відвідала іншу корпорацію, і надіслали електронний лист із підробленими матеріалами для подальшої роботи. Зловмисний електронний лист навіть містив пояснення, чому він не був надісланий зі звичайної робочої електронної адреси. LinkedIn, соціальна мережа для професіоналів, зараз регулярно використовується зловмисниками, які намагаються ідентифікувати адміністративних помічників важливих осіб у корпорації. Такі типи цільових атак можуть бути занадто дорогими для зловмисників низького рівня, але інші зловмисники продовжуватимуть експлуатувати цю критичну бізнес-функцію. Навчання користувачів та двофакторна автентифікація є хорошими інвестиціями в безпеку для Space Corp, головним чином тому, що зловмисні електронні листи історично були дорогим вектором атак. Однак для подальшого захисту організації

від атак через електронну пошту все ще потрібно розробити нові механізми запобігання та виявлення.

Веб-сайти є загальнодоступними і є вхідними воротами для кібератак. Організації використовують веб-сайти для досягнення ряду цілей, таких як реклама або освітня діяльність, або для задоволення деяких основних бізнес-потреб, таких як онлайн-банкінг або віддалений доступ до електронної пошти для співробітників (веб-пошта). Веб-сайти може бути складно повністю захистити. Розробники неминуче припускаються помилок, що призводять до неправильної конфігурації, яка робить веб-сайти вразливими. Впровадження виправлень з високою точністю також є складним завданням, зважаючи на постійний потік вразливостей, що виникають у додатках, а безпека веб-сайтів може бути серйозним викликом.

Існує ряд методів атак на веб-сайти. Міжсайтовий скриптинг (XSS) вводить шкідливий код у веб-додаток. Атаки методом грубої сили можуть отримати доступ до відкритих сторінок входу, вичерпно перевіряючи всі імена користувачів та паролі. Атаки з переходом по каталогах використовуються, коли зловмисник переходить до неавторизованої частини веб-сервера, вгадуючи ієрархію файлів.

Атаки на веб-сайти зазвичай мають один з трьох результатів. Одиночні хакери та хактивісти зазвичай намагаються зіпсувати веб-сайт, що робить їх виявлення дуже легким. Інші одиночні хакери або злочинці можуть намагатися витягти інформацію з сервера або бази даних, щоб продемонструвати свої навички або знайти дані, які можна продати. Нарешті, частина зловмисників намагатиметься зламати веб-сайт, щоб закріпитися в мережі, встановити постійну присутність, викрасти інтелектуальну власність або завдати шкоди мережі. Отримавши доступ до веб-сервера, зловмисник може встановити бекдори, завантажити інструменти для підвищення привілеїв і переміщатися по мережі [102].

Веб-сайти є привабливою мішенню, оскільки для їх атаки потрібні незначні ресурси, вони завжди відкриті для доступу, а також тому, що багато веб-сайтів мають постійний потік вразливостей. Зловмисники можуть негайно спробувати багато експлойтів проти веб-сайту, не витрачаючи час на профілювання організації

або вивчення довідкової інформації, яка була б необхідна для цілеспрямованої фішингової атаки. Багато популярних платформ для розробки веб-додатків, таких як ColdFusion від Adobe або веб-сервери Apache HTTP, мають численні помилки, які регулярно виявляються. Якщо команда розробників не стежить уважно за попередженнями про вразливості та не виправляє їх швидко, застаріле програмне забезпечення може швидко призвести до серйозних вразливостей. Деякі з найвідоміших і наймасштабніших вразливостей вплинули на веб-сервери. У 2014 році дослідники виявили вразливість Heartbleed, яка дозволяла неавторизованим особам отримувати інформацію з веб-сервера, яку можна було використовувати для крадіжки облікових даних та іншої інформації.

Веб-атаки не обмежуються лише веб-серверами, але можуть бути спрямовані і на інше мережеве обладнання. Наприклад, поширеним методом передачі файлів є використання FTP-серверів (File Transfer Protocol). FTP-сервери передають файли між клієнтом і сервером. Однак більшість цих серверів надсилають інформацію в незашифрованому вигляді, що робить дані вразливими для перехоплення зловмисниками. Крім того, багато FTP-серверів працюють на застарілому програмному забезпеченні, яке має відомі вразливості, а це означає, що зловмисники можуть використовувати скомпрометований FTP-сервер, щоб закріпитися в мережі.

Частота та серйозність інцидентів у часі дають унікальне уявлення про кібербезпеку в організації. Одна організація вважала, що кількість атак на веб-сайти збільшується, коли увага ЗМІ до них висока, і часто збільшувала штат Центру оперативної безпеки, очікуючи на додаткові атаки. Однак дані чітко показали, що атаки не корелювали з увагою ЗМІ, що дозволило організації скоротити кількість додаткового персоналу.

Через зміни в правилах звітності, частота виникнення подій, включаючи SQL-ін’єкції, XSS-атаки, атаки методом грубої сили та інші, не є добре відомою. Натомість, акцент робиться на моделюванні наслідків, оскільки дані про них є більш якісними.

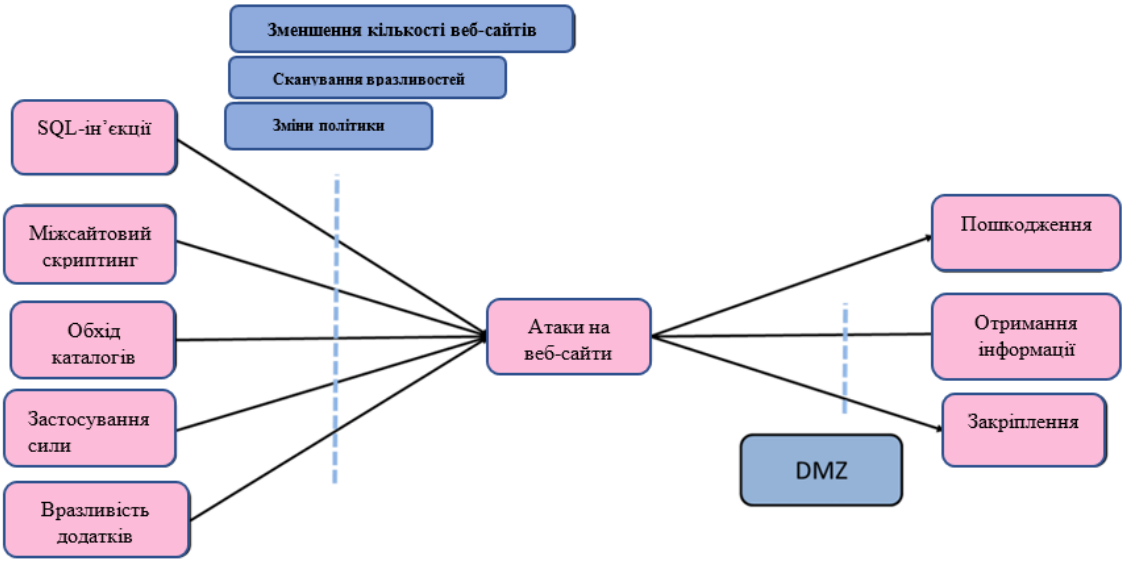



Рисунок 3.20 - Загальна модель атак на веб-сайти та засобів захисту

Наслідки для веб-сайтів можна умовно класифікувати за різними сценаріями, такими як псування веб-сайтів, витік інформації або спроби вторгнення в мережу. Кожен сценарій має типовий набір наслідків, пов'язаних з ним. Як зазначалося раніше, наслідки псування веб-сайтів подібні до графіті на будівлі або кидання цеглини у вікно магазину. Необхідні певні витрати на розслідування, щоб визначити, як зловмисник зламав систему, і переконатися, що атака не залишила на сервері постійного коду і не надала доступу до інших частин мережі. Також можливі певні витрати, пов'язані з переривання бізнесу.

Організації повинні визначити найбільш корисну модель для аналізу різних типів атак. Набір даних, який використовується для Space Corp, не містить достатньої інформації для розрізнення різних типів атак на веб-сайти. Інформація про ймовірних зловмисників також записується непослідовно. У деяких випадках вторгнення приписуються певним групам або особам, але в більшості випадків це не так. Тому Space Corp вирішила моделювати всі наслідки атак на веб-сайти з використанням ймовірнісного підходу.

Прямі витрати моделюються унікальним чином і базуються на історичних даних у поєднанні з оцінками експертів. Цей сценарій також представляє найгірший можливий варіант розвитку подій, за якого супротивник здатний проникнути в мережу Space Corp, переміщатися по системі, встановити контроль

над критичною інфраструктурою (у цьому випадку – обладнанням для управління супутниками) і вчинити дії, що призведуть до втрати космічного апарата. Експерти оцінюють, що цей сценарій є відносно малоймовірним (3% ймовірність на великий інцидент), але призведе до значних витрат для організації. Нарешті, Space Corp оцінює, що шкода репутації, пов'язана з інцидентами на веб-сайті, може бути змодельована за допомогою того самого процесу оцінки шкоди репутації, що використовується для інцидентів з витоком даних та зловмисними електронними листами (хоча і з тригером у 400 годин).

Використовуючи всю вищезазначену інформацію, проводиться моделювання за методом Монте-Карло для оцінки впливу інцидентів на веб-сайтах. Відразу стає зрозуміло, що інциденти на веб-сайтах є найдорожчим вектором атак для організації. Для підтвердження цих результатів можна провести аналіз чутливості декількох параметрів моделі (рисунок 3.21).

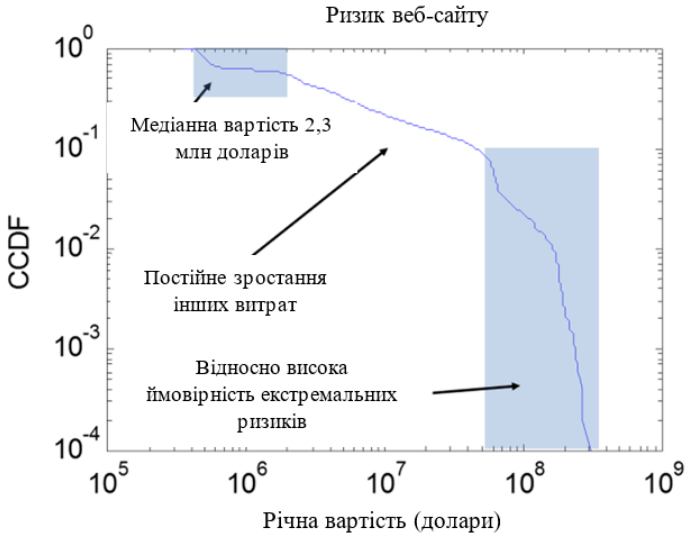



Рисунок 3.21 - Крива ризику веб-сайту

Наприклад, на рисунку 3.22 показано аналіз чутливості щодо порогу розслідування. Спостерігається крива ризику, що відповідає тривалості розслідування 500, 300 і 200 годин. Хоча поріг зміщує криву ризику вгору і вниз, іноді змінюючи збитки на мільйони доларів, загальний ризик постійно значно перевищує збитки, спричинені іншими типами інцидентів.

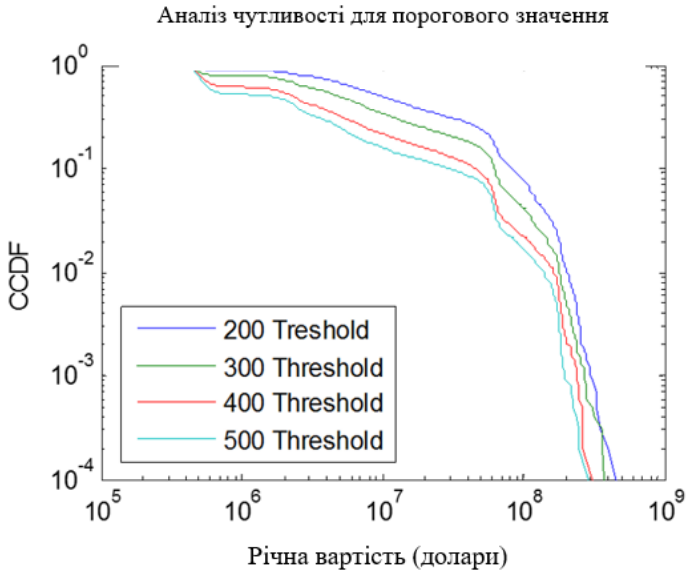



Рисунок 3.22 - Аналіз чутливості для порогу спрацьовування

Насправді важко побудувати правдоподібний сценарій, в якому інциденти на веб-сайті не є основним фактором ризику для Space Corp. Аналіз чутливості дозволяє аналітику підтвердити надійність результатів моделі. Це також демонструє цінність кількісного аналізу ризиків за відсутності досконалих даних. Всі оцінки, що використовуються в моделі, супроводжуються значною невизначеністю. Незважаючи на це, Space Corp може бути впевненою в рейтинговому порядку різних векторів ризику.

# ВИСНОВКИ

У роботі представлено обмежену кількість типів атак на конкретну організацію, призначених для оцінки ефективності декількох засобів захисту кібербезпеки.

1. Проведено комплексний аналіз сучасних підходів до класифікації та кількісної оцінки кіберризиків, на основі опрацювання міжнародних стандартів ISO/IEC 27005, NIST SP 800-30, COBIT та актуальних наукових досліджень у сфері кібербезпеки,що дало можливість сформувати теоретично обґрунтовану базу для побудови власної методики аналізу ризиків.

2. Досліджено методи моделювання загроз та ймовірнісні підходи оцінювання ризиків, включно зі сценарним, байєсівським та статистичним моделюванням інцидентів,на основі застосування математичного апарату теорії ймовірностей, статистики, методів системного аналізу та моделей FAIR/OCTAVE/CVSS,що дало можливість створити універсальну та адаптивну методику кількісного вимірювання ризику різної природи.

3. Виконано аналіз типових загроз, вразливостей та інцидентів у сучасних кіберсистемах, на основі оброблення даних із відомих публічних джерел, звітів про порушення безпеки, наукових статей та прикладів реальних атак (веб-атаки, соціальна інженерія, витоки даних, крадіжки носіїв),що дало змогу визначити критичні фактори ризику та їх статистичні характеристики.

4. Адаптовано та налаштовано розроблену методику для оцінки ризиків конкретної кіберсистеми, на основі аналізу її інфраструктури, моделі загроз, витоків даних, можливих сценаріїв атак і поведінкових характеристик порушника,що дало реалістичні кількісні оцінки ризику та можливість порівняти рівень небезпеки для різних типів інцидентів.

5. Розроблено рекомендації щодо мінімізації ризиків та оптимізації контролів безпеки, на основі результатів моделювання, аналізу розподілів збитків (CCDF), порівняння ризиків «до» та «після» впровадження захисних заходів,що

дало зниження очікуваних збитків, підвищення рівня захищеності системи та можливість обґрунтування пріоритетів інвестицій у безпеку.

6. Апробовано методику на реальній/модельній кіберсистемі, на основі практичного аналізу вразливостей, статистики інцидентів та моделювання наслідків атак, що дало підтвердження її практичної застосовності та готовності для використання фахівцями з інформаційної безпеки.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Krebs, B. (2014a, February 12). Email Attack on Vendor Set Up Breach at Target. Retrieved from http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target

2. Krebs, B. (2015a, February 9). Anthem Breach May Have Started in April 2014. Retrieved from http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/

3. Krebs, B. (2015b, August 14). Cyberheist Victim Trades Smokes for Cash. Retrieved from http://krebsonsecurity.com/2015/08/cyberheist-victim-trades-smokes-for-cash/

4. Greenberg, A. (2015, July 6). Hacking Team Breach Shows a Global Spying Firm Run Amok. Retrieved from http://www.wired.com/2015/07/hacking-team-breach-shows-global spying-firm-run-amok/

5. Cox, T. (2008). What's wrong with risk matrices? Risk analysis, 28(2), 497–512.

6. McLane, M., Gouveia, J., Citron, G. P., MacKay, J., & Rose, P. R. (2008). Responsible reporting of uncertain petroleum reserves. AAPG bulletin, 92(10), 1431–1452.

7. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 11(3), 431–448.

8. Garrick, B. J., Gekler, W. C., Goldfisher, L., Karcher, R. H., Shimizu, B., & Wilson, J. H. (1967). RELIABILITY ANALYSIS OF NUCLEAR POWER PLANT PROTECTIVE SYSTEMS (No. HN--190). Holmes and Narver, Inc., Los Angeles, Calif. Nuclear Div.

9. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87–92.

10. Daniels, M. (2014). Optimization of spacecraft architectures for earth-orbit satellite projects. Stanford dissertation.

11. Orman, H. (2003). The Morris worm: A fifteen-year perspective. IEEE Security & Privacy, (5), 35–43.

12. Glazer, E. (2015, August 3). J.P. Morgan to Accelerate Timeline for Cybersecurity Spending Boost. Retrieved from http://www.wsj.com/articles/j-p-morgan-to-accelerate-timeline for-cybersecurity-spending-boost-1438641746

13. Guikema, S. (2002). Optimal resource allocation in an engineering design team with asymmetric information. Stanford dissertation.

14. Korzak, E. (2014). Computer Network Attacks and International Law. Doctoral dissertation, University of London.

15. Miura-Ko, R. A., & Bambos, N. (2007, June). SecureRank: A risk-based vulnerability management scheme for computing infrastructures. In Communications, 2007. ICC'07. IEEE International Conference on (pp. 1455–1460). IEEE.

16. Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). Intrusion detection by machine learning: A review. Expert Systems with Applications, 36(10), 11994–12000.

17. Soo Hoo, K. J. (2000). How much is enough? A risk management approach to computer security. Stanford, Calif: Stanford University.

18. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438–457.

19. Thomas, R. C., Antkiewicz, M., Florer, P., Widup, S., & Woodyard, M. (2013). How bad is it?–a branching activity model to estimate the impact of information security breaches. A Branching Activity Model to Estimate the Impact of Information Security Breaches (March 11, 2013).

20. Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)–a practical quantitative model. Journal of Research and practice in Information Technology, 38(1), 45–56.

21. Whiteman, P., Winter, P. (2013). Network Risk assessment Tool (NRAT) with Cyber Threat Tracker (CTT). SURVIAC-TR-13-2085.

22. Freund, J., & Jones, J. (2014). Measuring and managing information risk: a FAIR approach. Butterworth-Heinemann.

23. Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

24. NIST. (2012). Guide for Conducting Risk Assessments (NIST SP-800-30rev1). The National Institute of Standards and Technology (NIST), Gaithersburg.

25. NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity.

26. Katsikas, S.K. (2009). Computer and information security handbook. Chapter 53. Morgan Kaufmann.

27. US-CERT Federal Incident Notification Guidelines. Retrieved from https://www.us cert.gov/incident-notification-guidelines

28. Alberts, C. J., & Dorofee, A. (2002). Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc.

29. Moore, T., & Anderson, R. (2011). Economics and Internet Security: A Survey of Recent Analytical, Empirical, and Behavioral Research.

30. Ponemon Institute. (2011). Cost of a Data Breach.

31. Greisiger, M. (2013). Cyber liability & data breach insurance claims a study of actual claim payouts. Technical report, NetDiligence.

32. Florêncio, D., & Herley, C. (2013). Sex, lies and cyber-crime surveys. In Economics of information security and privacy III (pp. 35–53). Springer New York.

33. Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI)–a practical quantitative model. Journal of Research and practice in Information Technology, 38(1), 45–56.

34. Maass, P., & Rajagopalan, M. (2012). Does Cyber Crime Really Cost $1 Trillion? Pro Publica, 1st August,{Online Resource} Available at: http://www. propublica. org/article/does cybercrime-really-cost-1-trillion [Accessed 26/11/12].

35. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300). Springer Berlin Heidelberg.

36. Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of Cyber Risk: An Empirical Analysis†. The Geneva Papers on Risk and Insurance–Issues and Practice, 40(1), 131–158.

37. Sinanaj, G., Muntermann, J., & Cziesla, T. (2015). How Data Breaches Ruin Firm Reputation on Social Media!–Insights from a Sentiment-based Event Study. In Wirtschaftsinformatik (pp. 902–916).

38. Goldstein, J., Chernobai, A., & Benaroch, M. (2011). An event study analysis of the economic impact of IT operational risk and its subcategories. Journal of the Association for Information Systems, 12(9), 606.

39. Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. The European Physical Journal B, 89(1), 1–12.

40. Ryan, J. J. C. H., & Jefferson, T. I. (2003, May). The use, misuse, and abuse of statistics in information security research. In Proceedings of the 2003 ASEM National Conference, St. Louis, MO.

Додаток А. Копії публікацій



***ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ***
***КАФЕДРА СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ***
***ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»***

науково-практичний симпозіум

# *ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ: СИСТЕМИ ТА РІШЕННЯ (ТІР:СТ – 2025)*

24 жовтня 2025 року
м. Тернопіль

## ЗМІСТ

УДК 681.51

***Якименко Н., Слободян В., Якименко Ю., Хомяк Р.***

*Західноукраїнський національний університет*

# МЕТОД КІЛЬКІСНОЇ ОЦІНКИ КІБЕРРИЗИКІВ НА ОСНОВІ ДОСТОВІРНИХ СТАТИСТИЧНИХ ІМОВІРНІСНИХ МОДЕЛЕЙ

**Вступ**. Кількісна оцінка кіберризиків залишається однією з найбільш складних і актуальних проблем сучасних організацій [1]. Незважаючи на зростання обізнаності щодо загроз інформаційній безпеці, керівники служб інформаційної безпеки (CISO) часто стикаються з труднощами у визначенні пріоритетних напрямів захисту. Зокрема, виникають сумніви щодо того, які ризики становлять більшу небезпеку - фізичні інциденти, пов'язані з втратою пристроїв, чи соціоінженерні атаки.

Сучасний ринок пропонує широкий спектр рішень для забезпечення кібербезпеки, однак постачальники цих рішень рідко надають кількісні оцінки впливу своїх технологій на загальний рівень ризику організації [2].

Унаслідок цього спостерігається тенденція до неефективного розподілу ресурсів та здійснення інвестицій у безпеку без належного обґрунтування. Типовим прикладом є ситуація, коли аналітики з безпеки переоцінюють внутрішні загрози (зловмисні дії інсайдерів), тоді як фактичні дані свідчать про значно більшу частоту зовнішніх атак, наприклад, на веб-сайти та веб-додатки.

Аналіз інцидентів упродовж п'ятирічного періоду в окремих організаціях показав, що реальні ризики, пов'язані з кібератаками на вебресурси (зокрема SQL-ін'єкції, дефейси тощо), значно перевищують загрозу від інсайдерських дій, хоча інтуїтивно може здаватися навпаки.

Відсутність достовірних методів кількісного вимірювання ефективності заходів кібербезпеки ускладнює прийняття стратегічних рішень щодо оптимізації витрат і розподілу бюджету. Інвестиції у шифрування даних, навчання персоналу з протидії фішингу або модернізацію мережевого обладнання часто здійснюються без порівняльної оцінки потенційного зниження ризику. Це призводить до низької ефективності витрат і нераціонального використання обмежених ресурсів.

**Мета:** розробка методу кількісного оцінювання кіберризиків на основі достовірних статистичних імовірнісних моделей.

## 1 Концептуальні основи моделювання кіберризиків на основі даних про інциденти

Кіберризик складається з поширених інцидентів з невеликим впливом у поєднанні з рідшими інцидентами, що мають більший вплив. Необхідно оцінити всю криву ризику, щоб особи, які приймають рішення, могли зрозуміти обидва типи ризику: історичні інциденти, які вже трапилися, а також нові сценарії, які, можливо, ще не траплялися. Оцінка цих двох типів інцидентів може вимагати різних методів моделювання [3].

У випадку кібербезпеки аналітики можуть використовувати експертні думки або моделі сценаріїв, які ще не відбулися, щоб отримати більш повну оцінку всієї кривої

ризику. Використовуючи цю структуру, кіберризик можна моделювати в трьох режимах (рисунок 1):

– модель на основі даних: базується на історичних подіях, якщо дані існують і є стабільними у часі;

– модель на основі сценаріїв: використовується для моделювання інцидентів, які ще не відбулися (зазвичай інциденти з великим впливом);

– режим перекриття: поєднує модель на основі даних та модель на основі сценаріїв шляхом перекриття кривих ризику, щоб уникнути подвійного підрахунку інцидентів.

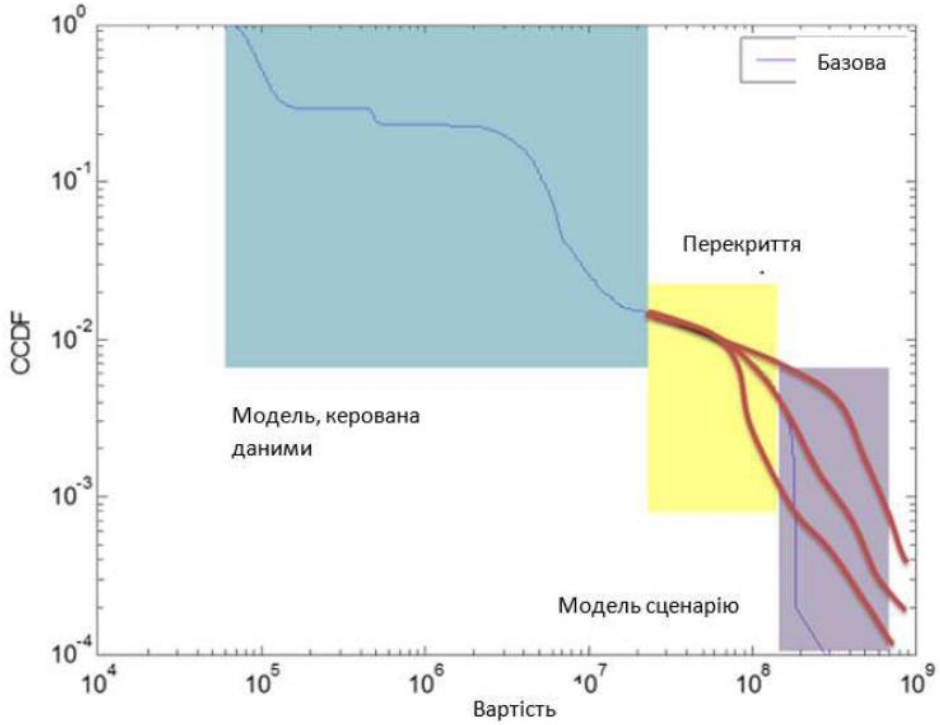



Рисунок 1 – Три режими кривої ризику: модель на основі даних, модель на основі сценаріїв та режим перекриття

Після об'єднання цих трьох режимів особа, яка приймає рішення, отримує повну характеристику кіберризику, з яким стикається організація.

## 2 Оцінка ризиків за допомогою моделювання методом Монте-Карло

Після моделювання розподілу різних типів атак, їх частоти та впливу, криву ризику на основі даних можна обчислити за допомогою моделювання методом Монте-Карло. Крім того, розподіл вхідних даних може базуватися на історичних даних (у випадку режиму на основі даних) або сценаріях (у випадку більш масштабних інцидентів).

Тому інциденти, що моделюються, могли відбутися в минулому, але також можуть бути новими сценаріями, які ще не спостерігалися. Іншими словами, модель Монте-Карло узагальнюється в метод моделювання навіть для інцидентів, які ще не відбулися.

Інциденти моделюються із заданою частотою, і кожен інцидент має відповідний вплив, взятий з розподілу. Вартість кожного інциденту розраховується в доларах.

Модель моделює один рік кіберінцидентів, хоча це можна легко змінити. Наприкінці моделювання всі витрати підсумовуються, щоб отримати загальні річні витрати. На основі великої кількості прогонів ($n$=10 000) розраховується доповнювальна кумулятивна функція розподілу.

Більш формально визначено наступні терміни для використання в моделюванні (таблиця 1).

Таблиця 1 – Терми для використання в моделюванні кіберризиків

| Символ | Значення |
|---|---|
| $C$ | Вартість |
| $I$<br>$J$ | Позначення інциденту<br>Позначення типу інциденту (веб-сайт, ел. пошта, шкідливе ПЗ, тощо) |
| $H$ | Години |
| $V$ | Ф-ції індикатора |
| $P_i$ | Ймовірність втрати для інциденту типу і |
| $DC_i$ | Прямі витрати для інциденту типу і |
| $PI_i$ | Втрата конфіденційної і-ції для інциденту типу і |
| $RD_i$ | Втрата репутації для інциденту типу і |
| $IP_i$ | Втрата інтелектуальної власності для інциденту типу і |
| $BI_i$ | Втрати від переривання бізнесу для інциденту типу і |

Загальна вартість кіберінцидентів в організації за рік – це просто сума вартості кожного інциденту, що стався.

$$\text{Річна вартість} = \sum_i \boldsymbol{C_i}. \quad (1)$$

Загальна вартість кожного інциденту визначається шляхом підсумовування кожної категорії впливу, а саме: витрати на розслідування, прямі витрати, переривання діяльності, шкода репутації, моніторинг кредитоспроможності та втрата інтелектуальної власності.

Припускається, що кожна година розслідування коштує 100 доларів, тому кількість годин, витрачених на розслідування інциденту, множиться на 100. У цій моделі робиться спрощене припущення, що витрати є умовно нерелевантними, враховуючи години розслідування. Можуть виникнути певні ситуації, в яких це припущення не спрацьовує, наприклад, коли втрата інтелектуальної власності збільшує ймовірність шкоди репутації. Загальна вартість визначається:

$$C_i = H_i * \$100 + DC_i + BI_i + RD_i + PI_i + IP_i. \quad (2)$$

Категорії впливу (переривання бізнесу, шкода репутації тощо) можуть залежати від типу $j$ інциденту (електронна пошта, веб-сайт, витік даних тощо). Вартість інциденту $i$ типу $j$ є функцією годин розслідування інциденту $i$, розподілу впливу, функцій індикаторів та умовних ймовірностей. Наприклад, вартість інциденту і типу «витік даних» можна записати наступним чином:

$$C_i = H_i * \$100 + RD_i + PI_i. \quad (4)$$

В результаті інциденту з витоком даних можуть виникнути лише витрати часу на розслідування, шкода репутації та розкриття конфіденційної інформації. Витрати можна додатково розбити на такі складові:

$$C_i = H_i * \$100 + V(H_i) * (RD_i + PI_i). \quad (5)$$

$$V(H_i) = \begin{cases} 1 \; if \; H_i \geq 500 \\ 0 \quad else \end{cases}. \quad (6)$$

$$PI_i = \{Uniform\ (60k\ to\ 5M)\}. \quad (7)$$

$$RD_i = \begin{cases} Uniform\ (1M\ to\ 2M), & \text{з ймовірністю } 0{,}45 \\ Beta\ Dist\ (100M\ to\ 160), & \text{з ймовірністю } 0{,}05 \\ 0, & \text{з ймовірністю } 0{,}5 \end{cases}. \quad (8)$$

Іншими словами, збитки від шкоди репутації та витрати на інформацію про приватність виникають лише в тому випадку, якщо час розслідування перевищує 500 годин, звідси і походить функція індикатора $V(H_i)$. Якщо це відбувається, з розподілу вибирається випадкова змінна, щоб отримати рівень збитків від інциденту.

Втрати конфіденційної інформації вибираються з рівномірного розподілу, а шкода репутації - з кускового розподілу, що представляє три типи результатів. Після того як вартість кожного інциденту вибрана з розподілів і обчислена, криву ризику можна отримати шляхом багаторазового моделювання та формування кумулятивної функції розподілу або, в даному випадку, додаткової кумулятивної функції розподілу.

На рисунку 2 показано діаграму рішень щодо кібербезпеки в організації та те, як частота, вплив і тип інциденту впливають на загальну вартість.

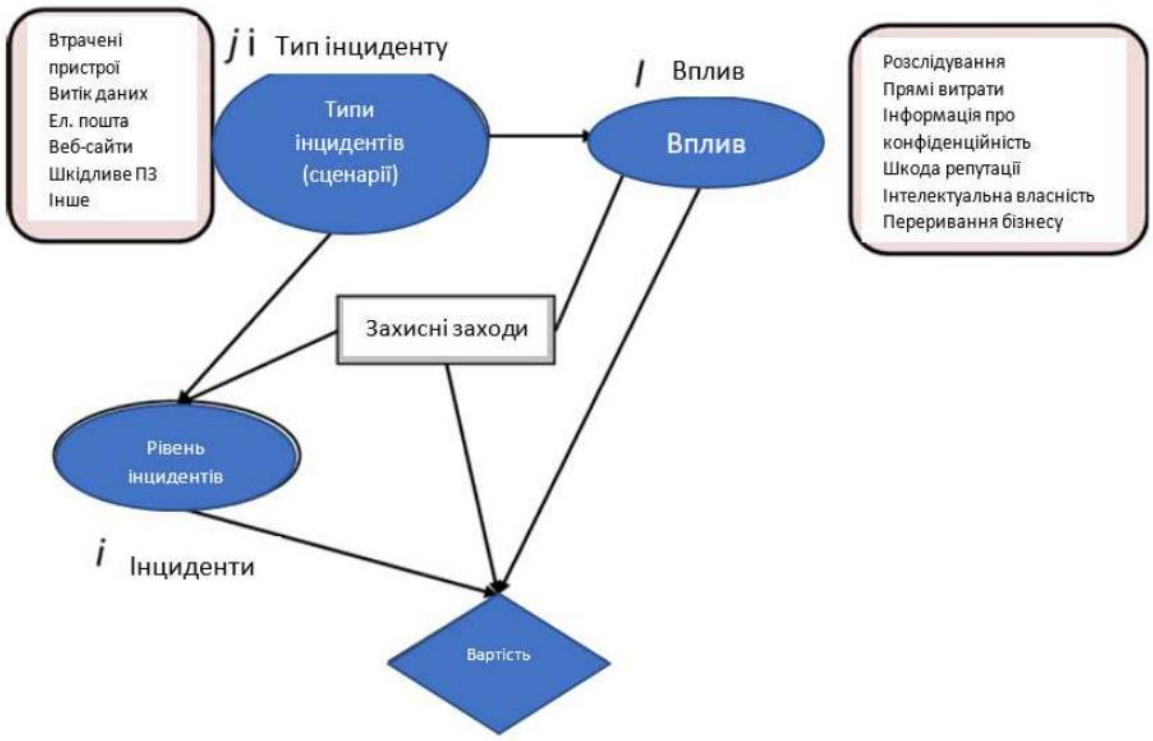



Рисунок 2 – Для розрахунку кривих ризику використовується моделювання методом Монте-Карло

Використання моделі, заснованої на інцидентах, є зручним, оскільки деякі невизначеності стають умовно нерелевантними для вартості, враховуючи інформацію про частоту, тип і вплив атак. Наприклад, аналітики можуть робити висновки про зловмисника, але ці дані не потрібні для розрахунку рентабельності інвестицій у засоби захисту. Для моделювання діаграми прийняття рішень, використовується метод Монте-Карло.

**Висновки.** У роботі запропоновано метод кількісної оцінки кіберризиків, який ґрунтується на достовірних статистичних та імовірнісних моделях, що забезпечують об'єктивніше та реалістичніше визначення рівня кіберзагроз для організації. Методика поєднує історичні дані про інциденти та сценарне моделювання майбутніх подій, що дозволяє будувати повну криву ризику з урахуванням як частих малозатратних інцидентів, так і рідкісних, але високовартісних атак.

Використання моделювання методом Монте-Карло дає змогу оцінити ймовірний розподіл щорічних збитків, враховуючи частоту, типи інцидентів і всі категорії їх впливу - прямі витрати, втрату конфіденційності, збитки репутації, порушення бізнес-процесів тощо. Такий підхід забезпечує можливість формування кількісних показників ризику, що є необхідними для прийняття обґрунтованих управлінських рішень щодо інвестицій у кібербезпеку.

Запропонована модель сприяє підвищенню ефективності розподілу ресурсів, оскільки дає змогу порівнювати очікуване зниження ризику від різних заходів кіберзахисту. Вона усуває залежність від суб'єктивних експертних оцінок та дозволяє уникнути переоцінки незначних загроз або недооцінки рідкісних, але критичних атак.

Таким чином, представлений метод є важливим інструментом у стратегічному управлінні кіберризиками, забезпечує прозорість і точність оцінювання, а також створює основу для економічно обґрунтованого планування заходів кібербезпеки.

**Перелік використаних джерел.**

1. Білявська Ю., Білявський В., Шестак Я., та інші. "Моніторинг кіберризиків у фінансовому секторі економіки." Financial and Credit Activity Problems of Theory and Practice, Том 3, № 62, 2025, с. 355–369.

2. Байдур О. Кількісна методологія оцінки ризиків кібербезпеки при відсутності фінансових даних про втрати." Кібербезпека: освіта, наука, техніка, Том 2, № 26, 2024, с. 95–114. https://doi.org/10.28925/2663-4023.2024.26.659

3. Franco, M.F., Mullick, A.R., Jha, S. "QBER: Quantifying Cyber Risks for Strategic Decisions." arXiv, 2024.




***ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ***
***ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ***
***КАФЕДРА КІБЕРБЕЗПЕКИ***
***ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»***

**Матеріали**
**науково-практичного симпозіуму**

# "ЗАХИСТ'ІНФОРМАЦІЇ'2025"

28 листопада 2025
Тернопіль

УДК 681.51

***Якименко Н., Слободян В., Якименко Ю., Хомяк Р.***

*Західноукраїнський національний університет*

# МЕТОДОЛОГІЯ КІЛЬКІСНОГО МОДЕЛЮВАННЯ КІБЕРРИЗИКІВ ДЛЯ ПІДТРИМКИ УПРАВЛІНСЬКИХ РІШЕНЬ В ОРГАНІЗАЦІЯХ

**Вступ**. Сучасні цифрові платформи, корпоративні інформаційні системи та мережеві сервіси перетворилися на критично важливі елементи діяльності організацій, що призвело до зростання залежності бізнесу від стійкості IT–інфраструктури. Одночасно із цим масштаби та складність кібератак суттєво збільшились, а економічні наслідки інцидентів почали вимірюватися мільйонами доларів. У таких умовах питання кількісного оцінювання кіберризиків набуває ключового значення, оскільки традиційні якісні методи (“високий–середній–низький”) не дають можливості виміряти реальні можливі втрати, порівняти альтернативні засоби захисту та обґрунтувати інвестиції [1].

Обмеженість якісних підходів пов’язана з їхньою суб’єктивністю та неврахуванням складних імовірнісних сценаріїв. Крім того, кіберзбитки мають асиметричний характер: більшість інцидентів є маловитратними, однак поодинокі атаки (витік даних, компрометація сервера, злом облікових записів адміністратора) можуть формувати «важкий хвіст» розподілу втрат. Саме тому сучасні моделі ризиків потребують використання статистичних розподілів, математичного апарату симуляцій та гібридного підходу до формування сценаріїв [2].

Розроблена методологія поєднує історичні дані, експертні оцінки та математичне моделювання, що дозволяє створювати реалістичну криву ризику, необхідну для управлінських рішень.

**Мета:** Розробка методології кількісного моделювання кіберризиків для підтримки управлінських рішень в організаціях.

## 1 Концептуальні основи моделювання кіберризиків на основі даних про інциденти

Методологія базується на формуванні математичної моделі збитків від кіберінцидентів, де загальна вартість події розглядається як сума її окремих компонент. Формально це описується як:

$$C = C_{invest} + C_{rep} + C_{conf} + C_{IP} + C_{bus}, \quad (1)$$

де $C_{invest}$ – витрати на розслідування,

$C_{rep}$ – втрати репутації,

$C_{conf}$ – збитки від компрометації конфіденційних даних,

$C_{IP}$ – шкода інтелектуальній власності,

$C_{bus}$ – втрати, пов’язані з порушенням бізнес–процесів.

Оскільки кожен компонент має стохастичний характер, він розглядається як випадкова величина з певним розподілом [3]. Для моделювання використовуються логнормальний, експоненційний або Парето–розподіли залежно від типу інциденту. Наприклад, витрати на компрометацію даних

описуються логнормальним розподілом:

$$C_{conf} \sim Lognormal(\mu, \sigma), \quad (2)$$

що відображає природну асиметрію втрат.

Частота появи інцидентів моделюється як пуассонівський процес:

$$N(t) \sim Poisson(\lambda t), \quad (3)$$

де λ – середня частота інцидентів за одиницю часу.

Композицію річних збитків визначає випадкова сума:

$$L = \sum_{i=1}^{N} C_i, \quad (4)$$

що є класичною моделлю сукупного збитку у задачах ризик–аналізу. Внаслідок стохастичності як частоти, так і величини втрат загальний розподіл річного збитку не має аналітичного розв'язку, тому використовується метод Монте–Карло.

У симуляціях генерується 10–100 віртуальних років діяльності організації, кожен із яких включає випадкову кількість інцидентів та їхню випадкову інтенсивність. Результатом є крива ризику – залежність імовірності перевищення певного рівня втрат: P(L>x), яка дозволяє визначати ключові показники, зокрема: Value–at–Risk (*VaR*) $VaR_{0.95}=\inf\{x:P(L\leq x)\geq 0.95\}$, та Expected Shortfall (*ES*) $ES_{0.95}=E[L|L>VaR_{0.95}]$.

Ці показники дозволяють прогнозувати не лише середній рівень збитків, а й очікувані максимальні втрати в гірших сценаріях.

## 2. Експериментальні результати

Методика була протестована на модельному наборі даних, що включає понад 20 000 записів про кіберінциденти різних типів. За результатами калібрування встановлено, що веб–атаки є найпоширенішими (38% від усіх подій), але найбільші збитки пов'язані з витоком даних, де максимальні втрати в окремих випадках перевищували 250 тис. доларів.

Симуляція 50 річних сценаріїв показала такі результати:

Середні річні очікувані збитки (Mean Annual Loss): MAL=1.84 млн. дол.

95% VaR (максимальний збиток у 95% сценаріїв): $VaR_{0.95}$=3.21 млн.дол.

Expected Shortfall (очікувані збитки в найгірших 5% років): $ES_{0.95}$=4.57 млн. дол.

Після моделювання ефективності засобів кіберзахисту (MFA, WAF, аналітика поведінки, регулярні тренінги персоналу) встановлено, що комбіновані заходи дозволяють:

- зменшити частоту інцидентів на 27%;
- знизити середню вартість інциденту на 11%;
- скоротити річні очікувані збитки приблизно на 32%, тобто: MALпісля≈1.25 млн. дол.

Ці результати демонструють здатність методології чітко визначати економічну ефективність заходів безпеки, що робить її дієвим інструментом для бюджетування та планування кіберзахисту.

**Висновки.** Запропонована методологія кількісного моделювання кіберризиків забезпечує комплексний підхід до аналізу можливих втрат

організації, поєднуючи статистичні моделі, сценарне прогнозування та симуляційні методи. Вона дозволяє враховувати як часті маловитратні інциденти, так і рідкісні події з катастрофічними наслідками, формувати реалістичні криві ризику та визначати ефективність заходів безпеки на основі кількісних показників. Експериментальні дослідження підтверджують, що застосування методології дає змогу суттєво підвищити точність управління кіберризиками, покращити розподіл ресурсів та забезпечити обґрунтованість управлінських рішень.

**Перелік використаних джерел.**

1. Albina Orlando Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk. *Risks*, 2021, Vol. 9, Issue 10, 184, pp. 1–12.

2. Bentley M., Stephenson A., Toscas P., Zhu Z. A Multivariate Model to Quantify and Mitigate Cybersecurity Risk. *Risks*, 2020, Vol. 8, Issue 2, Article 61, pp. 1–20.

3. Dzhamtyrova R., Maple C. Dynamic cyber risk estimation with Competitive Quantile Autoregression. *Data Mining and Knowledge Discovery*, 2022, Vol. 36, pp. 513–536.