СЕКЦІЯ XIV.
СИСТЕМНИЙ АНАЛІЗ, МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ

DOI 10.62731/mcnd-06.03.2026.002

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНКИ ВТРАТ ОРГАНІЗАЦІЇ ВІД ІНФОРМАЦІЙНИХ ЗАГРОЗ

Якименко Юрій Михайлович
ORCID ID: 0000-0002-6848-852X
канд. військ. наук, доцент,
доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, м. Київ, Україна

В сучасному світі інформація перетворилася на один з найцінніших активів будь-якої організації. Водночас із зростанням її значущості збільшується і кількість інформаційних загроз, які можуть призвести до значних фінансових, репутаційних та операційних втрат. Розуміння потенційних збитків від реалізації таких загроз є критично важливим для побудови ефективної системи інформаційної безпеки та прийняття обґрунтованих управлінських рішень щодо розподілу ресурсів на її забезпечення.

Для ефективної оцінки потенційних втрат необхідно чітко розуміти, з якими саме загрозами може зіткнутися організація та які наслідки ці загрози можуть мати. Інформаційні загрози можна класифікувати за різними ознаками [1]. Однією з поширених класифікацій є поділ загроз за аспектом інформаційної безпеки, на який вони спрямовані:

- Загрози конфіденційності: полягають у неправомірному доступі до інформації, що призводить до її розголошення або витоку. Це може стосуватися персональних даних, комерційної таємниці, державних секретів тощо.
- Загрози цілісності: спрямовані на несанкціоновану зміну або знищення інформації. Це може призвести до спотворення даних, підробки документів, порушення роботи систем.
- Загрози доступності: полягають у блокуванні доступу до інформації або інформаційних ресурсів для легітимних користувачів [2].

Прикладами можуть бути DDoS-атаки, вихід з ладу обладнання, програмні збої.

За джерелом виникнення загрози можна поділити на [1, 3]:

• Зовнішні: дії кіберзлочинців, хакерів, конкурентів, недобросовісних партнерів, стихійні лиха [1].

• Внутрішні: умисні або випадкові дії персоналу організації, відмови технічних засобів, помилки програмного забезпечення. Людський фактор часто відіграє значну роль у реалізації внутрішніх загроз.

Інші класифікації можуть враховувати спосіб реалізації загрози (наприклад, використання шкідливого програмного забезпечення, соціальна інженерія), об'єкт атаки (сервери, робочі станції, мережеве обладнання, дані) тощо. Важливо розуміти, що конкретний набір загроз є унікальним для кожної організації та залежить від сфери її діяльності, використовуваних технологій, рівня захищеності та інших факторів [3].

Реалізація інформаційних загроз може призвести до різноманітних втрат для організації. Ці втрати можна умовно поділити на прямі та непрямі (опосередковані), а також на кількісно вимірювані (фінансові) та якісні (нефінансові) – показано в табл. 1.

Таблиця 1

Типи можливих витрат

Тип	Приклад
Прямі фінансові	• Втрати від простою систем та бізнес-процесів]. • Витрати на відновлення даних та працездатності систем. • Витрати на розслідування. • Штрафи та компенсації за порушення законодавства або договірних зобов'язань. • Втрати від шахрайських операцій
Непрямі фінансові	• Втрата ринкової частки та конкурентних переваг. • Зниження вартості акцій компанії. • Витрати на відновлення ділової репутації. • Втрата клієнтів та партнерів через підрив довіри. • Додаткові витрати на аудит безпеки та впровадження нових заходів захисту після інциденту.
Нефінансові (якісні)	• **Репутаційні втрати.** Погіршення іміджу компанії в очах клієнтів, партнерів, інвесторів та громадськості. Це один з найскладніше оцінюваних, але часто найвідчутніших видів втрат. • **Втрата довіри.** Зниження рівня довіри з боку клієнтів, співробітників та партнерів. • **Порушення нормативно-правових вимог.** Невідповідність законодавчим та регуляторним нормам (наприклад, у сфері захисту персональних даних, банківської таємниці), що може призвести не лише до штрафів, але й до призупинення діяльності.

Продовження табл. 1

Тип	Приклад
	• **Соціальні та психологічні наслідки.** Стрес для співробітників, зниження їхньої продуктивності, плинність кадрів. • **Втрата інтелектуальної власності.** Розголошення ноу-хау, патентів, авторських розробок. • **Операційні збої.** Порушення нормального функціонування бізнес-процесів, навіть якщо вони не призводять до негайних прямих фінансових збитків.

[авторська розробка]

Після ідентифікації потенційних загроз та типів втрат, наступним важливим кроком є вибір та застосування адекватних теоретичних підходів для їх оцінки. Оцінка збитків від інформаційних загроз може здійснюватися за допомогою різних методів, які умовно поділяються на кількісні та якісні [4, 6]. Кожен з цих підходів має свої переваги, недоліки та сфери застосування.

Якісні методи оцінки спрямовані на визначення рівня ризику та потенційних збитків на основі експертних оцінок, описів та сценаріїв без точного грошового вираження. Вони допомагають пріоритезувати загрози та вразливості, коли кількісні дані відсутні або їх важко отримати.

•Метод сценаріїв. Передбачає розробку детальних сценаріїв реалізації загроз та аналіз їх можливих наслідків. Експерти оцінюють ймовірність кожного сценарію та серйозність його впливу на діяльність організації.

•Експертні оцінки. Залучення фахівців з інформаційної безпеки, представників бізнес-підрозділів та керівництва для оцінки потенційних збитків за певною шкалою (наприклад, низький, середній, високий рівень збитків) [6].

•Матриці ризиків (Risk Matrix). Дозволяють візуалізувати ризики шляхом зіставлення ймовірності виникнення загрози та рівня потенційної шкоди (впливу) [4, 6]. Ризики потрапляють у різні зони матриці (наприклад, низький, середній, високий, критичний), що допомагає визначити їх пріоритетність.

•Аналіз дерева атак (Attack Tree Analysis). Графічний метод моделювання можливих шляхів реалізації атаки на систему. Дозволяє ідентифікувати різні послідовності дій, що можуть призвести до успішної атаки, та оцінити ймовірність і наслідки кожного шляху.

• Метод Делфі. Ітеративна процедура анкетування групи експертів з метою досягнення консенсусу щодо оцінки ризиків та збитків [7].

Основні фактори, що враховуються при якісному аналізі, включають:

• Серйозність збитку (Damage): наскільки значними будуть наслідки атаки?

• Відтворюваність (Reproducibility): наскільки легко відтворити атаку?

• Експлуатованість (Exploitability): скільки зусиль потрібно для реалізації атаки?

• Кількість постраждалих користувачів (Affected users): скільки людей буде зачеплено?

• Виявлюваність (Discoverability): наскільки легко виявити загрозу чи вразливість?

Перевагами якісних методів є відносна простота застосування, менші часові та ресурсні затрати порівняно з кількісними методами, а також можливість використання в умовах невизначеності та браку точних даних. Недоліком є суб'єктивність оцінок та неможливість отримати грошове вираження збитків [2].

Кількісні методи оцінки мають на меті надати числову, зазвичай грошову, оцінку потенційним збиткам [2]. Це дозволяє більш обґрунтовано підходити до аналізу рентабельності інвестицій в заходи безпеки (Cost-Benefit Analysis) [2, 8].

Основні поняття та показники, що використовуються в кількісній оцінці:

Вартість активу (Asset Value - AV): грошова вартість інформаційного активу для організації.

Фактор впливу (Exposure Factor - EF): відсоток втрати вартості активу внаслідок реалізації конкретної загрози (знаходиться в діапазоні від 0 до 100%) [2].

Одинична очікувана втрата (Single Loss Expectancy - SLE): грошова сума збитку від одного інциденту. Розраховується як:

$$SLE=AV\times EF \quad (1)$$

Річна частота виникнення (Annualized Rate of Occurrence - ARO): очікувана кількість разів, яку певна загроза може реалізуватися протягом року [2].

Річні очікувані втрати (Annualized Loss Expectancy - ALE): загальна сума очікуваних збитків від конкретної загрози протягом року. Розраховується як:

$$ALE=SLE\times ARO \quad (2)$$

Існують інші кількісні методики та моделі, що використовуються в дослідницьких цілях в сфері кібербезпеки:

FAIR (Factor Analysis of Information Risk). Структурована методологія для кількісної оцінки інформаційних ризиків у фінансовому вираженні. Вона допомагає розкласти ризик на фактори, що піддаються оцінці, такі як частота подій загрози (Threat Event Frequency - TEF) та величина втрат (Loss Magnitude - LM) [5, 8].

Аналіз дерева рішень (Decision Tree Analysis). Використовується для моделювання різних можливих наслідків інциденту та пов'язаних з ними витрат і ймовірностей [6].

Метод Монте-Карло (Monte Carlo Simulation). Статистичний метод, що дозволяє моделювати розподіл можливих збитків шляхом багаторазового розрахунку з випадково генерованими вхідними даними в межах заданих діапазонів [8]. Це дає змогу отримати не просто точкову оцінку, а ймовірнісний розподіл втрат.

Перевагою кількісних методів є об'єктивність оцінок (за умови наявності достовірних даних) та можливість вираження ризиків і збитків у фінансових показниках, що полегшує прийняття рішень щодо інвестицій у безпеку [2]. Однак ці методи є більш складними, вимагають значних зусиль для збору даних та можуть бути непридатними для оцінки всіх типів втрат (наприклад, репутаційних).

Переваги якісних та кількісних підходів можна поєднати , якщо використати числові шкали для оцінки ймовірності та впливу. Але ці шкали не завжди можуть бути пов'язані безпосередньо з грошовими одиницями, а відображати тільки рівні (наприклад, від 1 до 5) [6]. Результатом може бути, наприклад, розрахунок індексу ризику втрат.

Вибір конкретного підходу або комбінації підходів залежить від цілей оцінки, доступності даних, ресурсів, корпоративної культури та специфіки самої організації. Часто на практиці використовується комбінований підхід, де спочатку проводиться якісний аналіз для ідентифікації та пріоритезації ключових ризиків, а потім для найбільш критичних з них застосовуються кількісні методи оцінки.

Висновки. На основі аналізу класифікації інформаційних загроз, типів можливих втрат та існуючих теоретичних підходів до їх оцінки, може бути розроблена концептуальна модель, яка б структурувала процес оцінки втрат організації. Ця модель повинна бути достатньо

гнучкою, щоб адаптуватися до різних умов та масштабів організацій, і водночас надавати чіткий алгоритм дій - від ідентифікації активів та загроз і закінчуючи розрахунком інтегрального показника втрат та формуванням звітності.

Список використаних джерел:

1. Класифікація загроз безпеці та пошкодження даних у комп'ютерних системах. *Https://www.kievoit.ippo.kubg.edu.ua/kievoit/2013/102/102.html*
2. Top 5 Risk Assessment Methodologies in Cybersecurity 2025 - Sprinto. 8 . *Https://sprinto.com/blog/risk-assessment-methodologies/*
3. What is a Cybersecurity Risk Assessment? - IBM. How to perform qualitative & quantitative security risk analysis - Infosec. *Https://netwave.ua/blog/sho-take-analiz-informacijnoyi-bezpeki-metodi-analizu-rizikiv-ib/*
4. How to perform qualitative & quantitative security risk analysis - Infosec. *Https://www.infosecinstitute.com/resources/general-security/perform-qualitative-quantitative-security-risk-analysis/*
5. Quantifying the Cost of Cybersecurity Risks vs. Investments - Legato Security. *Https://www.legatosecurity.com/blog/quantifying-the-cost-of-cybersecurity-risks-vs-investments*
6. Qualitative vs. Quantitative Cybersecurity Risk Assessment: What's the Difference? – SecurityScorecard. *Https://securityscorecard.com/blog/qualitative-vs-quantitative-risk-assessment*
7. How to Perform a Successful IT Risk Assessment - Hyperproof. *Https://hyperproof.io/resource/it-risk-assessment/*
8. Getting started with cyber risk quantification: Key concepts - Scrut Automation. *Https://www.scrut.io/post/getting-started-with-cyber-risk-quantification-key-concepts*