

МЕТОДИ ВЗАЄМОЗВ'ЯЗКУ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ДЛЯ ОЦІНЮВАННЯ РИЗИКІВ У КІБЕРСИСТЕМАХ

Я. Г. Федірко^{1,а}, В. І. Полуциганова¹

¹ Навчально-науковий Фізико-технічний інститут

Анотація

У цій статті запропоновано удосконалену математичну модель оцінки ризиків кібербезпеки, яка базується на врахуванні не лише наявності загроз, але й їхньої здатності експлуатувати конкретні вразливості інформаційної системи. На відміну від традиційних підходів, дана модель враховує взаємозв'язки між загрозами, які можуть підсилювати одна одну, а також вводить кількісну оцінку ступеня експлуатації вразливостей. Модель формалізує залежність ймовірності реалізації загрози від критичності вразливостей, які вона може експлуатувати, та від наявності супутніх загроз. Аналіз проведено шляхом порівняння з існуючими моделями та методиками оцінки ризиків.

Ключові слова: кібербезпека, оцінка ризиків, загрози, вразливості, матриця експлуатації, сумісність загроз.

Вступ

В сучасному цифровому світі, де кіберсистеми стають все складнішими та взаємопов'язаними, розуміння взаємозв'язку між вразливостями та загрозами є критично важливим для ефективного оцінювання та управління кіберзагрозами. Оцінка кіберзагроз передбачає не лише ідентифікацію потенційних небезпек, але й аналіз того, як ці небезпеки можуть використовувати слабкі місця в системі для завдання шкоди.

1. Стандартний метод оцінювання ризику

Традиційно ризик у сфері кібербезпеки розглядається як функція ймовірності реалізації загрози та потенційного збитку від її реалізації:

$$R = P \cdot D$$

де R – ризик, P – ймовірність, D – збиток. Проте така формула є занадто спрощеною і не враховує багатьох важливих аспектів взаємодії загроз та вразливостей в реальних інформаційних системах. Основними недоліками традиційних підходів до оцінки ризиків є:

1. Недостатнє врахування взаємозв'язків між різними загрозами;
2. Ігнорування залежності реалізації загрози від наявності конкретних вразливостей;
3. Відсутність диференціації ступеня експлуатації вразливостей різними загрозами;
4. Спрощене представлення критичності вразливостей без урахування їх специфіки.

Метою даного дослідження є розробка більш досконалої математичної моделі оцінки ризиків, яка враховуватиме не лише наявність загроз та їхній потенційний вплив, але й конкретні механізми реалізації загроз через експлуатацію вразливостей, а також взаємозв'язки між різними загрозами.

2. Аналіз існуючих моделей оцінки ризиків кібербезпеки

2.1. Огляд традиційних підходів

2.1.1. Якісні методи оцінки ризиків

Якісні методи оцінки ризиків, такі як матриці ризиків, набули широкого поширення завдяки своїй простоті та зрозумілості. У таких методах ризики класифікуються за якісними категоріями (високий, середній, низький) на основі суб'єктивних оцінок ймовірності та впливу. До найбільш відомих якісних методів належать:

- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [1];
- Методика NIST SP 800-30 [2].

Основним недоліком якісних методів є суб'єктивність оцінок та обмежені можливості для точного порівняння та пріоритизації ризиків.

2.1.2. Кількісні методи оцінки ризиків

Кількісні методи оцінки ризиків передбачають числову оцінку ймовірності та впливу загроз, що дозволяє отримати більш точні та об'єктивні результати. До найбільш поширених кількісних методів належать:

- FAIR (Factor Analysis of Information Risk) [3];

^аyarfed-ipt25@lil.kpi.ua

- Методика аналізу дерев подій та дерев відмов [4].

Проте навіть ці більш досконалі методи мають обмеження, пов'язані з необхідністю збору великої кількості даних та складністю врахування всіх взаємозв'язків між елементами систем [5, 6].

2.2. Особливості та недоліки існуючих моделей

2.2.1. Модель FAIR

Модель FAIR (Factor Analysis of Information Risk) [2] є одним із найбільш розвинених підходів до кількісної оцінки ризиків кібербезпеки. Вона базується на декомпозиції ризику на складові частини, включаючи частоту виникнення загрози та величину потенційного впливу. Незважаючи на свої переваги, модель FAIR має певні обмеження:

- Недостатнє врахування взаємозв'язків між різними загрозами;
- Відсутність формалізованого механізму оцінки впливу вразливостей на ймовірність реалізації загроз;
- Складність збору статистичних даних для точної оцінки параметрів моделі [6].

2.2.2. Підхід NIST SP 800-30

Методика, описана в NIST SP 800-30 [3], пропонує структурований підхід до оцінки ризиків інформаційної безпеки, що включає ідентифікацію загроз та вразливостей, оцінку ймовірності та впливу, а також визначення рівня ризику. Однак цей підхід також має певні недоліки:

- Переважно якісний характер оцінок;
- Обмежена формалізація взаємозв'язків між загрозами та вразливостями;
- Відсутність математичної моделі для кількісної оцінки впливу вразливостей на ймовірність реалізації загроз.

2.2.3. Модель аналізу графів атак

Модель аналізу графів атак є потужним інструментом для моделювання шляхів реалізації загроз через послідовну експлуатацію вразливостей. Вона дозволяє визначити найбільш ймовірні та небезпечні сценарії атак. Проте ця модель також має обмеження:

- Складність побудови повного графа атак для реальних систем;
- Недостатнє врахування кількісних характеристик вразливостей;
- Обмежені можливості для моделювання одночасної дії кількох загроз.

3. Ідея власної моделі оцінки ризиків

3.1. Формальний опис моделі

Запропонована модель базується на розширенні традиційного підходу до оцінки ризиків шляхом вве-

дення додаткових параметрів та залежностей, що відображають взаємозв'язки між загрозами та вразливостями. Введемо наступні позначення:

- $T = \{T_1, \dots, T_n\}$ – множина загроз;
- $V = \{V_1, \dots, V_m\}$ – множина вразливостей;
- $E_{ij} \in [0, 1]$ – матриця експлуатації: ступінь, в якому загроза T_i експлуатує вразливість V_j (0 — не експлуатує, 1 — повна експлуатація);
- $c_j \in [0, 1]$ – критичність (важливість) вразливості V_j ;
- S – матриця сумісності між загрозами, де $s_{ki} \in [0, 1]$ відображає ступінь впливу загрози T_k на ймовірність реалізації загрози T_i ;
- p_i – базова ймовірність загрози T_i ;
- D_i – потенційний збиток від реалізації загрози T_i .

Ключовою особливістю запропонованої моделі є визначення скоригованої ймовірності загрози $\tilde{p}_i$, яка враховує як наявність та критичність відповідних вразливостей, так і вплив інших загроз:

$$\tilde{p}_i = p_i \cdot \left(\sum_{j=1}^m E_{ij} \cdot c_j \right) + \sum_{k \neq i} s_{ki} \cdot p_k$$

Ця формула відображає два ключові аспекти:

- Перша частина $\left(p_i \cdot \sum_{j=1}^m E_{ij} \cdot c_j \right)$ враховує вплив вразливостей, які може експлуатувати загроза T_i , з урахуванням їхньої критичності та ступеня експлуатації;
- Друга частина $\left(\sum_{k \neq i} s_{ki} \cdot p_k \right)$ відображає вплив інших загроз на ймовірність реалізації загрози T_i .

Загальний ризик системи визначається як сума ризиків від усіх загроз:

$$R = \sum_{i=1}^n \tilde{p}_i \cdot D_i$$

3.2. Обґрунтування запропонованого підходу

Запропонована модель базується на кількох важливих спостереженнях щодо природи кіберзагроз та вразливостей:

1. Залежність реалізації загроз від вразливостей: Для успішної реалізації загрози необхідна наявність відповідних вразливостей. Модель враховує не лише наявність вразливостей, але й ступінь їх критичності та можливість експлуатації конкретними загрозами.
2. Взаємозв'язок між загрозами: Реалізація однієї загрози може підвищувати ймовірність реалізації інших загроз. Наприклад, успішна реалізація загрози компрометації облікових даних може підвищувати ймовірність несанкціонованого доступу до системи.
3. Диференційований підхід до оцінки вразливостей: Різні вразливості мають різну критичність та можуть бути експлуатовані різними загрозами з різною ефективністю. Модель враховує ці відмінності через матрицю експлуатації E_{ij} та коефіцієнти критичності c_j .

3.3. Порівняння з традиційними моделями

На відміну від традиційної формули ризику $R = P \cdot D$, запропонована модель враховує додаткові фактори та взаємозв'язки, що дозволяє отримати більш точну та реалістичну оцінку ризиків. Порівняно з моделлю FAIR, яка також прагне до кількісної оцінки ризиків, запропонована модель надає більш формалізований механізм врахування впливу вразливостей на ймовірність реалізації загроз. На відміну від підходу аналізу графів атак, який фокусується на послідовності дій злоумисника, запропонована модель зосереджується на кількісній оцінці взаємозв'язків між загрозами та вразливостями, що дозволяє більш точно оцінити загальний ризик системи.

4. Висновки

Взаємозв'язок між вразливостями та загрозами є фундаментальною концепцією в оцінці кіберзагроз. Запропонована модель оцінки ризиків кібербезпеки на основі взаємозв'язку загроз та вразливостей дозволяє більш точно та комплексно оцінювати ризики, враховуючи не лише наявність загроз та їхній потенційний вплив, але й конкретні механізми реалізації загроз через експлуатацію вразливостей, а також взаємозв'язки між різними загрозами. Ключовими перевагами запропонованої моделі є:

1. Комплексний підхід до оцінки ризиків, що враховує взаємозв'язки між загрозами та вразливостями;

2. Математична формалізація цих взаємозв'язків, що дозволяє кількісно оцінювати ризики;
3. Можливість пріоритизації заходів захисту на основі аналізу компонентів моделі.

Перелік використаних джерел

1. *Alberts C., Dorofee A.* OCTAVE Method Implementation Guide Version 2.0 : tech. rep. / Carnegie Mellon University. — Carnegie Mellon University, 2001. — 110 p.
2. *Standards N. I. of, Technology.* NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View : tech. rep. / National Institute of Standards ; Technology. — Gaithersburg, MD, 2011. — 53 p.
3. *HubSpot.* Introduction to Information Security Risk Assessment using FAIR (Factor Analysis of Information Risk). — n.d. — URL: <https://www.hubspot.com> ; Accessed: 2025-05-06.
4. *Copae M.* Attribute-Based Attack-Defense Trees for Security Analysis : Bachelor's thesis / Copae Marius. — Enschede : University of Twente, 2024.
5. *Архипов О.* Вступ до теорії ризиків: інформаційні ризики : монографія. — Київ : Нац. акад. СБУ, 2015.
6. *Cox Louis Anthony J.* Risk Analysis of Complex and Uncertain Systems. — New York : Springer Science+Business Media, LLC, 2009.