ВИЗНАЧЕННЯ СТРАТЕГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ БІМАТРИЧНІЙ ГРІ ЗЛОВМИСНИКА ТА CISO

Ібрагімова Д. Ф., Добринін І. С.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна

E-mail: diana.ibrahimova@nure.ua,
ihor.dobrynin@nure.ua

Abstract

The study presents a comprehensive approach for assisting the Chief Information Security Officer (CISO) in selecting optimal security strategies based on game-theoretical models. Using financial metrics and quantitative risk assessments, this approach balances strategic investments in security against the threat landscape. Comparative analysis of game-theoretical criteria enables a multi-dimensional view, demonstrating how different strategies adapt to varying risks and investment levels.

Із розвитком галузі інформаційних технологій кібератаки стають дедалі більш частими та небезпечними. Це викликає гостру потребу ефективного захисту інформаційних активів організацій. Існує низка документів, на які може спиратись організація у вирішенні цього питання. Наприклад, NIST Cybersecurity Framework (NIST CSF) дає певні рекомендації, як має працювати захист інформації [1], стандарт ISO/IEC 27001:2022 висуває певні вимоги до побудови системи управління інформаційною безпекою (СУІБ) [2]. Проте, вибір конкретної стратегії захисту залишається за головним спеціалістом з інформаційної безпеки (Chief Information Security Officer – CISO), який повинен розробити та обрати таку стратегію захисту, яка не тільки відповідає вимогам стандартів, а також раціонально використовує ресурси організації. Зважаючи на це, метою даної роботи є запропонувати CISO рекомендації щодо вибору найкращого підходу для визначення оптимальної стратегії захисту інформації в організації.

Одним із найбільш вдалих підходів є теорія ігор, яка дозволяє змоделювати взаємодію CISO і зловмисника у вигляді змагання та передбачити можливий результат. Ігрова концепція пропонує багато різних методів для побудови моделі змагання [3]. Наприклад, динамічні ігри ґрунтуються на поетапному прийнятті рішень у ході гри в залежності від дій противника, але в умовах реальних загроз взаємодія гравців частіш за все є одноразовою. Інший підхід – дуальні ігри з нульовою сумою, які передбачають, що виграші опонентів є протилежними [4], але нульова сума є скоріш окремим випадком, адже успіх зловмисника не обов'язково призводить до максимального збитку для CISO. Ще один наявний вид взаємодії – ігри з природою, які спираються на те, що одним із гравців є «природа», яка діє хаотично, але в кібербезпеці противник – не випадковий фактор. Тому, всі наведені підходи не є доцільними в нашому випадку, оскільки важливо врахувати раціональні дії обох сторін.

Отже, раціональним варіантом є побудова моделі на основі біматричної гри з ненульовою сумою, яка передбачає що кожен із гравців має свої стратегії та виграші, які представлені у вигляді платіжних матриць. Біматрична гра є одноходовою та ґрунтується на тому, що обидві сторони обирають певні стратегії, після чого розраховується результат зіткнення.

Навіть в межах обраного підходу, теорія ігор пропонує різні варіанти прийняття рішень. Тому, поставимо задачу – порівняти наявні методи та надати CISO рекомендацію щодо вибору з них тієї, яка задовольняє його потреби. Для цього, почнімо із загальних засад та попередніх кроків.

Введемо позначення. Стратегії CISO позначаємо $S_A = \{S_{A1}, S_{A2}, S_{A3}\}$, зловмисника – $S_H = \{S_{H1}, S_{H2}, S_{H3}\}$. Індекс і позначає «поточну» стратегію зловмисника серед усіх можливих, j – стратегію CISO. Стовпці та рядки матриці позначають стратегії CISO та зловмисника відповідно. На

перетині двох стратегій можна побачити виграші (збитки): G_{Hij} позначає виграш зловмисника, G_{Aij} – CISO. Матриці виграшів надано на рис. 1. Так як в даній роботі метою є вибір стратегії для CISO, у подальшому працюватимемо з першою матрицею.

	S_{A1}	S_{A2}	S_{A3}
S_{H1}	G_{A11}	G_{A12}	G_{A13}
S_{H2}	G_{A21}	G_{A22}	G_{A23}
S_{H3}	G_{A31}	G_{A32}	G_{A33}

	S_{A1}	S_{A2}	S_{A3}
S_{H1}	G_{H11}	G_{H12}	G_{H13}
S_{H2}	G_{H21}	G_{H22}	G_{H23}
S_{H3}	G_{H31}	G_{H32}	G_{H33}

Рис. 1. Платіжні матриці CISO та зловмисника відповідно

Як було сказано вище, елементи платіжної матриці є виграшами CISO та зловмисника в залежності від обраних стратегій. Щоб розрахувати виграш CISO для конкретної пари стратегій, необхідно взяти до уваги результат їхнього зіткнення. Виграш є результатом взаємодії обраної стратегії CISO S_{Aj} та стратегії зловмисника S_{Hi}. Значення виграшу показує різницю між потенційними втратами CISO в разі успішної атаки і вартістю його стратегії захисту:

$$G_{Aij} = -L_{ij} - C_{Aj} \ , \tag{1}$$

де L_{ij} – потенційні збитки CISO у разі успішної і-ї атаки S_H та обраної j-ї стратегії S_A,

C_{Aj} – витрати CISO на реалізацію j-ї стратегії захисту S_A.

У формулі (1) значення потенційних збитків та витрат на захист є від'ємними для підкреслення, що виграш для CISO в будь-якому разі буде мати витрати не залежно від успіху стратегії. У разі успішної атаки, потенційні збитки будуть залежати від того, наскільки значущим є цей актив для системи та яку його частку втрачено. Для обчислення потенційних збитків скористаємося формулою:

$$L_{ij} = AV \cdot EF_{ij} \ , \tag{2}$$

де AV –вартість активу (Asset Value), що захищається,

EF_{ij} – фактор впливу (Exposure Factor) успішної і-ої атаки при виборі j-стратегії СУІБ.

Кажучи про управління ризиками інформаційної безпеки, CISO має справу із невизначеністю, адже тип потенційної атаки заздалегідь не відомий. Тому, для таких випадків ефективним є вибір стратегії, спираючись на критерії оптимальності [5].

Критерій мінімаксу орієнтований на найгірший можливий результат. Спираючись на цей критерій, CISO має обрати стратегію, яка мінімізує максимальні втрати, незалежно від ймовірності успіху зловмисника:

$$S_m^* = \min_{S_{Aj} \in S_A} \max_{S_{Hi} \in S_H} |G_{Aij}|, \tag{3}$$

тобто для кожної фіксованої стратегії CISO S_{Aj} визначається найбільші втрати, які можуть виникнути, якщо атакуючий обере найгіршу для CISO стратегію S_{Hi}, а серед всіх найбільших витрат обирається мінімальна.

Критерій мінімаксу, з одного боку, забезпечує максимальний захист у найгіршому випадку, але з іншого – може бути надмірно категоричним, особливо у випадках обмеженого бюджету на розробку та підтримку СУІБ. Приділяючи увагу найгіршому результату, він не враховує ймовірність дій зловмисника.

Цю проблему вирішує критерій Лапласа. Використання критерію Лапласа базується на припущенні, що всі ймовірності дій опонента є рівномірно розподіленими. Використовуючи цей критерій, CISO обчислює середні витрати для кожної стратегії за формулою:

$$E(G_A) = \frac{1}{m} \sum_{i=1}^{m} G_{Aij} \ , \tag{4}$$

де m – кількість можливих стратегій зловмисника,

та обирає стратегію, яка їх мінімізує:

$$S_L^* = \arg\min_{S_{Aj} \in S_A} |E(G_A)| . \quad (5)$$

Критерій Лапласа зручний у випадках, коли інформація про ймовірність виникнення певної атаки невідома. Однак у разі доступності даних про частоту та ймовірність, можливо обрати більш ефективну стратегію на основі критерія Байєса.

Критерій математичного очікування Байєса передбачає, що CISO відома ймовірність, з якою зловмисник здійснить певну атаку. CISO повинен знати вразливості системи, які можуть стати векторами атак, а отже може передбачити ймовірність їх виникнення, використовуючи відомі бази даних, наприклад MITRE ATT&CK [6] чи CVEdetails [7]. За критерієм Байєса очікувані втрати обчислюються як середньозважена сума втрат для кожної можливої стратегії зловмисника, де ваги відповідають ймовірностям вибору хакером відповідної стратегії:

$$E(G_A) = \sum_{i=1}^{m} P(S_{Hi}) \cdot G_{Aij} , \quad (6)$$

де $P(S_{Hi})$ – ймовірність вибору зловмисником і-ї стратегії S_H.

Метою CISO є вибір стратегії, яка мінімізує очікувані втрати:

$$S_B^* = \arg\min_{S_{Aj} \in S_A} |E(G_A)| \quad (7)$$

Отже, всі розглянуті критерії будують модель змагань за окремим підходом: критерій мінімакса фокусується на максимальному зниженні ризику, Лапласа – на рівноважності сценаріїв, а Байєса – на ймовірності подій. Тому є висока ймовірність того, що в ході кількісних розрахунків кожен із критеріїв надасть відмінні одне від одного результати.

Враховуючи це, при виборі критерія оптимальності CISO слід спиратись на таки параметри, як розмір бюджету на впровадження СУІБ, наявність даних про попередні інциденти та критичність відомих вразливостей системи.

Якщо CISO відома інформація про ймовірності здійснення атак, оптимальним є вибір стратегії за критерієм Байєса, яка забезпечує зниження найімовірнішого ризика та збитків. Критерій мінімакса є корисним для попередження значних критичних втрат, коли бюджет на заходи безпеки є необмеженим, адже уникнення найгіршого сценарію в більшості випадків потребує значних ресурсів. Використання критерію Лапласа є доцільним для нових систем або в нестабільному середовищі загроз, коли статистичні дані недоступні, приблизні ймовірності атак важко визначити, але бюджет – обмежений.

Література

1. NIST CSWP 29. The NIST Cybersecurity Framework (CSF) 2.0. Effective from 2024-02-26. Official edition. Gaithersburg, Maryland, USA, 2024. 32 p.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL : https://www.iso.org/ru/standard/27001 (дата звернення: 01.11.2024)
3. Теорія ігор: курс лекцій : Електрон. мережне навч. вид. / уклад. Л. В. Барановська. Київ : Нац. техн. ун-т України «Київ. політехн. ін-т ім. Ігоря Сікорського», 2022. 254 с.
4. Добринін І., Борова М. Оптимізація вибору варіанту побудови системи захисту інформації від атак при антагоністичній грі. *Системи озброєння та військова техніка*. 2018. Т. 2, № 54. С. 89 – 93.
5. Ус С., Коряшкіна Л. Моделі й методи прийняття рішень : навч. посіб. Дніпропетровськ : ДВНЗ «Нац. гірн. ун-т», 2014. 300 с.
6. MITRE ATT&CK®. MITRE ATT&CK®. URL : https://attack.mitre.org (дата звернення: 18.10.2024).
7. CVE security vulnerability database. Security vulnerabilities, exploits, references and more. URL : https://www.cvedetails.com (дата звернення: 18.10.2024).