УДК 519.83:004.056

АНАЛІЗ СТІЙКОСТІ РІВНОВАГИ НЕША В БІМАТРИЧНІЙ МОДЕЛІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Ібрагімова Д. Ф., Добринін І. С.
e-mail: diana.ibrahimova@nure.ua, ihor.dobrynin@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В. В. Поповського
м. Харків, Україна

This work examines how changes in attack probabilities influence the equilibrium structure in a cybersecurity strategy selection model. The interaction between a defender (CISO) and an attacker is modeled as a bimatrix game with two defense strategies and two attack strategies. The payoff function is based on potential losses determined by the asset value, exposure factors, and the cost of security strategies. A threshold probability value is derived that indicates the point at which the optimal defense strategy changes. The results show how variations in attack probabilities affect the rational choice of defense strategies and support more flexible decision-making in information security management.

В умовах зростання кількості та складності кіберзагроз підвищується актуальність формалізованих методів вибору стратегії побудови системи управління інформаційною безпекою (СУІБ). Задача вибору стратегії може бути розглянута як взаємодія між головним спеціалістом з інформаційної безпеки (Chief Information Security Officer – CISO) та потенційним зловмисником.

Біматричні ігрові моделі дозволяють формалізувати інтереси сторін та визначити рівноважні стратегії. Такий підхід описано в роботі [1]. Зафіксовані значення параметрів моделі дозволяють визначити рівновагу Неша. Разом із тим, параметри є змінними, адже в реальних умовах середовище кіберзагроз є динамічним. У зв'язку з цим постає задача дослідити чутливість рівноважних стратегій до зміни параметрів моделі. Тому метою роботи є проаналізувати вплив характеристик, зокрема ймовірності здійснення атаки, на структуру рівноваги у біматричній грі.

Розглянемо взаємодію між CISO та порушником у вигляді гри розмірності 2×2, зосереджуючись на дослідженні впливу зміни ймовірностей атак. З боку порушника передбачається наявність двох альтернативних стратегій атаки, які утворюють повну групу подій, тоді як CISO може обрати одну з двох стратегій захисту S_1, та S_2, що відрізняються рівнем ефективності та вартістю впровадження: вартість реалізації стратегії S_1 становить 320 тис. у.о., тоді як S_2 – 275 тис. у.о. Вартість активу, що захищається, оцінюється в 2 млн. у.о. Потенційні втрати активу при реалізації атак характеризуються фактором впливу (Exposure Factor), що відображає його частку, яка може бути втрачена у разі успішної стратегії порушника. Для S_1 значення цього показника становить 0,6 для першої атаки та 0,25 для другої, тоді як для S_2 – 0,4 та 0,5 відповідно.

У роботі [1] описане застосування біматричної гри, де виграш (очікувані втрати, G) CISO формуються як різниця між потенційними збитками (добуток вартості головного активу та фактору впливу) та вартістю реалізації стратегії захисту. Використовуючи наведені вище дані разом із підходом [1], обчислюємо зіткнення опонентів, результат якого для CISO наведений на рис. 1.

	Стратегія 1	Стратегія 2
Атака 1	-1520000	-1075000
Атака 2	-820000	-1275000

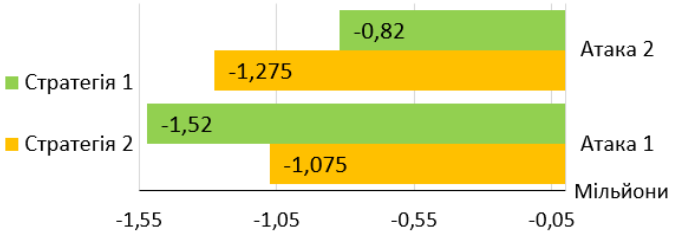

Рисунок 1 – Очікувані втрати головного спеціаліста з інформаційної безпеки при біматричній грі

У межах біматричної гри стан рівноваги Неша відповідає такому поєднанню стратегій, за якого жоден із гравців не має стимулу односторонньо змінювати власну стратегію [2]. Для CISO це значить, що за даних параметрів ризику обрана стратегія мінімізує його очікувані витрати (а отже – є оптимальною) з урахуванням раціональної поведінки порушника. Вихід із стану рівноваги відбувається у випадку зміни параметрів середовища (зокрема, ймовірностей атак), коли попередня стратегія перестає бути оптимальною.

Порівнюючи виграші CISO для S_1, та S_2, можна визначити порогове значення ймовірності атаки p^*, при якому CISO доцільно змінити стратегію:

$$G_1(p^*) = G_2(p^*)\ . \qquad (1)$$

Отримане порогове значення інтерпретується наступним чином: коли ймовірність застосування зловмисником його першої стратегії (p_1) менше за p^*, економічно доцільною є стратегія S_1, а при $p_1 > p^*$ перевагу набуває стратегія S_2.

На основі побудованої платіжної матриці, очікувані втрати CISO за умови вибору S_1 описуються функцією:

$$G_1(p_1) = -1520000p_1 + (-820000)(1 - p_1) = -700000p_1 - 820000, \quad (2)$$

а за умови вибору S_2:

$$G_2(p_1) = -1075000p_1 + (-1275000)(1 - p_1) = 200000p_1 - 1275000. \quad (3)$$

Для визначення порогової ймовірності функції (2) та (3) прирівнюються відповідно до умови байдужості між стратегіями (1). Зважаючи на це, розв'язання рівності дає $p^* = 0{,}505$.

Для аналізу отриманих результатів було побудовано графік залежності очікуваних втрат CISO від ймовірності реалізації першої атаки. Точка перетину функцій (2) та (3) відповідає пороговому значенню ймовірності p_1^*. На проміжку $p_1 \in [0{,}1;\ 0{,}505)$ S_1 показує свою перевагу, в той час як на проміжку $p_1 \in (0{,}505;\ 0{,}9]$ оптимальною є S_2. У точці $p_1 = 0{,}505$, що відповідає пороговому значенню, CISO є байдужим до вибору між двома стратегіями, оскільки очікувані втрати в обох випадках є однаковими. Окрім того, що графік дозволяє наочно визначити області, у яких кожна зі стратегій захисту набуває оптимальності, він також демонструє зміну рівноважного стану гри залежно від зміни параметрів середовища загроз.

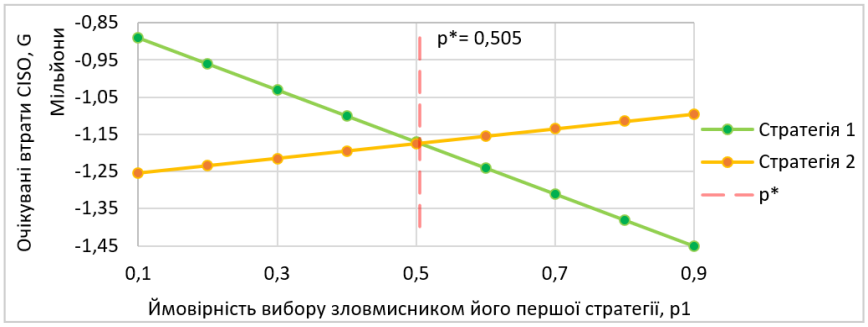

Рисунок 2 – Графічне визначення оптимальної стратегії захисту в залежності від ймовірності реалізації стратегії зловмисника

Таким чином, було з'ясовано, що значення порогової ймовірності атак визначає точку зміни структури рівноваги та характеризує чутливість оптимальної стратегії до змін зовнішнього середовища. Порогові значення доцільно використовувати як інструмент підтримки прийняття рішень при виборі стратегій захисту в системах управління інформаційною безпекою, адже вони дозволяють визначити оптимальну стратегії захисту залежно від актуальної оцінки ймовірностей атак, уникаючи повного перерахунку всієї моделі при зміні параметрів середовища.

Список використаних джерел:

1. Ібрагімова Д. Ф., Добринін І. С. Визначення стратегії захисту інформації при біматричній грі зловмисника та CISO. *«Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2024))* : Міжнар. науково-техн. конф., м. Харків, 13 – 14 листоп. 2024 р. 2024. С. 172 – 174.

2. Теорія ігор: курс лекцій / ред. В. Д. Романенко. Київ : КПІ ім. Ігоря Сікорського, 2022. 245 с.