МОДЕЛЮВАННЯ АДАПТАЦІЇ СТРАТЕГІЙ CISO У ДИНАМІЧНОМУ СЕРЕДОВИЩІ ЗАГРОЗ

Ібрагімова Д.Ф., Добринін І.С.

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

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

Abstract

The study presents an approach to selecting the optimal strategy for an Information Security Management System (ISMS) based on repeated games between the Chief Information Security Officer (CISO) and an attacker. The proposed model reflects the dynamic interaction and adaptation of strategies, allowing an analysis of stability and changes in strategic probabilities over time. The simulation was conducted using an example of an organization with defined set of possible attacks and defense strategies. The results show that equilibrium is not always achieved— in some scenarios, oscillations of probabilities occur, indicating continuous adaptation and shifting priorities of both sides. The proposed approach can be applied to support decision-making processes in selecting and optimizing cybersecurity strategies.

Вступ

Із розвитком інформаційних технологій кібератаки набувають усе більшого масштабу та складності. Це підвищує значущість кіберзахисту й актуалізує потребу в надійних механізмах захисту даних. Найкращою практикою щодо вирішення цього питання є впровадження системи управління інформаційною безпекою (СУІБ), що визначається стандартом ISO/IEC 27001:2022 [1]. Проте стандарт лише висуває вимоги до побудови СУІБ, у той час як задача обрати конкретну стратегію захисту інформації полягає на головного спеціаліста з інформаційної безпеки (Chief Information Security Officer, CISO). При цьому стратегія СУІБ має не лише відповідати стандартам, а і бути оптимальною серед усіх можливих. Зважаючи на це, метою даної роботи є запропонувати підхід, який CISO може використовувати в питанні вибору стратегії захисту інформації.

Хоча дотримання стандарту [1] і передбачає застосування ризик-орієнтовного підходу, він має певні недоліки, головний з яких – недостатня гнучкість. Робота [2] порівнює наведений підхід із іншим – теоретико-ігровим. Аналіз роботи [2] показує, що теоретико-ігровий підхід надає кількісну оцінку ефективності стратегій захисту. Тому, у межах цієї роботи застосовуватимемо теорію ігор для передбачення можливого результату зіткнення CISO та зловмисника при різних сценаріях.

Моделювання адаптації стратегій CISO

Для побудови моделі змагання існують різні типи змагань. Гра з нульовою сумою та класична біматрична гра, описані в роботах [3] та [4] відповідно, є не універсальними та дещо спрощеними, адже перша передбачає протилежні виграші опонентів, а друга хоч і вирішує цю проблему, проте все ще залишається статичною. Тому доцільним варіантом є використання повторювальної гри, яка є ітеративною, що дозволяє CISO змінювати поведінку в залежності від ефективності стратегії на попередньому етапі [5]. Наприклад, після масованої фішингової атаки CISO може провести додаткове навчання персоналу, тоді як зловмисник у наступному раунді змінює тип повідомлень.

Кожен із гравців має власну множину стратегій: для CISO – це сукупність заходів безпеки, для атакувальника – відповідні типи атак. Матриця виграшів використовується для визначення поточних результатів кожної взаємодії, однак, на відміну від статичних ігор, прийняття рішень у наступних іте-

раціях відбувається з урахуванням накопиченого досвіду. Ймовірність вибору кожної стратегії захисту змінюється пропорційно до її відносного успіху в попередньому раунді, що формально описується рівнянням:

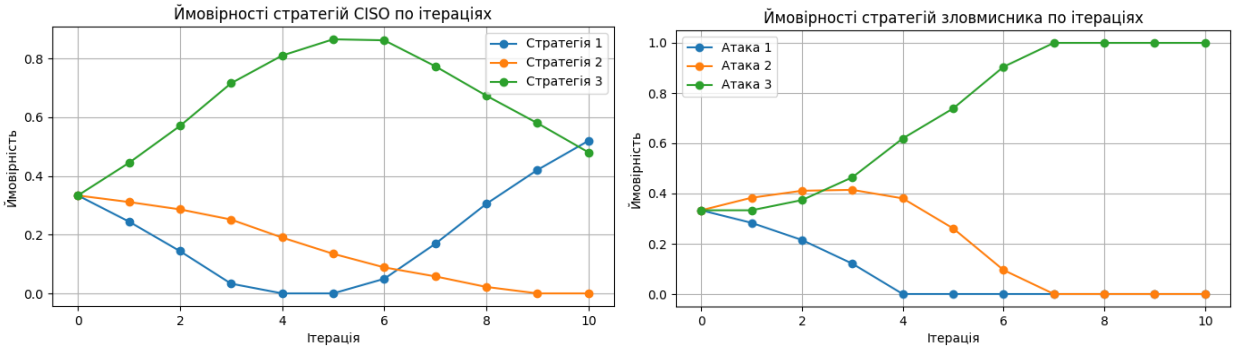
$$P_d^{(t+1)} = \frac{P_d^{(t)} \cdot (1 - \alpha L_d^{(t)})}{\sum_i P_{d,i}^{(t)} \cdot (1 - \alpha L_{d,i}^{(t)})}, \quad (1)$$

де $P_d^{(t)}$ – вектор ймовірностей стратегій на ітерації t;
$L_d^{(t)}$ – втрати на поточному кроці;
α – швидкість реакції на зміни у середовищі.

Ймовірності початкового вибору стратегій формуються із матриці виграшів, тоді як коефіцієнт адаптації α визначається емпірично. Таким чином стратегії, які забезпечують вищий за середній результат, мають тенденцію посилюватися, тоді як менш ефективні – поступово знижують свою ймовірність.

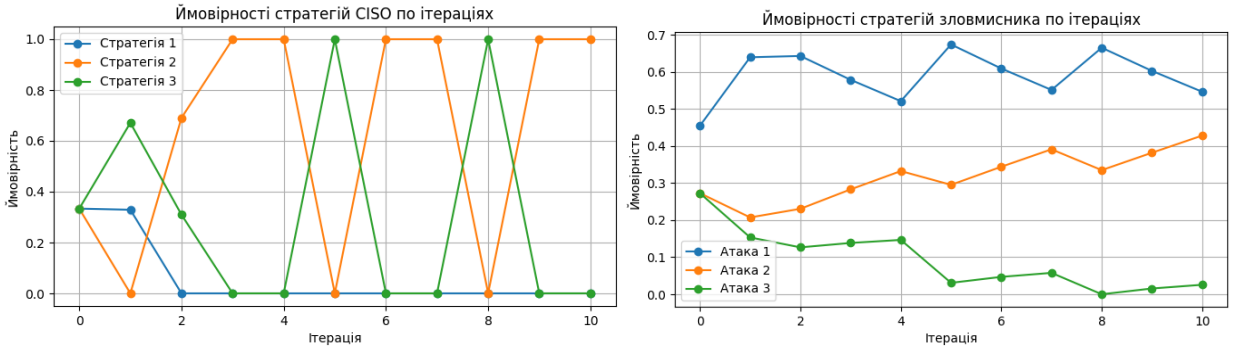
Для демонстрації практичного застосування запропонованої моделі реалізуємо її на прикладі умовної компанії. Передбачається, що CISO розробив 3 варіанти стратегій СУІБ та має на меті проаналізувати їхню ефективність. Зловмисник, у свою чергу, має 3 можливі варіанти атак. Алгоритм обчислення втрат наведений в роботі [4]. Для демонстрації результатів розглянуто два сценарії: стабільний та нестабільний.

Повторювальна гра показує, як оптимальність стратегії змінюється під впливом накопиченого досвіду. У процесі багатоетапної взаємодії CISO коригує свої ймовірності вибору стратегій у залежності від ефективності рішень на попередньому кроці. На рис. 1 наведено графіки динаміки ймовірностей: система наближається до стану рівноваги в разі стабілізації показників. У разі відсутності сталого стану гри або зміні поведінці, спостерігаємо коливання, наведені на рис. 2.



а) **б)**

Рис. 1. Розв'язання повторювальної гри між зловмисником та CISO
а) оцінювання стратегій CISO; б) оцінювання стратегій зловмисника



а) **б)**

Рис. 2. Розв'язання повторювальної гри між зловмисником та CISO за відсутності стабільного стану гри
а) оцінювання стратегій CISO; б) оцінювання стратегій зловмисника

Для визначення, який зі стратегій слід надати перевагу, варто спиратись на очікувані втрати. Якщо одна стратегія має значно більшу ймовірність P і при цьому низькі втрати – це є доказом її переваги. В іншому випадку, для аналізу результатів гри обчислюється очікуване значення втрат:

$$\mathrm{E}[\mathrm{L_d(t)}] = \sum_{\mathrm{a}} \mathrm{q_a(t)} \cdot \mathrm{L_{a,d}} \ , \tag{2}$$

де $\mathrm{q_a(t)}$ – ймовірність застосування атаки ана ітерації t;
$\mathrm{L_{a,d}}$ – втрати захисника у випадку реалізації атаки аза умови вибору стратегії d.

Для прийняття рішення CISO може або спиратись на мінімальне значення очікуваних втрат, або на середнє значення за весь період гри:

$$\overline{\mathrm{E}[\mathrm{L_d}]} = \frac{1}{T}\sum_{t} \mathrm{E}[\mathrm{L_d(t)}] \, . \tag{3}$$

Стратегію із мінімальним значенням $\overline{\mathrm{E}[\mathrm{L_d}]}$ можна вважати кращою.

Висновки

Отримані результати показують, що повторювальна гра між зловмисником та CISO, на відміну від статичних, дозволяє врахувати зміну ймовірностей стратегій у часі. Запропонований підхід має перевагу у вигляді динамічності. Враховуючи накопичений досвід, модель стає наближеною до реальних сценаріїв, а отже – має достатньо високий рівень ефективності. Проте до недоліків підходу можна віднести складність моделювання, викликану великою кількістю необхідних параметрів, та потребу у значних обчислювальних ресурсах, особливо при великій кількості ітерацій або стратегій.

Практичні результати моделювання показали, що не завжди вдається досягти стану рівноваги: у деяких сценаріях ймовірності стратегій змінюються циклічно – це демонструє високу конкурентну спроможність стратегій опонентів. Оптимальність стратегії CISO визначається очікуваними втратами.

Література

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 28.10.2025).

2. Ібрагімова Д. Ф., Добринін І. С. SNW-аналіз підходів до побудови систем управління інформаційною безпекою. *Радіоелектроніка та молодь у XXI столітті. Т. 4 : Конференція "Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій* : матеріали 29-го Міжнар. молодіж. форуму, м. Харків, 16 – 19 квіт. 2025 р. 2025. С. 67 – 69.

3. Добринін І. С., Борова М. П. Оптимізація вибору варіанту побудови системи захисту інформації від атак при антагоністичній грі. *Системи озброєння і військова техніка*. 2018. Т. 2, № 54. С. 89 – 93.

4. 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.

5. Теорія ігор: курс лекцій / ред. В. Д. Романенко. Київ : КПІ ім. Ігоря Сікорського, 2022. 254 с.