ВИЗНАЧЕННЯ СТРАТЕГІЇ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ БЕЗКОАЛІЦІЙНОЇ ГРИ ДВОХ ГРАВЦІВ ІЗ НЕНУЛЬОВОЮ СУМОЮ

Фукс М.А., Добринін І.С.

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

Україна.

E-mail: maksymillian.fuks@nure.ua
ihor.dobrynin@nure.ua

Abstract

The work was dedicated to the development of a new approach describing the way to choose optimal strategies by a chief information security officer based on the mathematical tools of the game theory using economic components, namely the financial and economic evaluation of investments with the account of quantitative risk analysis from the perspective of both participators of a modeled game. Yet before that, the work also reveals the analysis of certain approaches to develop ISMS, taking into account the problem of the determination the best one to apply, which is considered as a multi-criteria optimization problem.

Вступ

Кібербезпека грає помітну роль у сучасному світі, адже стала ключовим фактором у визначенні успішності чи невдачі всієї компанії. Питання функціонування систем управління інформаційною безпекою (СУІБ) з кожним днем все більше порушується в компаніях, які дійсно дбають про власну репутацію. Наразі існує певна низка стандартів і методик, на основі яких можна розробити та впровадити СУІБ, проте в багатьох із них акцентується увага лише на необхідності розгортання та впровадження певних засобів захисту інформації, але не надаються рекомендації щодо процесу детермінування оптимальних стратегій для впровадження. З іншого боку, до уваги необхідно брати також обмежені фінансові ресурси та принцип розумної достатності при побудові ефективної та дієвої СУІБ.

Метою дослідження є розробка математичної моделі біматричної гри між зловмисником та адміністратором безпеки (Chief Information Security Officer, CISO) з урахуванням економічних показників для визначення оптимальної стратегії захисту інформації від можливих атак при обмеженому бюджеті компанії.

Актуальність дослідження полягає в розробці підходу для вибору оптимальної стратегії створення СУІБ на основі математичного апарату теорії ігор із використанням фінансово-економічної оцінки інвестицій із урахуванням показників кількісного аналізу ризиків.

Основна частина

Прийняття СУІБ є стратегічним рішенням організації на проектування та впровадження якої впливають як потреби, так і цілі, розмір, структура, вимоги для безпеки та наявні організаційні процеси у цій організації. Побудова СУІБ ґрунтується на ризик-орієнтованому підході та спрямована на створення, реалізацію, експлуатацію, моніторинг, аналіз, підтримку та підвищення ефективності інформаційної безпеки (ІБ). У межах СУІБ розглядають структуру системи, політики, дії щодо планування, обов’язки, практики, процедури, процеси та ресурси організації [1].

Існує низка підходів спираючись на які компанія може розробити та впровадити СУІБ. Такими є підходи, зазначені в стандартах International Organization for Standardization (ISO) та Federal Information Processing Standard (FISP), публікаціях The National Institute of Standards and Technology (NIST), серії стандартів 8500.x міністерства оборони США, Security Technical Implementation Guide (STIG), документах The European Union Agency for Cybersecurity (ENISA), нормативно-правових актах Національного банку України, тощо.

Аналіз зазначених підходів показав, що в них робиться акцент на безумовне забезпечення фінансування процесу створення, впровадження та функціонування СУІБ. Так, наприклад, стандарт ISO/IEC 27001 містить розділ 7, у якому згадується забезпечення СУІБ, а саме пункт 7.1, про ресурси: «Організація повинна визначити та забезпечити ресурси, які необхідні для розробки, впровадження і підтримку функціонування та безперервного покращення системи управління інформаційною безпекою» [2]. Схожі вимоги висуває і Постанова №95 Національного банку України [3].

Отже, будь-яка методика передбачає окреслення інвестиційних ресурсів для забезпечення необхідного рівня безпеки організації. Проте ні в одній документації не згадується як саме детермінувати необхідний об'єм фінансування для організації, звернувши увагу на розумну достатність у побудові системи захисту інформації. Відповідно до принципу розумної достатності стійкість системи може вважатися достатньою, якщо час на проникнення значно більший за час старіння інформації або ж витрати на проникнення до системи значно перевищує вигоду для зловмисника. Будь-яка організація при обмеженому бюджеті має великий ряд інвестиційних можливостей у ринковій економіці, отож і виникає необхідність оптимізації інвестиційного портфеля. При тому постає питання вибору певної найбільш доречної методики на основі якої будувати СУІБ, тобто виникає багатокритеріальна задача оптимізації.

Проблемі визначення ефективності проведених інвестицій у кібербезпеку загалом присвячено доволі багато літератури, публікацій та певних методів. Отримання в результаті математичного моделювання методом теоретико-ігрового підходу ймовірнісної поведінки гравців щодо впровадження ними певних стратегій допомагає спрогнозувати можливі кроки гравців та отримати прогнозований результат гри.

Так у [4] запропоновано впровадження математичного апарату теорії ігор для оптимізації вибору способу побудови системи захисту інформації (СЗІ) від атак використовуючи антагоністичну модель гри з нульовою сумою. У більшості роботах береться до уваги сторона, що захищається, для якої і будується відповідна матриця з функціями виграшів. Зловмисник, у свою чергу, залишається осторонь, адже вводиться припущення, що виграш адміністратора дорівнює програшу зловмисника, що й характеризує антагоністичну гру.

Традиційний фінансово-економічний індекс описує неповну характеристику інвестицій в інформаційну безпеку, тому що відкидаються інтереси зловмисника, що є грубим спрощенням гри, що моделюється. У результаті зазначених недоліків бажано застосовувати методику, яка надаватиме можливість знаходження оптимальних стратегій захисту інформації для інвестування на основі моделі з явною присутністю економічного показника не тільки для адміністратора безпеки, а й для зловмисника, що призведе до збільшення обсягу гри та інформації в ній шляхом переходу від антагоністичної версії гри до біматричної, де інтереси обох гравців представляються окремими матрицями, відходячи від припущення про нульову суму виграшів обох гравців.

Раціональність учасників лежить в основі таких ігор, адже прагнення до максимізації власного виграшу для кожного суб'єкту веде до значних обмежень кількості можливих варіантів прийняття рішення. Використання теоретико-ігрового підходу для моделювання процесу боротьби за реалізацію власних інтересів між Chief Information Security Officer (CISO) та зловмисником є резонним, адже вони обидва є раціональними, розумними і некооперативними, та мають на меті максимізацію власних функцій виграшу шляхом застосування певних стратегії.

Нехай I={2} – кількість гравців, в якості стратегій яких зображується набір $S_1 = \{a_1,a_2,\ldots,a_n, a_1+a_2,\ldots, a_{n-1}+a_n\}$ та $S_2 = \{b_1,b_2,\ldots,b_m\}$, де n і m кількості таких поодиночних стратегій. Таким чином усі можливі стратегії адміністратора безпеки разом з утвореними комбінаціями створюватимуть певну кількість r – рядків матриці та представлятимуть собою різноманітні засоби захисту інформації (ЗЗІ) і створені комбінації з них для одночасного впровадження, а кількість стратегій зловмисника m – його можливі атаки. Платіжні матриці гравців представлені на рис. 1.

	b_1	b_2	b_3	…	b_m
a_1	$U_A(a_1,b_1)$	$U_A(a_1,b_2)$	$U_A(a_1,b_3)$	…	$U_A(a_1,b_m)$
a_2	$U_A(a_2,b_1)$	$U_A(a_2,b_2)$	$U_A(a_2,b_3)$	…	$U_A(a_2,b_m)$
a_3	$U_A(a_3,b_1)$	$U_A(a_3,b_2)$	$U_A(a_3,b_3)$	…	$U_A(a_3,b_m)$
…	…	…	…	…	…
a_n	$U_A(a_n,b_1)$	$U_A(a_n,b_2)$	$U_A(a_n,b_3)$	…	$U_A(a_n,b_m)$
a_1+a_2	$U_A(a_1+a_2,b_1)$	$U_A(a_1+a_2,b_2)$	$U_A(a_1+a_2,b_3)$	…	$U_A(a_1+a_2,b_m)$
…	…	…	…	…	…
$a_{n-1}+a_n$	$U_A(a_{n-1}+a_n,b_1)$	$U_A(a_{n-1}+a_n,b_2)$	$U_A(a_{n-1}+a_n,b_3)$	…	$U_A(a_{n-1}+a_n, b_m)$

	b_1	b_2	b_3	…	b_m
a_1	$U_B(a_1,b_1)$	$U_B(a_1,b_2)$	$U_B(a_1,b_3)$	…	$U_B(a_1,b_m)$
a_2	$U_B(a_2,b_1)$	$U_B(a_2,b_2)$	$U_B(a_2,b_3)$	…	$U_B(a_2,b_m)$
a_3	$U_B(a_3,b_1)$	$U_B(a_3,b_2)$	$U_B(a_3,b_3)$	…	$U_B(a_3,b_m)$
…	…	…	…	…	…
a_n	$U_B(a_n,b_1)$	$U_B(a_n,b_2)$	$U_B(a_n,b_3)$	…	$U_B(a_n,b_m)$
a_1+a_2	$U_B(a_1+a_2,b_1)$	$U_B(a_1+a_2,b_2)$	$U_B(a_1+a_2,b_3)$	…	$U_B(a_1+a_2,b_m)$
…	…	…	…	…	…
$a_{n-1}+a_n$	$U_B(a_{n-1}+a_n,b_1)$	$U_B(a_{n-1}+a_n,b_2)$	$U_B(a_{n-1}+a_n,b_3)$	…	$U_B(a_{n-1}+a_n, b_m)$

Рис. 1. Платіжна матриця CISO та зловмисника відповідно

Функції виграшів адміністратора безпеки та зловмисника визначатимуться $U_A(S)$ та $U_B(S)$ відповідно при певній ситуації S. Для зображення інтересів обох сторін конфлікту необхідно використати кількісну характеристику функцій виграшу, які доцільно будувати на основі фінансово-економічних оцінок. Концепція розрахунку рентабельності інвестицій застосовується до будь-яких інвестицій. Процес забезпечення безпеки інформації не є винятком. Інвестуючи, робиться прогноз на зменшенні ризиків, які загрожують важливим активам, отож відбувається аналіз рентабельності інвестицій у безпеку на основі розрахунку кількості збитків, які вдалося уникнути завдяки цим інвестиціям. Показник повернення інвестицій у кібербезпеку, тобто функцію виграшу адміністратора безпеки пропонується розглядати у такому вигляді:

$$ROSI = \frac{AV \bullet EF_j \bullet ARO_j \bullet RM_{ij} - cost_i}{cost_i}, \quad (1)$$

де AV – Asset Value;

EF_j – Exposure Factor, тобто втрачена частина активу при появі j-ї атаки;

ARO_j – Annualized Rate of Occurrence при j-ї атаці;

RM_{ij} – Risk Mitigated, тобто ефективність відбиття j-ї атаки при впровадженні i-ї стратегії захисту чи їх комбінацій;

$cost_i$ – загальні витрати на підтримку та впровадження певної i-ї стратегії захисту інформації чи їх комбінації.

Отже, розрахунок показника ROSI (1) для отриманої множини пар складає функцію виграшу адміністратора безпеки, що й задає платіжну матрицю A таблиці наданої на рис. 1. Таким чином елементи матриці представляють кількісну характеристику вигоди впровадження певної стратегії захисту інформації проти можливих атак зловмисника, тобто:

$$U_A(i,j) = ROSI(i,j). \quad (2)$$

Для отримання ефективних результатів математичного моделювання між функціями виграшів обох гравців необхідно зберігати кореляцію. Саме тому необхідно індекс рентабельності (1) поєднати разом із відповідним показником з боку зловмисника, що зображуватиме виграш, який зловмисник очікує від успішної атаки понад втратами внаслідок впровадження механізмів захисту інформації. Показник повернення інвестицій в атаку, тобто функцію виграшу з боку зловмисника, пропонується будувати за формулою:

$$ROA = \frac{GAIN \bullet \left(1 - RM_{ij}\right) - cost_j - loss_{ij}}{cost_j + loss_{ij}}, \quad (3)$$

де GAIN – оцінка очікуваного прибутку;

RM_{ij} – Risk Mitigated, тобто ефективність відбиття j-ї атаки при впровадженні i-ї стратегії чи їх комбінацій;

$cost_j$ – витрати зловмисника на підготовку атаки;

$loss_{ij}$ – додаткові витрати зловмисника при проведенні j-ї атаки через впровадження i-ї стратегії чи їх комбінацій.

Отже, розрахунок показника ROA (3) для отриманої множини пар складає функцію виграшу зловмисника, що й задає платіжну матрицю B таблиці наданої на рис. 1. Кількісна репрезентація елементів матриці показує виграші зловмисника від проведення певної атаки при впроваджених контрзаходах адміністратора, і зображується як:

$$U_B(i,j) = ROA\ (i,j). \tag{4}$$

Наступним етапом є розв'язання створеної гри двох осіб на основі даних з формул (2) та (4), що задається наступним виразом:

$$\Gamma = \langle S_1, S_2, ROSI(i,j),\ ROA\ (i,j)\rangle. \tag{5}$$

Після побудови платіжних матриць обох гравців для проведення моделювання та отримання результату можна використати алгоритм Лемке-Хаусона [5]. Таким чином відбуватиметься визначення оптимальної стратегії захисту інформації адміністратором безпеки базуючись на отриманому векторі власної змішаної стратегії. У результаті отримуємо ситуацію рівноваги для біматричної гри, а саме: пару змішаних стратегій. Інтерпретація отриманих результатів полягає в тому, що певний гравець повинен дотримуватися конкретної, отриманої, стратегії, оскільки вона перевершує виграші від інших стратегій.

Висновки

У даному дослідженні було запропоновано методику визначення оптимальної стратегії захисту інформації на основі математичної моделі біматричної гри між зловмисником та адміністратором безпеки з урахуванням економічних показників для допомоги визначення оптимальної стратегії захисту інформації від можливих атак при обмеженому бюджеті компанії. Провівши аналіз найпоширеніших методик, на основі яких підприємство може побудувати СУІБ було окреслено спільну проблему розглянутих методик, а саме: відсутність рекомендацій щодо оптимізації вибору стратегій захисту і обрання доцільних методів та засобів захисту керуючись принципом розумної достатності та обмежений рівень фінансування.

Вирішення цієї проблеми лежить у можливості використання математичного апарату теорії ігор, зокрема біматричної гри, у якій інтереси обох гравців представляються окремими матрицями для проведення більш точного моделювання і відмови від припущення про нульову суму виграшів. Після побудови матриць було знайдено рішення, яке надало можливість адміністратору безпеки ясно оцінити ситуацію, а саме вибрати найкращий засіб захисту.

У порівнянні з роботою [4], де показник повернення інвестицій будується на основі ймовірностей для побудови лише матриці адміністратора, запропонована в цій роботі методика не суперечить, а тільки доповнює наявні та пропонує спиратися саме на показники кількісної оцінки ризиків у створенні функцій виграшів обох суперників і проводити моделювання в розрізі біматричної гри.

Запропонована методика визначення стратегії захисту інформації на основі теоретико-ігрового підходу буде корисною як відповідальній особі за інформаційну безпеку підприємства, так і керівникам, адже пропонується застосування математичного апарату задля детермінування найкращого та ефективного вибору механізмів та засобів забезпечення безпеки в певній ситуації з урахуванням обмеженого бюджету організації, дотримуючись принципу розумної достатності.

Література

1. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с. : іл.

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: 07.11.2023).

3. Правління Національного банку України. Постанова 28.09.2017 № 95 Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text (дата звернення: 07.11.2023).

4. Добринін І. С. Оптимізація вибору варіанту побудови системи захисту інформації від атак при антагоністичній грі / І. С. Добринін, М. П. Борова. // Системи озброєння і військова техніка. – 2018. – С. 89–93.

5. Lemke C. E., Howson, Jr. J. T. Equilibrium Points of Bimatrix Games. Journal of the Society for Industrial and Applied Mathematics. 1964. Т. 12, № 2. С. 413–423. URL: https://doi.org/10.1137/0112033 (дата звернення: 08.11.2023).