УДК 005.7:519.83]:004.056

СТРАТЕГІЯ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МАТЕМАТИЧНОГО АПАРАТУ ТЕОРІЇ ІГОР

Фукс М. А.
Науковий керівник – к.т.н., доцент Добринін І.С.
Харківський національний університет радіоелектроніки,
каф. інфокомунікаційної інженерії імені В.В. Поповського,
м. Харків, Україна
тел. +38(066) 163-90-04

The aim of the work is to analyze the possibilities of the implementation of the mathematical model of a bimatrix game between the security administrator and attacker for determining an optimal security information strategy against possible attacks with a limited budget for the company. Different methodologies for implementing ISMS reflect the need to deploy and implement information security measures but do not present recommendations on how to conduct the selection. Therefore, CISO has to rely on its experience only. To assist him in defining the best strategy, the implementation of a bimatrix game was considered.

Інформаційна безпека займає помітне місце у інвестиціях компаній, адже все більше учасників бізнесу розуміють, що завдяки досягненню певного рівня безпеки та впровадження необхідних методів захисту від атак можна запобігти втратам. Насправді, інвестиції у механізмі захисту неспроможні принести прямий приріст прибутку, бо забезпечується скоріш мінімізація втрат від можливих атак. Отже, запобігання можливих втрат може розглядатися як економія різноманітних ресурсів усієї бізнес-системи.

Проблемі визначення ефективності проведених інвестицій у кібербезпеку присвячено доволі багато літератури, публікацій та певних методів, наприклад, метод аналізу ієрархій Томаса Сааті, теорія корисності або використання математичного апарату теорії ігор. У роботі [1] досліджується можливість застосування нечіткого багатокритеріального методу на основі парних порівнянь альтернатив для проведення аналізу при виборі кращого варіанту СЗІ. Також згадується принцип Беллмана-Заде, який стверджує, що найкращою може вважатися та альтернатива, яка найбільш серед інших відповідає усім створеним критеріям, а також не допускається нестача одних показників надлишком інших. Робота [2] зосереджується на пропонуванні теоретико-ігрового методу, що оптимально розподіляє ресурси направлені на кібербезпеку. Пропонується біматрична гра, що представляє імітацію середовища кібербезпеки, де доказується, що стратегія Неша для захисника є мінімаксною. Також пропонується застосування методу сингулярного розкладання SVD для знаходження приблизного значення точки рівноваги.

Існує велика кількість підходів, на основі яких компанія може розгорнути власну СМІБ, наприклад, стандарти International Organization for

Standardization (ISO) та Federal Information Processing Standard (FISP), публікації The National Institute of Standards and Technology (NIST), серія стандартів 8500.x, Security Technical Implementation Guide (STIG), документи The European Union Agency for Cybersecurity (ENISA), нормативно-правові акти, методологія IT-Grundschutz, тощо. Процес визначення прийнятного ризику та вибір оптимальних стратегій для використання CISO – нелегка задача, адже навіть у вищезазначених методологіях відображена лише необхідність розгортання та впровадження засобів захисту інформації, але не представлені рекомендації щодо того, як саме провести оптимізацію вибору. Зазвичай наявне також обмежене фінансування, а тому необхідно поєднувати виділені фінансові можливості, потрібні методи захисту і принцип розумної достатності для отримання у результаті ефективної та якісної СМІБ.

Вирішення висвітленої проблеми лежить у представленні взаємовідносин між учасниками, які мають різні чи навіть протилежні мотиви, за допомогою математичного апарату теорії ігор. Використання теоретико-ігрового підходу для моделювання процесу боротьби за реалізацію власних інтересів між 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. Тактика кожного з гравців детермінується ходами іншого.

Наявні різноманітні типи ігор, які розкривають моделювання по-різному. Найчастіше для моделювання використовують антагоністичну гру, де некооперативні гравці мають повністю протилежні виграші. Але у цьому випадку, насправді, робиться припущення, що втрати організації дорівнюють виграшу зловмисника, що і є грубим спрощенням усієї гри. Для уникнення подальших проблем та некоректних результатів наявна можливість застосування дещо іншого типу ігор, а саме біматричних ігор.

Використання біматричних ігор у моделюванні взаємодії CISO та зловмисника не суперечить наявним публікаціям та методологіям і може використовуватися як альтернатива, що використовує більше вхідних даних, адже вона розглядає як інтереси CISO, так і зловмисника, а тим самим спроможна представити більш точний результат.

Список використаних джерел:

1. Шматко О. В. Багатокритеріальний вибір систем захисту інформації за допомогою нечітких парних порівнянь альтернатив / О. В. Шматко, Є. В. Сичев. // ХПІ. – 2011. – С. 161–164.

2. Andrew Fielder. Game Theory Meets Information Security Management / Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria. // IFIP International Federation for Information Processing. – 2014. – С. 15.