УДК 004.056:004.94

ЗАСТОСУВАННЯ ІГРОВОЇ МОДЕЛІ ДЛЯ ДОСЛІДЖЕННЯ ОПТИМАЛЬНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Румянцева О.В
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В.
Харківський національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
тел+38(099) 029-93-20

The report reviews the application of a game model to investigate the optimality of information security systems. The report also highlights the importance of considering multiple stakeholders and their competing interests when designing a secure system. It outlines the steps involved in developing a game model, including identifying players, defining strategies. The report described how simulation and optimization techniques can be used to evaluate different scenarios and identify the optimal solution. Ultimately, the report concludes that game models can provide a useful tool for designing secure systems and highlights its potential to improve decision-making in the field of information security.

У доповіді розглядаються особливості застосування ігрової моделі як інструменту моделювання при оптимізації систем захисту інформації.

Ігрова модель – це математичний інструмент, що використовується для аналізу стратегічних ситуацій, у яких приймають рішення кілька учасників (гравців), кожен із яких прагне максимізувати свою вигоду. Ігрова модель складається з гравців, правил гри та набору стратегій, які кожен гравець може вибрати. Гравці можуть приймати рішення одночасно чи послідовно, залежно від типу гри. Кожен гравець намагається вибрати найбільш вигідну стратегію з огляду на стратегії інших гравців [1].

У контексті захисту інформації гравцями можуть виступати зловмисники, які намагаються отримати несанкціонований доступ до захищеної інформації, та захисники, які намагаються запобігти таким атакам та захистити інформацію. Ігрова модель може бути використана для визначення оптимального балансу між захистом інформації та її доступністю для легітимних користувачів. Під час створення ігрової моделі необхідно враховувати різні фактори, такі як можливості нападаючого, вартість захисту та ризики порушення безпеки. На основі цієї моделі можна проводити симуляції, в яких гравці приймають рішення та взаємодіють один з одним, щоб визначити оптимальний проект системи захисту інформації [2].

Одним із прикладів ігрової моделі, яка може бути використана для дослідження оптимальності проекту системи захисту інформації, є модель «Stackelberg», яка включає двох гравців – лідера та послідовника. Лідер є

захисником, який приймає рішення про ступінь захисту інформації, а послідовник – нападника, який намагається проникнути в систему.

У цій моделі лідер ухвалює рішення першим, а послідовник реагує на це рішення. Лідер може вибирати різні рівні захисту, а послідовник може вибирати різні способи атаки. Мета кожного гравця – максимізувати свою вигоду. Результати симуляції можуть показати оптимальний рівень захисту інформації та оптимальні стратегії захисту від атак. Таким чином, ігрова модель може бути корисним інструментом для дослідження оптимальності проекту системи захисту інформації, дозволяючи враховувати різні фактори та знаходити баланс між захистом та доступністю інформації. Ігрова модель дозволяє оцінити ефективність різних стратегій захисту інформації та вибрати найкращу. Також вона може використовуватись для аналізу впливу зміни параметрів системи захисту інформації на її ефективність. В ігровій моделі можуть бути використані різні критерії оцінки, наприклад, час проникнення зловмисника, рівень шкоди, можливість виявлення та запобігання атаки тощо. Оцінка проводиться з урахуванням усіх можливих сценаріїв дій як зловмисників, так і адміністраторів системи захисту інформації.

У результаті аналізу ігрової моделі можна виявити вразливості системи та вжити заходів щодо їх усунення. Також можна визначити оптимальне співвідношення між витратами на захист та можливим збитком від атаки, що дозволить вибрати найбільш оптимальний варіант захисту інформації. Також використання ігрової моделі для аналізу оптимальності проекту системи захисту інформації дозволяє ухвалити обгрунтовані рішення, які зменшать ймовірність витоку інформації та захистять систему від можливих атак. Крім того, використання ігрової моделі дозволяє розглянути різні сценарії атаки та оцінити ступінь їхнього впливу на систему захисту інформації. Це може допомогти виявити слабкі місця в системі та покращити її захист. В цілому, використання ігрової моделі для дослідження оптимальності проекту системи захисту інформації є потужним інструментом, який може допомогти розробникам проекту прийняти більш обгрунтовані рішення та створити більш ефективну систему захисту інформації.

Список використаних джерел:

1. Петров, В. Г. (2019). Використання ігрових технологій для дослідження вразливості інформаційних систем. Проблеми захисту інформації, (2), 47-54.

2. Баранова, Н.І. (2011). Методи і засоби захисту інформації в комп'ютерних системах. Київ: ВПЦ «Київський університет». (с. 272)