МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. Ф.М. ДОСТОЕВСКОГО

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

Сборник материалов
VII Международной научной конференции,
посвященной памяти С.С. Ефимова

(Омск, 22 ноября 2019 г.)

ISBN 978-5-7779-2458-2

Омск

ИЗДАТЕЛЬСТВО
ОМСКОГО ГОСУДАРСТВЕННОГО
УНИВЕРСИТЕТА

2020

УДК 519.83:004.056

Т.В. Вахний, А.К. Гуц, В.С. Заполин

Омский государственный университет им. Ф.М. Достоевского,
г. Омск, Россия

ПРИМЕНЕНИЕ БИМАТРИЧНЫХ И ИЕРАРХИЧЕСКИХ ИГР ДЛЯ ОПТИМИЗАЦИИ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ

При построении и анализе современных систем защиты информации активно используется математический аппарат теории игр [1–3]. С помощью игровых методов можно анализировать взаимодействие между администратором безопасности и злоумышленниками, имеющими разные интересы. В данной работе путем решения иерархических и биматричных игр рассчитывались наиболее оптимальные наборы программных средств защиты компьютерной системы. В биматричных играх предполагается, что игроки (администратор безопасности и злоумышленник) выбирают свои стратегии одновременно и однократно, а в иерархических играх существует фиксированный порядок ходов – первый ход делает ведущий игрок, а затем свои стратегии выбирает ведомый игрок. Иерархическая игра представляет собой математическую игру, в которой игроку верхнего уровня иерархии известна стратегия второго игрока при существовании неопределенных факторов [4–6]. Итогом такой игры является максимально гарантированный результат игрока верхнего уровня.

Было реализовано два типа иерархических игр – в одной ведущим игроком был администратор безопасности, а во второй – злоумышленник.

В первом случае предполагается, что более опытным игроком является администратор безопасности, он имеет представление как о возможных атаках, которые могут нанести ущерб компьютерной системе, так и о способах им противостоять, а также может предсказать реакцию злоумышленника. Поэтому именно он делает первый ход и ему принадлежит ведущая роль в иерархической игре. Затем свои стратегии выбирает злоумышленник,

который в этой иерархической игре является ведомым игроком. Стратегиями первого игрока являются различные комбинации программных средств для защиты, а стратегиями второго игрока – различные комбинации угроз компьютерной безопасности. Оптимальной стратегией администратора в работе считается такой набор программных продуктов, который обеспечивает сведение к суммарному минимуму ущерба, нанесённого компьютерной системе, и затрат на приобретение программных продуктов. Исследование проводилось в интересах администратора безопасности, поэтому предполагалось, что возможные угрозы злоумышленника направлены на нанесение наибольшего ущерба компьютерной системе и каждый игрок стремится, по возможности, максимизировать свою функцию выигрыша.

Во второй иерархической игре предполагалось, что более опытным игроком является злоумышленник, который прекрасно осведомлен о всех способах защиты информационного ресурса, на который организует атаку, поэтому теперь он выступает ведущим игроком. Администратор в этой иерархической игре уступает хакеру не только в инициативе, но и в знаниях уязвимостей защищаемой им системы.

На основе описанного подхода было создано программное приложение, которое находит решение биматричных и иерархических с выбором ведущего игрока игр, вычисляя несколько наиболее оптимальных наборов средств защиты из имеющихся в распоряжении администратора безопасности программных продуктов. Анализ результатов расчетов иерархических и биматричных игр может быть полезен администратору безопасности в принятии более верных решений в вопросах оптимизации защиты компьютерной системы.

Литература

1. *Гуц А.К., Вахний Т.В.* Теория игр и защита компьютерных систем: учебное пособие. Омск : Изд-во ОмГУ, 2013. 160 с.
2. *Вахний Т.В., Гуц А.К., Новиков Н.Ю.* Матрично-игровая программа с выбором критерия для определения оптимального набора средств защиты компьютерной системы // Математические структуры и моделирование. 2016. № 2 (38). С. 103–115.

3. *Вахний Т.В., Гуц А.К., Бондарь С.С.* Учет вероятностей хакерских атак в игровом подходе к подбору программных средств защиты компьютерной информации // Математические структуры и моделирование. 2015. № 3 (35). С. 91–105.
4. *Вахний Т.В., Гуц А.К.* Иерархические игры и защита компьютерных систем // Омские научные чтения – 2018: материалы Второй Всероссийской научной конференции (Омск, 10–15 декабря 2018 г.). Омск: Изд-во Ом. гос. ун-та, 2018. С.174–175.
5. *Damjanovic-Behrendt V.* Stackelberg Security Game for Optimizing Security of Federated Internet of Things Platform Instances // World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering. 2017. Vol. 11, no. 5. P. 529–534.
6. *Lee P., Clark A., Alomair B., Bushnell L., Poovendran R.* Passivity-Based Distributed Strategies for Stochastic Stackelberg Security Games // Proceedings of 6th International Conference «GameSec 2015», London, UK, November 4–5, 2015. P. 113–129. URL: http://www.ee.washington.edu/research/nsl/papers/Gamesec2015.pdf.