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
VI Международной научной конференции,
посвященной памяти Б.А. Рогозина

(Омск, 23 ноября 2018 г.)

Омск

2018

УДК 519.83:004.056

Т.В. Вахний, А.К. Гуц, Г.В. Хейловский

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

ПРИМЕНЕНИЕ ИГРОВЫХ МЕТОДОВ ДЛЯ ОПТИМИЗАЦИИ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Рост возможностей вычислительной техники и расширение сферы ее применения сопровождается повышением требований к информационной безопасности не только компьютерных систем, но и информации, передающейся по сетевым соединениям. В настоящее время на рынке представлено огромное разнообразие средств защиты, и администратору безопасности приходится принимать субъективные решения о выборе в пользу тех или иных программных продуктов. С ростом уровня защищённости компьютерной системы и сети могут возникать определённые неудобства, ограничения и трудности для пользователей, связанные с тем, что набор программных средств может потребовать огромное количество ресурсов, приводя к нехватке вычислительной мощности. Поэтому часто необходимо выбирать оптимальный вариант защиты, который бы не создавал больших трудностей в пользовании компьютерной системой и одновременно обеспечивал достойный уровень информационной безопасности. Применение самых различных методов математической теории игр позволяет обеспечить как оптимизацию стратегий защиты, так и выбора конкретных программных продуктов для защиты компьютерных систем и сетей [1–6].

В данной работе для поиска оптимального набора программных средств защиты компьютерной системы и сети предлагается провести математическую игру двух игроков, одним из которых является администратор компьютерной системы, а другим – злоумышленник. Стратегиями первого являются различные комбинации программных средств для защиты, а стратегиями

второго – различные комбинации угроз компьютерной безопасности. Поскольку целью данной работы являлось определение оптимальной стратегии защиты (такого набора программных продуктов, который обеспечит сведение к суммарному минимуму ущерба, нанесённого компьютерной системе, затрат на приобретение программных продуктов и задействованных вычислительных ресурсов), то можно считать, что возможные угрозы злоумышленника направлены на нанесение наибольшего ущерба компьютерной системе и сети. С учетом того, что выигрыши администратора и злоумышленника скорее всего выражаются в отличных суммарных цифрах, то вместо матричной игры двух лиц с нулевой суммой, когда выигрыш хакера будет равен проигрышу администратора безопасности, следует использовать биматричную игру. При составлении платежных матриц игроков стратегии администратора можно выбрать, например, как ее строки, стратегии злоумышленника – как столбцы, а на их пересечении проставить цену каждой партии для каждого игрока (сумма ущерба от атаки с затратами на приобретение программных средств и требуемых вычислительных ресурсов для администратора и выигрыши злоумышленника в его матрице).

На основе описанного подхода было создано программное приложение, которое по введённым значениям стоимости средств защиты и величинам вероятностей реализации угроз безопасности вычисляет оптимальный набор средств защиты из имеющихся в распоряжении администратора безопасности программных продуктов. Описанное в данной работе программное приложение проводит диагностику компьютера и выбирает для него оптимальный набор программных средств защиты, который не будет приводить к нехватке вычислительной мощности. К тому же оно дает рекомендации по оптимизации аппаратной части устройства, чтобы вычислительной мощности хватило обеспечить более высокий уровень защищенности.

Литература

1. *Гуц А.К., Вахний Т.В.* Теория игр и защита компьютерных систем: учебное пособие. Омск: Изд-во Ом. гос. ун-та, 2013. 160 с.
2. *Вахний Т.В., Гуц А.К., Бондарь С.С.* Учет вероятностей хакерских атак в игровом подходе к подбору программных средств защиты ком-