Математическое и компьютерное моделирование:
материалы III Международной научной конференции
(Омск, 12 ноября 2015 г.). Омск, 2015. С. 185–186. УДК 519.83+681.3.067

Т.В. Вахний, А.К. Гуц, Н.Ю. Новиков

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

МАТРИЧНО-ИГРОВАЯ ПРОГРАММА С ВЫБОРОМ КРИТЕРИЯ ДЛЯ ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНОГО НАБОРА СРЕДСТВ ЗАЩИТЫ КОМПЬЮТЕРОВ

На рынке представлено огромное разнообразие средств защиты компьютерных систем. Часто необходимо выбрать оптимальный вариант защиты, который бы не создавал больших трудностей в его использовании для защиты компьютерной системы и одновременно обеспечивал бы достойный уровень защиты информации. Подчас нахождение такого оптимального способа обеспечения безопасности является очень сложной задачей; администратору безопасности приходится принимать субъективные решения при выборе того или иного программного продукта. Использование теории матричных игр позволяет обеспечить оптимизацию выбора программных продуктов для защиты компьютерной информации.

На сегодяшний день мы не можем говорить о разнобразии программных средств защиты, основанных на использования теории игр. Нами создан программный продукт, в основу которого положена теория матричных игр и который предназначен в помощь администаторам, отвечающим за безопасность компьютерных систем.

При написании программы осуществлялся следующий подход. Получить различные стратегии игроков – хакера и администратора – можно путем простого перебора всех возможных атак для хакера и аналогичного перебора все участвующих в игре программных средств защиты для администратора. Однако при таком подходе получаем более миллиона стратегий, что естественно сказалось бы на скорости работы программного приложения. Чтобы сократить количество стратегий игроков, возможные способы атаки и средства стратегии были разделены по группам. В таком случае из каждой группы атак выбирается одна с максимальным ущербом, а из каждой группы средств защиты выбирается одно с минимальной стоимостью. Из получившихся списков атак и средств

защиты составляются стратегии игроков путем перебора всех возможных комбинаций. Выбор оптимальной стратегии администратора безопасности осуществляется по одному из четырех критериев оптимальности: критерий крайнего пессимизма Вальда, критерий максимального математического ожидания Байеса, критерий недостаточного основания Лапласа и критерий пессимизма-оптимизма Гурвица.

Суммарные затраты получаются суммированием величины ущерба, который может быть нанесен при реализации текущей стратегии хакера, если система не была защищена от нее средствами защиты из текущей стратегии администратора безопасности, и общей стоимости всех средств защиты из текущей стратегии администратора безопасности. Подсчет ущерба от реализации угроз вычисляется в два этапа. Сначала текущая стратегия хакера сопоставляется с каждым из средств защиты из текущей стратегии администратора безопасности, и если средство защищает от каких-то угроз из текущего набора, то данные угрозы удаляются из набора. Сопоставляя текущий набор угроз со всеми средствами из текущей стратегии администратора безопасности, получаем некоторое количество угроз, от которых система в данном случае не защищена. Полученные угрозы нужно соотнести со всеми имеющимися угрозами и суммировать величины ущерба тех угроз, которые присутствуют в полученном наборе. Далее эти две суммы складываются, и получается ущерб при применении текущей пары стратегий хакера и администратора безопасности.

Так как предполагается, что хакер стремится нанести как можно больший вред компьютерной системе, то необходимо для каждой стратегии администратора безопасности выбрать максимальную величину суммарных затрат среди значений, соответствующих текущей стратегии и всем стратегиям хакера. Таким образом, для каждой стратегии администратора безопасности вычисляется максимально возможные суммарные затраты. Логично теперь из всех полученных максимальных величин ущерба (суммарных затрат) выбрать минимальное значение. Стратегия, соответствующая данному значению, и будет искомой оптимальной стратегией.

В работе был создан программный продукт, который по введенным значениям стоимости средств защиты и ущерба от применения всех возможных пар атака-защита, позволяет рассчитать оптимальный набор средств защиты компьютерной системы по одному из четырех вышеупомянутых критериев.