МИНИСТЕРСТВО ОБАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

Сборник материалов
Международной научной конференции

(Омск, 21 ноября 2014 г.)

Омск

2014

rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения: 19.10.2014).
3. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей: руководящий документ. URL: http://fstec.ru/component/content/article/114-tekhnicheskaya-zashchita-informatsii/dokumenty/spetsialnye-normativnye-dokumenty/382-rukovodyashchij-dokument-prikaz-predsedatelya-gostekhkomissii-rossii-ot-4-iyunya-1999-g-n-114 (дата обращения: 19.10.2014).
4. Hash Function: GOST R 34.11-2012. URL: https://tools.ietf.org/html/rfc6986 (дата обращения: 19.10.2014).

УДК 004.056.5:005.311.7

Т.В. Вахний, А.К. Гуц, С.Ю. Кузьмин
Омский государственный университет им. Ф.М. Достоевского

ТЕОРЕТИКО-ИГРОВОЙ ПОДХОД К ПОДБОРУ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Работа в глобальной сети интернет связана с постоянными угрозами информационной безопасности. Для защиты данных от вредоносных программ и внешних хакерских атак, использующих уязвимости в программном обеспечении, необходимы, прежде всего, антивирусная система и межсетевой экран. Использовать антивирусную систему со встроенным персональным межсетевым экраном не всегда оказывается предпочтительным решением. В таких случаях становится актуальным вопрос подбора антивирусной системы и межсетевого экрана.

Современные антивирусные системы и межсетевые экраны обладают большим количеством разнообразного функционала и инструментария для решения задач защиты данных, при этом у них могут частично совпадать функциональные возможности. Администратору безопасности среди всего разнообразия представленных на рынке программных продуктов приходится принимать субъективные решения, основываясь лишь на изуче-

нии их описания. В данной работе предлагается применить игровой подход к подбору наиболее оптимального набора антивирусной системы и межсетевого экрана.

Для поиска наиболее оптимальных стратегий защиты информационных ресурсов была проведена математическая игра двух игроков, одним из которых являлась система защиты компьютерной информации, а другим – возможные угрозы безопасности информации. Поскольку целью данной работы являлось определение оптимальной стратегии защиты (такого набора программных продуктов, который обеспечит сведение к минимуму ущерба, нанесенного компьютерной системе), то можно считать, что возможные угрозы злоумышленника направлены на нанесение наибольшего ущерба компьютерной системе. При таком предположении выигрыш хакера будет равен проигрышу администратора безопасности, и можно рассматривать матричную игру двух лиц с нулевой суммой.

В качестве стратегий администратора безопасности будем понимать строки x_i ($i = 1,\ldots,n$) (различные средства защиты компьютерной информации) некоторой матрицы (табл. 1), а в качестве стратегий злоумышленника – ее столбцы y_j ($j = 1,\ldots,m$) (возможные угрозы безопасности информации). К стратегиям также можно отнести различные сочетания из угроз и различные сочетания средств защиты. Прекращение использования или добавление новой угрозы или средства защиты можно рассматривать как переход от одной стратегии к другой.

Таблица матричной игры

	y_1	y_2	…	y_m
	$p(y_1)$	$p(y_2)$	…	$p(y_m)$
x_1	a_{11}	a_{12}	…	a_{1m}
…	…	…	…	…
x_n	a_{n1}	a_{n2}	…	a_{nm}

Для проведения на компьютере игры A надо также знать результаты игры при каждой паре стратегий x_i и угроз y_j

(например, a_{ij} – причинённый ущерб) и вероятности реализации $p(y_j)$ каждой угрозы y_j.

В данной работе коэффициенты матрицы a_{ij} определяли, учитывая только те угрозы, которые пропускались, т.е. не отражались соответствующими средствами защиты. Для определения коэффициентов матрицы игры между угрозами и средствами защиты было протестировано прохождение пакета из 15 тысяч угроз через различные антивирусные системы и межсетевые экраны. Вероятность реализации каждой угрозы $p(y_j)$ определялась как отношение количества угроз данного типа к количеству всех угроз в пакете.

Наилучшей в условиях имеющейся информации об угрозах считалась стратегия системы защиты компьютерной информации, т. е. набор средств защиты, для которой будет минимальна сумма

$$\sum_j a_{ij} p(y_j).$$

На основе описанного подхода было создано программное приложение, которое по введённым значениям стоимости средств защиты, проценту проникновения угроз и величинам вероятностей их реализации вычисляет оптимальный набор средств защиты из имеющихся в распоряжении администратора безопасности программных продуктов.

В реализованном приложении предусмотрено нахождение оптимального набора с возможностью ограничения по стоимости программного обеспечения. Компьютерные эксперименты показали, что среди участвующих в матричной игре антивирусных систем и межсетевых экранов наиболее оптимальным набором оказались Eset Nod 32 и Kaspersky Internet Security. Дальнейшее дополнение матрицы игры другими видами угроз и средствами защиты позволит подобрать наиболее оптимальный набор из большего числа программных средств защиты.