Математические структуры и моделирование
2014. № 4(32). С. 240–246

УДК 519.83+681.3.067

ОПТИМАЛЬНЫЙ ПОДБОР АНТИВИРУСНОЙ ПРОГРАММЫ И МЕЖСЕТЕВОГО ЭКРАНА С ПОМОЩЬЮ ТЕОРИИ ИГР

Т.В. Вахний
доцент, к.ф.-м.н., e-mail: vahniytv@mail.ru
А.К. Гуц
профессор, д.ф.-м.н., e-mail: aguts@mail.ru
С.Ю. Кузьмин
студент, e-mail: sergkuz2@gmail.com

Факультет компьютерных наук, Омский государственный университет им. Ф.М. Достоевского

Аннотация. Описывается применение теоретико-игрового подхода к поиску наиболее оптимального набора программных средств защиты компьютерных информационных ресурсов на примере подбора антивирусной системы и межсетевого экрана.

Ключевые слова: оптимальный набор средств защиты, защита информации, теория игр.

Введение

Работа в глобальной сети Интернет связана с постоянными угрозами информационной безопасности. Компьютерные системы предприятий и организаций очень часто становятся объектами, на которые направлены помыслы злоумышленников. Посредством компьютерной атаки можно либо уничтожить систему, либо временно ограничить доступ к ней. В любом случае предприятия несут как финансовые потери, так и моральные, как, например, банки, уровень доверия к которым падает, если они стали жертвами атаки хакеров.

Атаки на информационные ресурсы могут быть самыми разнообразными: от несанкционированного проникновения до заражения системы вирусами. 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 разнообра-

зия представленных на рынке программных продуктов приходится принимать субъективные решения, основываясь лишь на изучении их описания.

В данной работе предлагается применить теоретико-игровой подход к подбору наиболее оптимального набора антивирусной системы и межсетевого экрана. Важно отметить, что теория игр в последние годы интенсивно используется в исследованиях по организации систем защиты компьютерных информационных ресурсов от внешних угроз [1].

1. Постановка задачи и игровой подход

Для поиска наиболее оптимальных стратегий защиты информационных ресурсов была проведена математическая игра двух игроков [1–3], 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, нанесённого 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 — её 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.

Построив игровую матрицу (табл. 1) и проанализировав её, можно заранее оценить процент возможного пропуска угроз и затраты каждого решения по защите компьютерной информации. Проведение матричной игры позволит определить наиболее эффективные варианты для всего диапазона угроз.

Таблица 1. Таблица матричной игры

		y_1	y_2	...	y_m
x_1	$p(x_1)$	a_{11}	a_{12}	...	a_{1m}
x_2	$p(x_2)$	a_{21}	a_{22}	...	a_{2m}
...	...	...	...	...	...
x_n	$p(x_n)$	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

$$\sum_{j=1}^{m} a_{ij} p(y_j).$$

В расчётах для каждой стратегии в качестве коэффициента a_{ij} выбирается наименьший из коэффициентов для соответствующих программных средств защиты информации в отдельности.

2. Матрица игры

Для определения коэффициентов матрицы игры между угрозами и антивирусными системами было протестировано прохождение пакета из 15 тысяч угроз через различные антивирусные системы. В таблице 2 представлены полученные результаты. На пересечении каждой строки и столбца стоит число пропущенных угроз соответствующей антивирусной системой.

Таблица 2. Результаты расчета вероятности угроз

	Вирусы	Spyware	Adware	Maleware	Баннер	Веб-угрозы	Фишинг	Трояны	Черви
Kaspersky Antivirus		3				5	2		3
McAfee Antivirus			3		2			3	
Avast Pro Antivirus	5			2		5			4
Eset Nod 32		5					2		1
Panda Antivirus		2			3			1	

Вероятность реализации каждой угрозы в данной работе определялась как отношение количества угроз данного типа к количеству всех угроз в пакете. В таблице 3 приведены полученные значения для всех возможных угроз в пакете.

Поскольку установить сразу несколько антивирусных систем одновременно нельзя, то лучшей будет та, которая пропустит меньшее число угроз. Такой

антивирусной системой оказалась McAfee Antivirus. Аналогично были определены коэффициенты матрицы игры между угрозами и межсетевыми экранами (см. табл. 4). Наименьшее число угроз среди рассмотренных межсетевых экранов пропустил Kaspersky Internet Security.

После составления общей матрицы игры, в которой стратегиями администратора безопасности были антивирусные системы и межсетевые экраны, и проведения матричной игры, наиболее оптимальным набором оказались антивирусная система Eset Nod 32 и межсетевой экран Kaspersky Internet Security. Дальнейшее дополнение матрицы другими видами угроз и средствами защиты позволит подобрать наиболее оптимальный набор из большего числа программных средств защиты.

Таблица 3. Результаты расчета вероятности угроз

		y_1	y_2
Вирусы	13%	Веб-угрозы	13%
Spyware	12%	Фишинг	9%
Adware	10%	Трояны	16%
Maleware	9%	Черви	8%
Баннеры	10%		

Таблица 4. Число пропущенных угроз межсетевыми экранами

	Вирусы	**Spyware**	**Adware**	**Maleware**	**Баннер**	**Веб-угрозы**	**Фишинг**	**Трояны**	**Черви**
Kaspersky Internet Security			3		4		2		
McAfee Internet Security	1		3					3	
Avast Internet Security				2		5	2		4
Eset Smart Security	1		4	3		2			1
Panda Internet Security				3	3				5

3. Интерфейс реализованного программного приложения

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

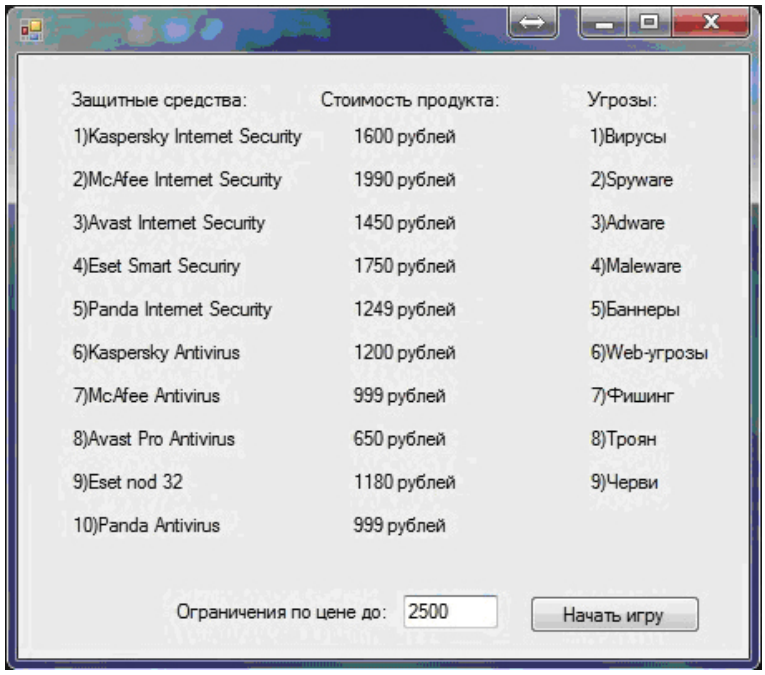

Рис. 1. Интерфейс начального окна приложения

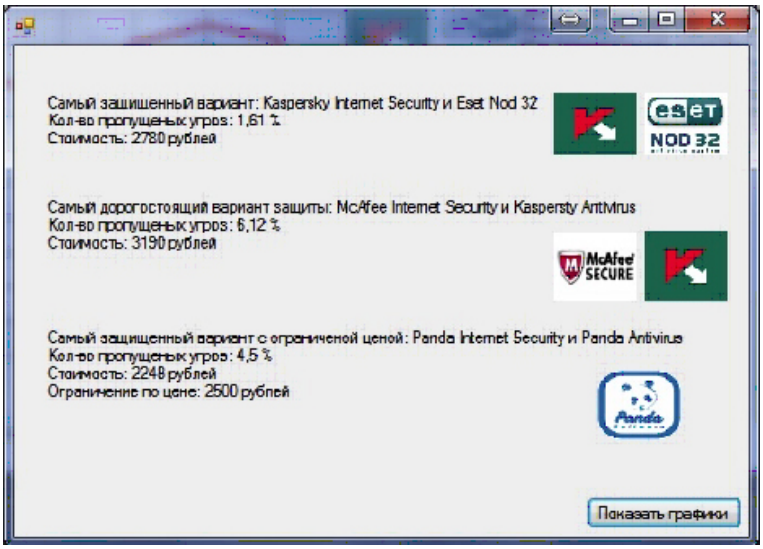

Рис. 2. Окно приложения с результатом игры

нахождение оптимального набора с возможностью ограничения по стоимости программного обеспечения (рис. 1).

Применение предложенного программного продукта позволяет находить наиболее оптимальный набор средств защиты компьютерной информации и анализировать полученные результаты. На рис. 2 показаны результаты расчётов наилучшей пары при выборе из антивирусных систем и межсетевых экранов.

Реализованное приложение позволяет более детально просмотреть результа-

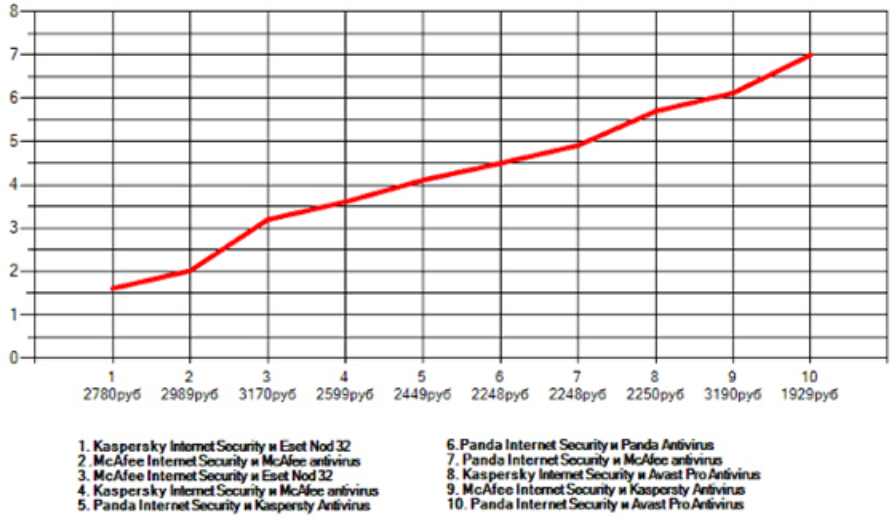

Рис. 3. Результаты анализа проникновения угроз для 10 лучших решений

ты проведённых расчётов для десяти наиболее оптимальных решений (рис.3).

Приложение было разработано на языке программирования C# для операционной системы Windows. В реализованном приложении предполагается дополнение матрицы другими видами угроз и средствами защиты. В случае нескольких решений предпочтение отдаётся более дешёвому набору программных продуктов.

4. Заключение

Применение предложенного в данной работе программного продукта даст администратору безопасности возможность выбрать наиболее оптимальный набор средств защиты компьютерной информации, а также оценить эффективность уже используемого программного обеспечения.

Литература

1. Вахний Т.В., Гуц А.К. Теория игр и защита компьютерных систем: Учебное пособие. Омск: Изд-во ОмГУ, 2013. 160 с.
2. Вахний Т.В., Гуц А.К. Теоретико-игровой подход к выбору оптимальных стратегий защиты информационных ресурсов // Математические структуры и моделирование. 2009. № 19. С.104-107.
3. Вахний Т.В., Гуц А.К., Константинов В.В. Программное приложение для выбора оптимального набора средств защиты компьютерной информации на основе теории игр // Вестник Омского университета. 2013. № 4 (70). С. 201-206.

OPTIMAL SELECTION OF THE ANTIVIRUS PROGRAM AND THE FIREWALL BY MEANS OF THE GAME THEORY

T.V. Vahniy
Associent Professor, Ph.D. (Phys.), e-mail: vahniytv@mail.ru
A.K. Guts
Associent Professor, Ph.D. (Phys.), e-mail: aguts@mail.ru
S.Yu. Kuzmin
Student), e-mail: sergkuz2@gmail.com

Omsk State University n.a. F.M. Dostoevskiy

Abstract. Application of the game theory approach to search for the most optimal set of defence computer system software is described on the example of antivirus system and firewall selection.

Keywords: optimal selection of software, game theory, information defence.