Вестн. Ом. ун-та. 2013. № 4. С. 201–206.

УДК 004.056.5:005.311.7

Т.В. Вахний, А.К. Гуц, В.В. Константинов

ПРОГРАММНОЕ ПРИЛОЖЕНИЕ ДЛЯ ВЫБОРА ОПТИМАЛЬНОГО НАБОРА СРЕДСТВ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ НА ОСНОВЕ ТЕОРИИ ИГР

Представлено программное приложение, позволяющее производить поиск наиболее оптимального набора средств защиты компьютерных информационных ресурсов. Применение реализованного в данной работе программного продукта даст администратору безопасности возможность оценить эффективность используемого программного обеспечения и выбрать наиболее оптимальный набор средств защиты компьютерной информации.

Ключевые слова: программа, защита информации, теория игр.

Введение

В настоящее время, по мере развития и расширения сферы применения средств вычислительной техники, острота проблемы обеспечения безопасности вычислительных систем и защиты хранящейся и обрабатываемой в них информации от различных угроз все более возрастает. В первую очередь эта проблема связана с широким распространением локальных и особенно глобальных компьютерных сетей. Защита информации необходима для уменьшения вероятности утечки (разглашения), модификации (умышленного искажения) или утраты (уничтожения) информации, представляющей определенную ценность для ее владельца.

Сегодня на рынке представлено огромное разнообразие средств защиты компьютерной информации, и администратору безопасности приходится принимать субъективные решения о выборе в пользу тех или иных программных продуктов. Использование теории матричных игр позволяет обеспечить оптимизацию выбора программных продуктов для защиты компьютерной информации.

Постановка задачи и игровой подход

Для поиска наиболее оптимальных стратегий защиты информационных ресурсов можно провести математическую игру двух сторон, одной из которых является система защиты компьютерной информации, а другая – возможные атаки хакеров. Нанесение хакером ущерба обычно является скорее следствием его действий, чем не самой целью. В действительности при атаке он может преследовать какие-то свои цели, порой известные лишь ему. Поскольку целью данной работы являлось определение администратором безопасности оптимальной стратегии защиты, а цели атакующих хакеров были неважны, то можно считать, что хакер увлечен желанием нанести как можно больший ущерб атакуемой компьютерной системе. При таком предположении выигрыш хакера будет равен проигрышу администратора безопасности, и можно получить матрицу для игры двух лиц с нулевой суммой.

В качестве стратегий хакера будем понимать строки $x_i \quad (i = 1,...,n)$ некоторой матрицы, а в качестве стратегий администратора безопасности – ее столбцы $y_j \quad (j = 1,...,m)$. К стратегиям хакера можно отнести различные виды компьютерных атак, а к стратегиям администратора – различные средства защиты компьютерной информации.

В настоящее время рынок может предложить огромное количество программных продуктов, обеспечивающих защиту компьютерной информации. Чтобы ограничиться выбором конечного списка программных продуктов, был исследован ресурс Anti-Malware.ru, который проводит независимую экспертизу персональных и корпоративных продуктов и сервисов по информационной безопасности. Анализ выбранных средств защиты позволяет каждому программному продукту сопоставить возможность устранить определенные угрозы.

Для проведения на компьютере игры *A* надо также знать результаты игры при каждой паре стратегий x_i и y_j (например, a_{ij} причинённый хакером материальный ущерб) и вероятности реализации атак хакеров $p(x_i)$ при выбранной стратегии x_i. Вероятности реализации атак $p(x_i)$ могут быть определены по результатам статистических исследований. Полезно установить систему обнаружения хакерских атак (IDS), например, свободно распространяемую систему Honeynet. Она позволяет набрать статистику, с помощью которой можно выявить наиболее распространённые типы атак x_i и вычислить вероятности $p(x_i)$ хакерских стратегий. Если вероятности атак неизвестны, то можно предположить, что все они равновероятны, т. е. $p(x_i) = 1/n$.

В качестве коэффициентов a_{ij} матрицы игры *A* можно рассматривать, например, годовые потери для всех вариантов комбинаций x_i $(i = 1,...,n)$ и y_j $(j = 1,...,m)$. Для этого нужно сопоставить каждую атаку с каждым методом защиты и определить ущерб, который может быть при этом нанесён. Покупка, установка и использование средств защиты могут требовать дополнительных затрат, что также нужно вносить в ущерб при расчётах.

Построив игровую матрицу (табл. 1) и проанализировав её, можно заранее оценить затраты каждого решения по защите компьютерной информации и выбрать наиболее эффективные варианты для всего диапазона атак. Если построена игровая матрица *A*, в которой результатами игры являются материальные потери от атак, то наилучшей в условиях имеющейся информации об атаках будет стратегия системы защиты компьютерной информации y_i, при которой будут минимальны средние потери, т. е. будет минимальна сумма:

$$\sum_{i-1}^{n} a_{ij} p(x_i) .$$

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 выбора наиболее оптимального набора средств защиты компьютерных информационных ресурсов в математической игре в качестве стратегий следует использовать различные сочетания из атак и методов защиты. Прекращение использования или добавление нового средства (атаки или защиты) можно рассматривать как переход от одной стратегии к другой.

Целью игрока I (хакера) в матричной игре является, естественно, получение, по возможности, большего выигрыша. Цель же игрока II (администратора) состоит в том, чтобы дать хакеру I возможно меньший выигрыш. Поэтому разумное поведение игроков в матричной игре должно основываться на следующих рассуждениях.

Пусть игрок I выбирает некоторую свою стратегию i. Тогда в наихудшем случае (а в теории игр игроки предполагаются весьма осторожными и рассчитывают на наименее благоприятный для себя поворот событий; такое наименее благоприятное для игрока I положение дел может наступить, например, в том случае, когда стратегия i станет известной игроку II) он получит выигрыш

$$\min_j a_{ij} .$$

Предвидя такую возможность, игрок I должен выбрать свою стратегию i_0 так, чтобы максимизировать этот свой минимальный выигрыш:

$$\min_j a_{i_0 j} = \max_i \min_j a_{ij} . \qquad (1.1)$$

Значит, стоящий в правой части написанного равенства «максимин» является гарантированным выигрышем игрока I. Симметричные рассуждения, проводимые за игрока II, показывают, что игрок II должен выбирать такую свою стратегию j_0, что

$$\min_i a_{ij_0} = \min_j \max_i a_{ij} . \qquad (1.2)$$

Здесь стоящий справа «минимакс» является тем выигрышем игрока I, больше которого он при правильных действиях противника получить не может. Поэтому фактический выигрыш игрока I должен при разумных действиях партнеров лежать между правыми частями формул (1.1) и (1.2). Выигрыш игрока I называется значением игры и равен элементу матрицы $a_{i_0 j_0}$ [1; 2].

Расчет ущерба от применения тех или иных стратегий хакером

Для расчета ущерба, наносимого той или иной стратегией хакера, требуются следующие данные:

- общее число угроз;
- набор угроз из текущей стратегии хакера;
- величины ущерба для каждой угрозы;
- общее число средств защиты;
- набор средств защиты из текущей стратегии администратора безопасности;
- стоимость каждого из средств защиты;
- соотношение каждого средства защиты с угрозами, от которых оно защищает.

Ущерб складывается из величин 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 из общей стоимости всех средств защиты из текущей стратегии администратора безопасности.

Для подсчета общей стоимости нужных средств защиты необходимо сопоставить текущий набор средств защиты и все имеющиеся средства защиты и суммировать величины стоимости тех средств, которые присутствуют в первом наборе.

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. В результате сопоставления текущего набора угроз со всеми средствами из текущей стратегии администратора безопасности получается некоторое количество угроз, от которых система в данном случае не защищена. Полученные угрозы нужно сопоставить со всеми имеющимися угрозами, а также суммировать величины ущерба тех угроз, которые присутствуют в полученном наборе. Далее эти две суммы складываются, в результате и получается ущерб при применении текущей пары стратегий хакера и администратора безопасности.

Вычисление оптимальной стратегии для администратора безопасности

Для вычисления оптимальной стратегии необходимы следующие данные:

- все возможные комбинации из угроз, которые может реализовать хакер;
- все возможные комбинации из продуктов, обеспечивающих защиту;
- величины ущерба от применения тех или иных пар стратегий (см. предыдущий раздел).

В качестве основы для расчетов берется формула (1.2). Для начала составляется таблица (матрица), строками которой являются стратегии хакера, а столбцами – стратегии администратора безопасности. На пересечении стратегий ставятся величины ущерба, рассчитанные по алгоритму из предыдущего раздела.

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

Описание программного продукта

В данной работе был реализован программный продукт, который по введённым значениям стоимости средств защиты и ущерба от применения всех возможных пар «атака – защита» вычисляет оптимальный набор из имеющихся в его базе программных продуктов. На рис. 1 представлена главная страница реализованного приложения.

Справа на главной странице реализованного приложения расположен список используемых продуктов, обеспечивающих безопасность компьютерной информации. При каждом элементе он имеет поле типа «checkbox», что позволяет использовать в расчетах не все предложенные продукты, а только часть из них. Под списком продуктов есть ссылка «подробнее», нажав на которую можно более детально ознакомиться с имеющимися продуктами. Данная ссылка открывает новую страницу, где перечислены продукты, указана их цена и дано краткое описание (рис. 2). Название каждого продукта также является ссылкой, ведущей на страницы соответствующих продуктов на официальных сайтах производителей.

В связи с тем что каждое из описанных выше средств обеспечения безопасности защищает сразу от нескольких угроз, необходимо каждому средству защиты поставить в соответствие угрозы, от которых оно способно защитить. Анализ возможностей перечисленных в предыдущем разделе средств защиты позволяет каждому продукту поставить в соответствие определенные угрозы. Результат приведен в табл. 2. Столбцы представляют средства защиты с номерами, соответствующими таблице на рис. 2, а строки представляют возможные угрозы с номерами из таблицы слева на рис. 1.

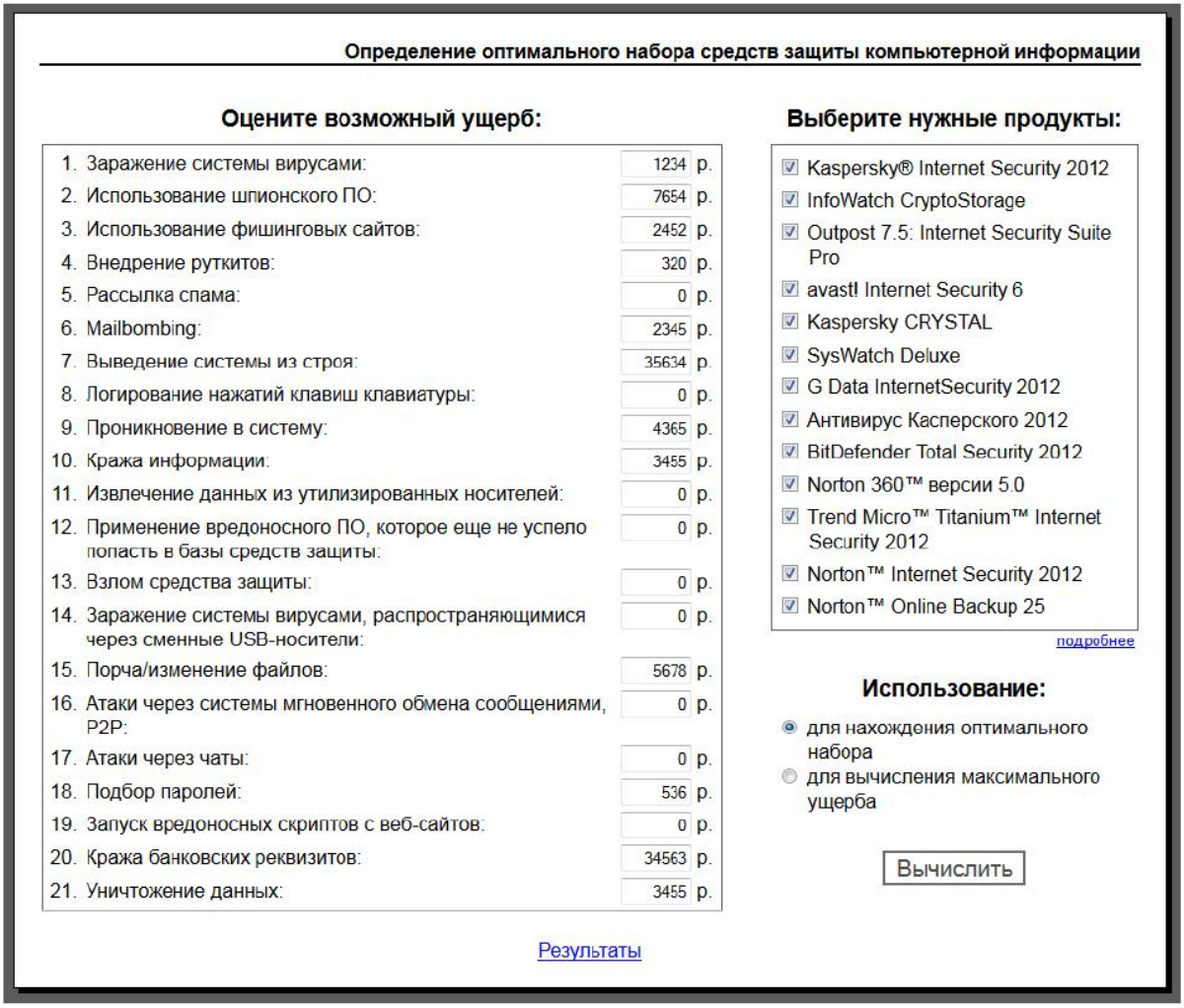

Рис. 1. Главная страница приложения

Рис. 2. Подробное описание программных продуктов,
обеспечивающих защиту информации (стратегии j=1,2,3,4,…)

Таблица 2

Соответствие средств защиты (стратегий *j*) и возможных угроз (стратегий *i*)

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	+		+	+	+	+		+	+	+	+	+	
2	+		+	+	+		+	+	+	+	+	+	
3	+				+		+	+		+	+	+	
4	+			+	+			+					
5	+		+	+	+		+		+	+	+	+	
6				+			+			+		+	
7	+				+			+		+		+	
8								+					
9	+		+	+	+		+		+	+	+	+	
10		+			+						+		+
11		+			+						+		
12			+										
13			+			+							
14			+										
15			+			+					+		
16				+						+		+	
17				+			+			+		+	
18					+								
19	+		+	+	+	+	+			+	+	+	
20							+						
21					+				+	+	+		+

Определение оптимального набора средств защиты компьютерной информации

Результаты

№	Набор средств защиты	Стоимость	Максимальный ущерб	Сумма
1	2, 4, 8, 9	4674	3502	8176
2	2, 4, 8	3689	5734	9423
3	2, 3, 4, 8, 9	5973	3016	8989

Назад

Рис. 3. Результат вычислений приложения

Под списком средств защиты находится блок под названием «Использование» (см. рис. 1). Он определяет, как будут использованы выбранные выше средства защиты. Первый режим означает, что из выбранных продуктов будут составлены все возможные комбинации, и из этих комбинаций будет выбрана оптимальная. Второй режим – что будет произведено вычисление максимального ущерба при использовании выбранных средств. Также следует отметить, что при переключении на первый режим все поля типа «checkbox» заполняются, а на втором режиме очищаются. Это сделано для того, чтобы при выборе своего набора средств на проверку не приходилось постоянно вручную очищать все ненужные поля. Особенно это критично, если для выбора доступно большое число средств защиты.

С левой стороны главной страницы расположен список возможных угроз (рис. 1). Здесь необходимо оценить в рублях, какой ущерб может быть нанесен при реализации той или иной угрозы. По умолчанию в данном программном продукте все величины ущерба равны нулю, и администратору безопасности потребуется их заполнение на основе установленной системы обнаружения хакерских атак и их статистического анализа.

В самом низу главной страницы приложения находится кнопка «Вычислить» (см. рис. 1). По ее нажатии производятся необходимые вычисления и выводится результат (рис. 3). Если в текущей сессии уже проводились какие-то вычисления, то ниже блока

«Использование» будет отображена ссылка «Результаты», пройдя по ней, можно ознакомиться с результатами вычислений, полученными ранее. После нажатия на кнопку «Вычислить» или ссылку «Результаты» открывается блок с результатами вычислений (рис. 3).

Результат вычислений содержит таблицу со следующими полями:

1) номер подпункта;

2) набор из средств защиты (в зависимости от режима является либо оптимальным набором, либо набором средств, который был выбран на главной странице);

3) общая сумма стоимости средств защиты;

4) максимальный ущерб, который можно получить, используя данный набор средств защиты;

5) сумма стоимости средств защиты и максимального ущерба.

Результат последнего вычисления добавляется в конец таблицы. При выборе из базы данных оптимального набора программных продуктов для защиты компьютерной информации предпочтение отдаётся более дешёвым аналогам. Таким образом, администратор безопасности может сначала получить оптимальный набор методов защиты, а потом изменять его, сверяясь с получающейся величиной максимального ущерба. При этом, если вычисление проводилось в режиме поиска оптимального набора средств защиты, то новая запись имеет белый фон. Если же производился подсчет максимального ущерба для выбранных средств защиты, то запись выделяется серым фоном. Как видно из рис. 3, оптимальная стратегия всегда имеет общую сумму ущерба меньшую, чем у стратегий, составленных пользователем, даже если они выигрывают по стоимости средств защиты или величине ущерба.

Приложение позволяет распечатать страницу как с описанием используемых продуктов, обеспечивающих безопасность компьютерной информации, так и с результатами вычислений. Для того чтобы данные имели подходящий для печати вид, используются альтернативные каскадные таблицы стилей. При отправке страницы на печать они автоматически преобразуют ее в нужную форму. Чтобы распечатать список средств защиты, нужно всего лишь, находясь на странице с их описанием, воспользоваться функцией печати, предлагаемой браузером. Результаты вычислений можно печатать как с главной страницы, так и со страницы с самими результатами.

Средства разработки и среда выполнения приложения

Реализованный в данной работе программный продукт представляет собой веб-приложение, полностью выполняющееся на стороне клиента. Интерфейс его создается с помощью HTML и CSS, взаимодействие с пользователем и простые операции осуществляются языком JavaScript, а сложные ресурсоемкие вычисления доверяются Java-апплету.

Приложение должно запускается в браузере. Но одного лишь браузера недостаточно для корректной работы приложения. Для работы Java-апплета на машине, с которой запускается приложение, должна стоять JVM (виртуальная машина Java). HTML, CSS и JavaScript в настоящее время поддерживаются всеми популярными браузерами, но не всегда одинаково. Из-за проблем совместимости приложение, которое успешно запускается в одном браузере, может некорректно работать в другом.

При разработке данного приложения использовались Java Runtime Environment версии 6 update 30 от компании Oracle и браузер Mozilla Firefox 9.0.1. Поэтому корректную работу приложения можно гарантировать только при использовании этого программного обеспечения.

Заключение

Применение реализованного в данной работе программного продукта даст администратору безопасности возможность оценить эффективность используемого программного обеспечения и выбрать наиболее оптимальный набор средств защиты компьютерной информации.

ЛИТЕРАТУРА

[1] Матричные игры / под ред. Н. Н. Воробьева. М : ФМ, 1961. 280 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.