Математические структуры и моделирование
2015. № 3(35). С. 91–105

УДК 519.83+681.3.067

УЧЁТ ВЕРОЯТНОСТЕЙ ХАКЕРСКИХ АТАК В ИГРОВОМ ПОДХОДЕ К ПОДБОРУ ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Т.В. Вахний
к.ф.-м.н., доцент, e-mail: vahniytv@mail.ru
А.К. Гуц
д.ф.-м.н., профессор, e-mail: guts@omsu.ru
С.С. Бондарь
студент, e-mail: dx-5_razor@mail.ru

Омский государственный университет им. Ф.М. Достоевского

Аннотация. Описывается программное приложение для расчёта оптимального набора средств защиты компьютерной информации на основе теории игр с учётом вероятностей хакерских атак. Протестированы на совместимость друг с другом все используемые в игре программные средства защиты, использовано два подхода к определению величин вероятностей хакерских атак, выполнено сравнение результатов с учётом найденных величин вероятностей и без учёта.

Ключевые слова: Защита информации, теория игр, хакерские атаки, оптимальная стратегия, программный продукт.

Введение

Проблемы защиты информации, хранящейся в корпоративных компьютерных системах, беспокоят не только владельцев информационных ресурсов и специалистов в области компьютерной безопасности, но и многочисленных рядовых пользователей персональных компьютеров. В настоящее время на рынке представлено огромное разнообразие средств защиты компьютерной информации, и неизбежно приходится принимать субъективные решения о выборе в пользу тех или иных программных продуктов.

Естественным является желание иметь программное приложение, с помощью которого можно делать выбор в пользу того или иного программного средства защиты компьютерной информации.

Использование теории игр позволяет обеспечить оптимизацию выбора программных продуктов для защиты информации, хранящейся в компьютерных системах [1–5].

В статье описывается программное приложение, решающее подобную задачу. Кроме того в данной работе уделено внимание как изучению статистики хакерских атак, так и определению вероятностей возможных атак опытным путём. Было создано программное приложение для расчёта оптимального набора

средств защиты компьютерной информации на основе теории игр с учётом найденных величин вероятностей. Приводится сравнение полученных оптимальных наборов программных средств защиты с учётом и без учёта вероятностей атак.

1. Постановка задачи и игровой подход

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, 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 столбцы x_j $(j = 1, ..., m)$ (различные средства защиты компьютерной информации) некоторой матрицы (табл. 1), а в качестве стратегий злоумышленника — её строки y_i $(i = 1, ..., n)$ (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. **Платежная матрица и вероятности**

		x_1	x_2	...	x_m
y_1	$p(y_1)$	a_{11}	a_{12}	...	a_{1m}
y_2	$p(y_2)$	a_{21}	a_{22}	...	a_{2m}
...	...	...	...	...	...
y_n	$p(y_n)$	a_{n1}	a_{n2}	...	a_{nm}

Для проведения на компьютере игры A надо также знать результаты игры при каждой паре стратегий x_j и угроз y_i (например, a_{ij} — причинённый ущерб) и вероятности реализации $p(y_i)$ каждой угрозы y_i. Наилучшей в условиях имеющейся информации об угрозах считалась стратегия системы защиты компьютерной информации, т. е. набор средств защиты x_i, для которой будет

минимальна сумма

$$\sum_{i=1}^{n} a_{ij} p(y_i). \tag{1}$$

2. Матрица игры

В настоящее время рынок может предложить огромное количество программных продуктов, обеспечивающих защиту компьютерной информации. Для участия в матричной игре были отобраны 12 наиболее популярных из представленных на сайте независимого информационно-аналитического центра информационной безопасности Anti-Malware.ru.

1. Kaspersky® Anti-Virus.
2. Kaspersky® Internet Security.
3. Kaspersky® Total Security.
4. InfoWatch CryptoStorage.
5. BitDefender Total Security 2015.
6. Avast Internet Security.
7. Avast Premier.
8. Norton Security.
9. Norton Online Backup.
10. Trend Micro™ Titanium™ Internet Security.
11. G Data Anti-virus.
12. Sys Watch Deluxe.

При составлении матрицы игры перечисленные выше программные продукты и их возможные сочетания определяем как ходы или стратегии администратора безопасности.

На сайтах производителей можно ознакомиться с возможностями защитных программных продуктов и узнать, от каких угроз они защищают. Список программных средств защиты необходимо постоянно обновлять, так как рынок продуктов для защиты компьютерной информации постоянно меняется. В качестве угроз сохранности компьютерной информации были выбраны следующие:

1. Заражение системы вирусами.
2. Использование шпионского программного обеспечения (ПО).
3. Использование фишинговых сайтов.
4. Внедрение руткитов.
5. Рассылка спама.
6. Mailbombing.
7. Выведение системы из строя.
8. Логирование нажатий клавиш клавиатуры.
9. Проникновение в систему.
10. Кража информации.
11. Извлечение данных из утилизированных носителей.
12. Применение вредоносного программного обеспечения, которое еще не успело попасть в базы данных средств защиты.

13. Взлом средств защиты.

14. Заражение системы вирусами, распространяющимися через съёмные USB-носители.

15. Порча/изменение файлов.

16. Атаки через системы мгновенного обмена сообщениями, P2P.

17. Подбор паролей.

18. Запуск вредоносных скриптов с веб-сайтов.

19. Кража банковских реквизитов.

20. Уничтожение данных.

В качестве возможных стратегий хакеров были как данные угрозы в отдельности, так и всевозможные сочетания из этих угроз. В таблице 2 приведено сопоставление средств защиты с угрозами, от которых они защищают. Столбцы этой таблицы соответствуют выбранным программным продуктам защиты информации, а строки — выбранным угрозам. На их пересечении стоит знак «+», если программный продукт защищает от соответствующей угрозы.

Для проведения игры необходимо также учитывать, что некоторые программные продукты не совместимы друг с другом. Для проверки выбранных средств защиты на совместимость была использована программа Oracle VM Virtual Box, которая позволяет пользователям создавать, импортировать и запускать на своих компьютерах несколько виртуальных машин одновременно, с различными конфигурациями, разными версиями Windows или с другими операционными системами, такими как Linux или Mac OS X.

В таблице 3 отражена совместимость выбранных средств защиты. Столбцы и строки этой таблице соответствуют номерам средств защиты, знак "+" на их пересечении указывает, что соответствующие программные продукты совместимы, т. е. они не мешают работе друг друга.

Компоненты матрицы игры

$$a_{ij} = \textbf{стоимость средства защиты } x_j + \textbf{ущерб от удачной атаки } y_i.$$

3. Интерфейс реализованного программного приложения

На основе описанного подхода было создано программное приложение, которое по введённым значениям стоимости средств защиты и величинам вероятностей хакерских угроз вычисляет оптимальный набор средств защиты из имеющихся в распоряжении администратора безопасности программных продуктов. В реализованном приложении предусмотрено нахождение оптимального набора с учётом величин вероятностей хакерских атак. Интерфейс приложения состоит из нескольких компонент, располагающихся на основной форме:

1. Список средств защиты, обеспечивающих защиту компьютерной информации, расположен с правой стороны основной формы, каждое из средств защиты имеет поле типа «checkbox», позволяющее выбирать определённый набор средств защиты (рис.1).

Таблица 2. **Сопоставление программных средств защиты с угрозами**

№	1	2	3	4	5	6	7	8	9	10	11	12
1	+	+	+		+	+	+	+		+		+
2		+	+		+	+	+	+		+	+	
3	+	+	+			+	+	+		+	+	
4	+	+	+									
5					+		+	+		+	+	
6						+	+	+			+	
7		+	+				+	+		+		
8	+	+	+			+	+					
9	+	+	+		+			+		+		
10		+	+	+						+		
11				+								
12						+						
13	+	+	+				+					+
14	+	+	+									
15									+			+
16	+	+	+			+	+	+		+		
17	+	+	+			+	+	+		+		
18			+				+					+
19			+				+					
20					+				+			

2. Под списком средств защиты есть ссылка «подробнее», нажав на которую можно более детально ознакомиться с выбранными программными продуктами. Данная ссылка открывает новую форму, где перечислены средства защиты, указана их цена, а также дано краткое описание каждого из них (рис. 2).

3. С левой стороны формы расположен список возможных угроз (рис. 3). Здесь необходимо оценить в рублях, какой ущерб может быть нанесён при реализации той или иной угрозы, а также вероятность реализации этой угрозы.

4. В правом нижнем углу страницы находятся три кнопки: «Рассчитать», «Выделить все/ Снять все», «Автозаполнение вероятностей» (рис. 4).

При нажатии на кнопку «Выделить все/Снять все» изменяются все поля типа «checkbox» (рис. 1) на противоположные. При нажатии на кнопку «Автозаполнение вероятностей» происходит автоматическое заполнение всех полей вероятностей хакерских атак равными значениями.

Таблица 3. **Совместимость выбранных средств защиты**

№	1	2	3	4	5	6	7	8	9	10	11	12
1	+			+					+			+
2		+		+					+			+
3			+	+					+			+
4	+	+	+	+	+	+	+	+	+	+	+	+
5				+	+				+			+
6				+		+			+			+
7				+			+		+			+
8				+				+	+			+
9	+	+	+	+	+	+	+	+	+	+	+	+
10				+					+	+		+
11				+					+		+	+
12	+	+	+	+	+	+	+	+	+	+	+	+

Рис. 1. Средства защиты

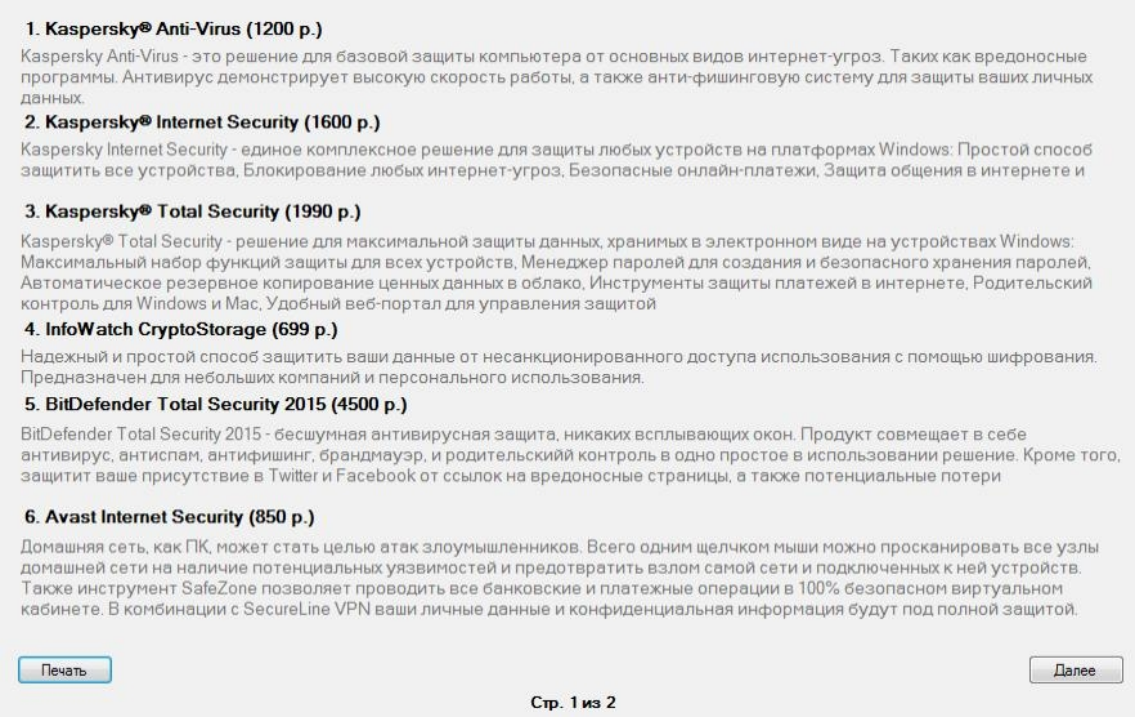

Рис. 2. Описание средств защиты

При нажатии на кнопку «Рассчитать», производятся необходимые вычисления, и полученные три наиболее оптимальных набора средств защиты записываются в форму результатов (рис. 5).

Результаты, представленные на рис. 5, — это лучшие стратегии защиты из неполного списка средств защиты. В игре участвовали только средства защиты 4, 8, 10 и 12, а вероятности атак брались из табл. 4. Видно, что ущерб оказывается больше, чем в случае использования полного списка средств защиты (сравните данные рисунков 5 и 7).

Применение предложенного программного продукта позволяет находить наиболее оптимальный набор средств защиты компьютерной информации и анализировать полученные результаты.

Угрозы	Ущерб		Вероятность	
Заражение системы вирусами		р.		%
Использование шпионского ПО		р.		%
Использование фишинговых сайтов		р.		%
Внедрение руткитов		р.		%
Рассылка спама		р.		%
Mailbombing		р.		%
Выведение системы из строя		р.		%
Логирование нажатий клавиш клавиатуры		р.		%
Проникновение в систему		р.		%
Кража информации		р.		%
Извлечение данных из утилизированных носителей		р.		%
Применение вредоносного ПО, которое еще не успело попасть в базы данных средств защиты		р.		%
Взлом средств защиты		р.		%
Заражение системы вирусами, распространяющимися через съемные USB - носители		р.		%
Порча/изменение файлов		р.		%
Атаки через системы мгновенного обмена сообщениями, P2P		р.		%
Подбор паролей		р.		%
Запуск вредоносных скриптов с веб-сайтов		р.		%
Кража банковских реквизитов		р.		%
Уничтожение данных		р.		%

Рис. 3. Список возможных угроз

4. Определение величин вероятностей хакерских атак и учёт их в расчётах

Вероятности реализации каждой угрозы $p(y_j)$ можно принять равными. Нажав на кнопку «Автозаполнение вероятностей», получим в нашем случае вероятность каждой хакерской атаки 5%. На рис. 6 показаны результаты расчётов для случая равновероятных атак при предположении, что ущерб от каждой угрозы составляет 10000 руб.

В этом случае оптимальным средством для защиты компьютерной информации является Kaspersky Total Security, его стоимость 1990 руб., максимальный урон от пропущенных атак равняется 2500 руб., и сумма цены данного средства защиты и максимального ущерба составит 4490 рублей. Учёт в расчётах величин вероятностей хакерских атак может сказаться на результатах работы приложения. По данным портала http://www.sicherheitstacho.eu/ с 01.05.2014 по 01.05.2015 при помощи ловушек для хакеров (honeypot) было зарегистрировано около 141 миллиона атак. На основе соотношения этих атак были рассчитаны вероятности их реализации, они приведены в таблице 4.

Результаты расчётов оптимального набора средств защиты компьютерной информации при использовании приведённых в табл. 4 значений вероятностей атак приведены на рис. 7.

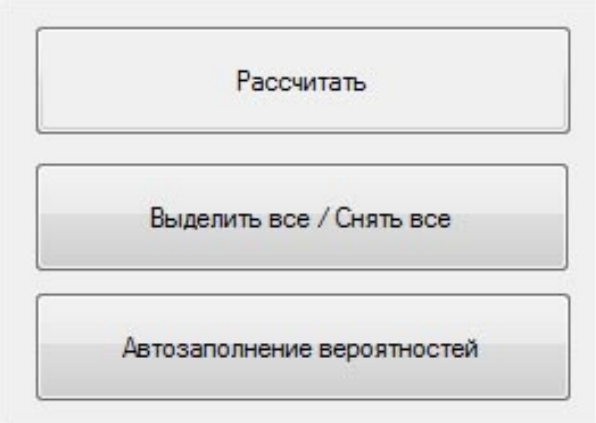

Рис. 4. Набор кнопок

Результаты

№	Набор средств защиты	Стоимость	Максимальный ущерб	Сумма
1	8 4 Norton Security, InfoWatch CryptoStorage,	2498	4199	6697
2	8 12 Norton Security, Sys Watch Deluxe,	2699	4100	6799
3	10 4 12 Trend Micro™ Titanium™ Internet Security, InfoWatch CryptoStorage, Sys Watch Deluxe,	2249	4899	7148

Печать

Рис. 5. Окно результатов вычислений приложения. Выбирались лучшие стратегии из неполного списка средств защиты (в игре участвовали только средства защиты 4, 8, 10 и 12; вероятности атак взяты из табл. 4)

Результаты

№	Набор средств защиты	Стоимость	Максимальный ущерб	Сумма
1	3 Kaspersky® Total Security ,	1990	2500	4490
2	2 Kaspersky® Internet Security,	1600	3500	5100
3	7 Avast Premier,	1950	3500	5450

Печать

Рис. 6. Результаты вычислений для случая равных вероятностей хакерских атак

Таблица 4. **Статистические данные вероятностей хакерских угроз**

№	Угрозы	Количество	% от общих
1	Заражение системы вирусами	10235490	~10%
2	Использование шпионского ПО	5052303	~5%
3	Использование фишинговых сайтов	4040020	~4%
4	Внедрение руткитов	5019764	~5%
5	Рассылка спама	5042300	~5%
6	Mailbombing	5023450	~5%
7	Выведение системы из строя	10200102	~10%
8	Логирование нажатий клавиш клавиатуры	3020400	~3%
9	Проникновение в систему	2014050	~2%
10	Кража информации	7042030	~7%
11	Извлечение данных из утилизированных носителей	7002000	~7%
12	Применение вредоносного ПО, которое еще не успело попасть в базы данных средств защиты	5040200	~5%
13	Взлом средств защиты	2010300	~2%
14	Заражение системы вирусами, распространяющимися через съемные USB-носители	2020540	~2%
15	Порча/изменение файлов	2010530	~2%
16	Атаки через системы мгновенного обмена сообщениями, P2P	2000500	~2%
17	Подбор паролей	5052030	~5%
18	Запуск вредоносных скриптов с веб-сайтов	4002500	~4%
19	Кража банковских реквизитов	5002940	~5%
20	Уничтожение данных	11004205	~10%

Результаты

№	Набор средств защиты	Стоимость	Максимальный ущерб	Сумма
1	3 4 12 Kaspersky® Total Security , InfoWatch CryptoStorage, Sys Watch Deluxe,	3589	2299	5888
2	2 4 12 Kaspersky® Internet Security, InfoWatch CryptoStorage, Sys Watch Deluxe,	3199	3199	6398
3	7 4 12 Avast Premier, InfoWatch CryptoStorage, Sys Watch Deluxe,	3549	2899	6448

Печать

Рис. 7. Результаты расчётов при использовании статистических данных для определения вероятностей угроз

Таблица 5. **Вероятности атак, полученные с помощью Kaspersky Total Security**

№	Угрозы	Количество	% от общих
1	Заражение системы вирусами	14	~41%
2	Использование фишинговых сайтов	7	~20%
3	Применение вредоносного ПО, которое еще не успело попасть в базы данных средств защиты	3	~9%
4	Заражение системы вирусами, распространяющимися через съемные USB-носители	3	~9%
5	Порча/изменение файлов	3	~9%
6	Запуск вредоносных скриптов с веб-сайтов	4	~12%

Результаты

№	Набор средств защиты	Стоимость	Максимальный ущерб	Сумма
1	3 Kaspersky® Total Security ,	1990	1800	3790
2	1 Kaspersky® Anti-Virus,	1200	3000	4200
3	2 Kaspersky® Internet Security.	1600	3000	4600

Печать

Рис. 8. Результаты расчётов для вероятностей, полученных опытным путем с помощью Kaspersky Total Security

В этом случае оптимальным набором средств защиты компьютерной информации являются три программных продукта: Kaspersky Total Security, InfoWatch и Sys Watch Deluxe. Их общая стоимость 3589 руб., максимальный урон от пропущенных атак равняется 2299 руб., и сумма цен данных средств защиты и максимального ущерба составит порядка 5588 рублей. Таким образом, учёт величины вероятностей хакерских атак потребовал дополнить систе-

му защиты ещё двумя программными средствами.

Было интересно также получить величины вероятностей угроз для обычного пользователя персонального компьютера опытным путём. Для этого на персональный компьютер был установлен Kaspersky Total Security. За месяц работы на персональном компьютере антивирус обнаружил 34 атаки, результаты приведены в таблице 5. На основе данных наблюдений также были рассчитаны вероятности атак на персональный компьютер (ПК).

Результаты расчётов приложения для величин вероятностей атак, полученных с помощью Kaspersky Total Security, представлены на рисунке 8.

Как видно из рис. 8, в этом случае самым оптимальным средством для защиты компьютерной информации оказался Kaspersky Total Security, как и в случае равных вероятностей атак. Следовательно, в настоящее время для защиты компьютерной информации на ПК обычного пользователя оптимальным вариантом является использование только одного программного продукта Kaspersky Total Security. Для защиты компьютерных систем организации предпочтительнее изучать статистику атак и использовать большее количество программных средств для защиты информации.

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.

5. Пути усовершенствования разработанной программы

Созданное программное приложение может быть улучшено следующим образом.

1. Игра, описанная в начале статьи, не является в прямом смысле матричной, поскольку не является игрой с нулевой суммой. Поэтому было бы целесообразно найти критерий оптимальности пары стратегий (x_{j_*}, y_{i_*}) администратора и хакера соответственно и сравнить их с найденной оптимальной стратегией x_{j_0}.

Напомним, что оптимальным мы считали такой набор средств защиты x_{j_0}, для которого минимальна сумма

$$\sum_{i=1}^{n} a_{ij} p(y_i),$$

т.е.

$$\sum_{i=1}^{n} a_{ij_0} p(y_i) = \min_{1 \le j \le m} \sum_{i=1}^{n} a_{ij} p(y_i).$$

2. Во-вторых, полезно было бы оценить как риск, связанный с использованием оптимальной стратегии x_j, так и степень защищённости компьютерной

системы при использовании администратором стратегии x_j защищаемой компьютерной системы. Степень защищённость ресурса при использовании стратегии x_j защиты при использовании в хакерской атаке стратегии y_i можно с помощью показателя

$$S_{ij} = \frac{1}{p(y_i)L_i(1-k_{ij})}, \tag{2}$$

где $p(y_i)$ — вероятность стратегии нападения y_i, L_i — стоимость ущерба ресурсу от атаки y_i (стратегии y_i), $K_{ij} \in [0,1)$ — вероятность преодоления механизма защиты, определяемого стратегией x_j при атаке y_i. При этом величина

$$Risk_i = p(y_i)L_i(1-K_{ij}) \tag{3}$$

– это риск, возникающий при применении атаки y_i, в случае использования стратегии защиты x_j. Величина

$$S_j = \frac{1}{\sum\limits_{i=1}^{n} p(y_i)L_i(1-K_{ij})} \tag{4}$$

характеризует суммарную защищённость ресурса в случае использования стратегии защиты x_j. Наконец, величина

$$S = \frac{1}{\sum\limits_{j=1}^{m}\sum\limits_{i=1}^{n} p(y_i)L_i(1-K_{ij})} \tag{5}$$

– это защищённость ресурса в случае использования всех имеющихся стратегий защиты и всех учитываемых типов хакерских атак.

Рассмотрим подробнее значения величин S_{ij} и S. Две крайности в их поведении следует отметить:

1) если $p(y_i) = 1$, т.е. достоверно используется стратегия атаки y_i и с ее помощью легко преодолевается механизм защиты x_j, т.е. $K_{ij} = 1$, то $S_{ij} = \infty$. Таким образом, незащищённость ресурса в данной ситуации характеризуется значением $S_{ij} = \infty$. Более того, если все используемые средства и стратегии защиты выбраны неверно или неправильно настроены, т.е. все $K_{ij} = 1$, то имеем ситуацию полной незащищённости компьютерной системы, характеризуемой значением, как видно из формулы (5), $S = \infty$;

2) если стратегия защиты x_j при достоверной атаке y_i не оставляет шанса на проникновение в компьютерную систему, т.е. при $p(y_i) = 1$ и $K_{ij} = 0$, то $S_{ij} = 1/L_i$.

Хотя мы охарактеризовали K_{ij} как вероятность преодоления стратегии защиты x_j при атаке y_i и, следовательно, она может находиться в ходе набора соответствующей статистики, при более тщательном анализе видно, что эта величина зависит и от опыта хакера. Очень опытный хакер легко преодолевает любую защитную систему, применяемую средним администратором безопасности, который не обладает таким азартом в предвкушении успеха, как хакер, и не готов сидеть «денно и нощно» на рабочем месте. Противодействовать

хакерским атакам можно за счёт сведения к минимуму возможных потерь, а для этого и создана теория игр, в том числе, и представляемое в данной статье программное приложение. Оно даёт среднему администратору безопасности инструмент противодействия хакерским атакам, с помощью которого минимизируются потери и даётся время для приобретения собственного антихакерского опыта.

Заметим, что можно организовать игры, учитывающие азартное поведение хакера [2,6,7]. Целесообразно создать соответствующее программное приложение.

6. Заключение

Программный продукт, описанный в статье, — это скорее проект защитного приложения, облегчающего администратору безопасности выбор как стратегии защиты, так и выбор программных продуктов, обеспечивающих защиту информации, размещённой в компьютерной системе.

Применение предложенного в данной работе программного продукта даёт администратору безопасности возможность выбрать наиболее оптимальный набор средств защиты компьютерной информации, а также оценить эффективность уже используемого программного обеспечения. В реализованном приложении есть возможность учёта вероятности хакерских атак, что в некоторых случаях может существенно повлиять на результаты расчётов посредством проведённой игры.

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.
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.
4. Вахний Т.В., Гуц А.К., Кузьмин С.Ю. Оптимальный подбор антивирусной программы и межсетевого экрана с помощью теории игр // Математические структуры и моделирование. 2014. № 4 (32). С. 240–246.
5. Вахний Т.В., Гуц А.К., Теория игр и защита компьютерных систем: Учебное пособие. Омск : Изд-во ОмГУ, 2013. 160 с.
6. Кемень Дж., Томсон Дж. Влияние психологического отношения на исходы игры / В кн.: Матричные игры / Под. ред. Н.Н. Воробьева. М. : ФМ, 1961. 280 с.
7. Вахний Т.В., Гуц А.К. Теоретико-игровое моделирование поведения азартного нарушителя при защите информационных ресурсов // Межвузовская научно-практическая конференция «Информационные технологии и автоматизация управления». Омск : ОмГТУ, 2009. С. 166–167.

THE ACCOUNTING OF PROBABILITIES OF HACKER ATTACKS IN GAME APPROACH TO SELECTION OF DEFENCE SOFTWARE FOR COMPUTER INFORMATION

T.V. Vahniy
Ph.D. (Phys.-Math.), Ass. Prof., e-mail: vahniytv@mail.ru
A.K. Guts
Dr.Sc.(Phys.-Math.), Professor, e-mail: guts@omsu.ru
S.S. Bondar'
student, e-mail: dx-5_razor@mail.ru

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

Abstract. The software application for the calculation of optimal strategy of computer information defense based on the game theory with account of probabilities of hacker attacks is described. Compatibility of all used in the game defence software is tested. Two approaches to determination of probabilities of hacker attacks are used. A comparison of the results with and without consideration of the found probabilities is performed. Keywords: Information security, game theory, hacker attacks, optimal strategy, software product.

Keywords: Information security, theory of games, hacker attacks, optimal strategy, software product.