Математические структуры и моделирование
2016. № 2(38). С. 103–115

УДК 519.83+004.056

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

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
Н.Ю. Новиков
студент, e-mail: novnicku@gmail.ru

Омский государственный университет им. Ф.М. Достоевского

Аннотация. В статье представлено программное приложение, позволяющее на основе теории игр находить по различным критериям оптимальный набор средств защиты компьютерной информации.

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

Введение

В настоящее время, по мере роста возможностей вычислительной техники и расширения сферы её применения, возрастает актуальность обеспечения безопасности компьютерных систем и защиты хранящейся в них информации. Развитие глобальной сети Интернет и сопутствующих технологий достигло такого высокого уровня, что деятельность любого предприятия в целом и каждого пользователя в отдельности уже невозможно представить без электронной почты, web-рекламы, общения в режиме «онлайн» и т. д. Однако тот, кто использует Интернет, подвержен риску быть атакованным злоумышленниками, и, как следствие, потерять доступную через сеть ценную информацию. Теперь наряду с локальными атаками существуют возможности для удалённого нанесения вреда компьютерной системе. Кроме того, нападению может подвергнуться не только отдельно взятый компьютер, но и сама информация, передающаяся по сетевым соединениям.

На рынке представлено огромное разнообразие средств защиты компьютерной информации, однако, с ростом уровня защищённости системы возникают и определённые неудобства в её использовании, ограничения и трудности для пользователей. Поэтому часто необходимо выбрать оптимальный вариант защиты, который бы не создавал больших трудностей в пользовании компьютерной системой и одновременно обеспечивал достойный уровень защиты информации.

Подчас создание такого оптимального решения безопасности является очень сложным, 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 [1–7].

В данной работе предлагается применить теоретико-игровой подход к выбору оптимальных вариантов защиты компьютерных систем. На основе описанного подхода было создано программное приложение, которое позволяет на основе теории игр рассчитать оптимальный набор средств защиты компьютерной информации по одному из четырёх реализованных в нём критериев.

1. Постановка задачи и игровой подход

Для поиска оптимального набора программных средств защиты компьютерной системы можно провести математическую игру двух сторон, одной из которых является система защиты компьютерной информации, а другой – возможные атаки хакеров. Нанесение хакером ущерба обычно является скорее следствием его действий, а 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 такой стратегии защиты, при которой возможные потери от атак будут минимальны, а цели атакующих хакеров были неважны, то можно считать, что хакер увлечён 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 $(i = 1, ..., n)$ некоторой матрицы (табл. 1), а в качестве стратегий администратора безопасности – её столбцы y_j $(j = 1, ..., m)$. К стратегиям хакера можно отнести различные атаки на компьютерную систему и их комбинации, а к стратегиям администратора – различные средства защиты компьютерной информации и их комбинации.

Для проведения на компьютере игры A надо также знать результаты игры при каждой паре стратегий x_i и y_j (например, a_{ij} – это материальный или финансовый ущерб, который может быть нанесён компьютерной системе при использовании злоумышленником своей i-ой, а администратором безопасности своей j-ой стратегии и общей стоимости средств защиты из j-ой стратегии администратора безопасности).

В качестве коэффициентов матрицы a_{ij} игры A можно рассматривать, например, годовые материальные или финансовые потери для всех вариантов комбинаций x_i и y_j. Для вычисления коэффициентов матрицы необходимо сопоставить все атаки из i-ой стратегии злоумышленника со средствами защиты из j-ой стратегии администратора и вычеркнуть те атаки, от которых защищает хотя бы одно средство защиты. Искомая величина — это сумма возможного ущерба от оставшихся атак из стратегии злоумышленника и стоимости используемых средств защиты.

Таблица 1. **Таблица матричной игры**

	y_1	y_2	...	y_m
x_1	a_{11}	a_{12}	...	a_{1m}
x_2	a_{21}	a_{22}	...	a_{2m}
...	...	...	...	...
x_n	a_{n1}	a_{n2}	...	a_{nm}

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, при которой будут минимальны средние потери, т.е. будет минимальна сумма $\sum\limits_{i=1}^{n} a_{ij}$.

Целью хакера в матричной игре является, естественно, получение по возможности большего выигрыша. Цель же администратора безопасности состоит в том, чтобы дать хакеру наименьший выигрыш. В простейшем случае, администратор будет выбирать такую стратегию, которая позволит ему минимизировать выигрыш хакера. Тогда значение игры будет равно элементу матрицы:

$$a_{i_0 j_0} = \min_j \max_i a_{ij}.$$

Для защиты компьютерной информации администратор может применить и другие критерии, помимо критерия минимакса, к подбору оптимального набора программных средств [3].

2. Критерии выбора оптимальной стратегии администратора

Администратор безопасности стремится выбрать такую стратегию, которая позволит ему свести к минимуму наносимый компьютерной системе ущерб от реализации тех или иных угроз. Поставим в соответствие каждой стратегии администратора j число $W_j(A)$, вычисляемое с помощью платёжной матрицы A. Критерий выбора оптимальной стратегии для администратора состоит в том, чтобы взять $W_{j0} = \min\limits_j W_j(A)$. Для нахождения числа $W_j(A)$ можно использовать различные критерии [3] к выбору оптимальной стратегии администратора [3].

1. Критерий крайнего пессимизма Вальда ориентирует игрока на самые неблагоприятные для него условия и, следовательно, на крайне осторожное, осмотрительное поведение при выборе стратегии. По этому критерию за оптимальную принимается стратегия, которая в наихудших условиях гарантирует максимальный выигрыш. Для администратора безопасности максимальным

выигрышем будет сведение к минимуму наносимого компьютерной системе ущерба от реализации тех или иных угроз. Следовательно, согласно критерию Вальда $W_j(A) = \max\limits_i a_{ij}$ и администратор выбирает такую стратегию, при которой наименьший выигрыш является наибольшим среди наименьших выигрышей всех стратегий. Т. е. по критерию Вальда оптимальной будет стратегия

$$W_{j0} = \min_j \max_i a_{ij}. \tag{1}$$

Этот критерий уместен в тех случаях, когда администратор не столько хочет выиграть (т. е. чтобы ущерб компьютерной системы был самым минимальным из возможных), сколько не хочет проиграть (т. е. чтобы ущерб компьютерной системы не был самым максимальным из возможных).

2. Критерий максимального математического ожидания Байеса предполагает, что администратору безопасности известны вероятности p_i, с которыми злоумышленник применяет свои стратегии. Полагают, что $W_j(A) = \sum\limits_{i=1}^{n} p_i a_{ij}$ и оптимальной является стратегия, при которой

$$W_{j0} = \min_j \sum_{i=1}^{n} p_i a_{ij}. \tag{2}$$

Вероятности реализации атак могут быть определены по результатам статистических исследований [5, 6]. Можно изучить статистику хакерских атак за определённый промежуток времени, например, по данным портала http://www.sicherheitstacho.eu/. Также полезно установить систему обнаружения хакерских атак (IDS), которая позволит самостоятельно набрать статистику, с помощью которой можно выявить наиболее распространённые типы атак и вычислить вероятности p_i хакерских стратегий.

3. Критерий недостаточного основания Лапласа можно использовать администратору безопасности при наличии неполной информации о вероятностях реализации хакерских атак или если вероятности всех стратегий злоумышленника равны. Если предположить, что все хакерские атаки равновероятны, т. е. $p_i = 1/n$, где n – количество стратегий хакера, то от критерия Байеса перейдём к критерию Лапласа. Согласно критерию Лапласа $W_j(A) = \frac{1}{n}\sum\limits_{i=1}^{n} a_{ij}$ и оптимальной является стратегия

$$W_{j0} = \frac{1}{n} \min_j \sum_{i=1}^{n} a_{ij}. \tag{3}$$

Использование данного критерия оправдано, если минимизация риска проигрыша представляется менее существенным фактором принятия решения, чем максимизация среднего выигрыша.

4. Критерий пессимизма-оптимизма Гурвица является промежуточным между критериями крайнего пессимизма и крайнего оптимизма. Согласно критерию Гурвица $W_j(A) = c\max\limits_i a_{ij} + (1-c)\min\limits_i a_{ij},\ c \in [0,1]$ — коэффициент

пессимизма. Крайнему пессимизму ($c = 1$) можно противопоставить крайний оптимизм ($c = 0$, критерий азартного игрока), когда ставка делается на самый большой возможный выигрыш, т. е. на самый маленький элемент платёжной матрицы (наименьший ущерб компьютерной системе). Оптимальной является стратегия администратора, при которой

$$W_{j0} = \min_j \{c \max_i a_{ij} + (1 - c) \min_i a_{ij}\}. \tag{4}$$

Коэффициент пессимизма $c \in [0, 1]$ выбирается из субъективных соображений администратора безопасности.

3. Стратегии хакера и администратора безопасности

В данной работе для участия в матричной игре были отобраны следующие, в настоящее время довольно популярные программные продукты, обеспечивающие защиту компьютерной информации:

1. СЗИ от НСД Secret Net 7.
2. Программно-аппаратный комплекс «Соболь».
3. UserGate Proxy & Firewall.
4. Security Studio Endpoint Protection.
5. McAfee LiveSafe Promo box.
6. Антивирус Касперского Internet Security 2014 Multi-Device Russian Edition.
7. Антивирус ESET NOD32 SMALL Business Pack newsale for 10 user (NOD32SBP-NS-BOX-1-10).
8. Антивирус Symantec Norton Antivirus 2013.
9. Программный межсетевой экран ИКС.
10. VIPNet Office Firewall.
11. Zecurion Zserver (Storage Security).
12. Iperius Backup Full 4.0.2.
13. Handy Backup Professional для бэкапа Lotus Notes Электронная лицензия/ключ.
14. DeviceLock Endpoint DLP Suite.

При составлении матрицы игры перечисленные выше программные продукты и их возможные сочетания были определены как стратегии администратора безопасности. На сайтах производителей можно ознакомиться с их возможностями и узнать, от каких угроз они защищают.

В качестве возможных стратегий хакеров в данной работе были выбраны всевозможные сочетания из следующих 27 угроз сохранности компьютерной информации: DoS, DDoS, TearDrop, Trin00, Smurf-атака, атака Fraggle, SYN-флуд, Win32, Melissa, MsBlast, Kraken, вирус, червь, троян, L0phtCrack, атака с подбором пароля, SATAN, IP-спуффинг, сниффинг пакетов, ShadowSecurityScan, NetBus, BackOrifice, удалённое проникновение, Maibombing, Brute force attack, атака «Man in the middle».

Получить различные стратегии игроков можно было путём простого перебора всех возможных атак для хакера и аналогичного перебора всех участвующих в игре программных средств защиты для администратора. Однако при таком подходе получалось более миллиона стратегий, что, естественно, сказалось бы на скорости работы программного приложения. Чтобы сократить количество стратегий игроков, атаки и средства защиты 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 путём перебора всех возможных комбинаций. Выбор оптимальной стратегии администратора безопасности осуществляется по одному из четырёх критериев, описанных выше.

Суммарные затраты получаются суммированием величины ущерба, который может быть нанесён при реализации текущей стратегии хакера, если система не была защищена от неё средствами защиты из текущей стратегии администратора безопасности, и общей стоимости всех средств защиты из текущей стратегии администратора безопасности.

Подсчёт 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. Сопоставив текущий набор 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 и суммировать величины ущерба тех угроз, что 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 вычисляются 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.

4. 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, позволяет рассчитать оптимальный набор средств защиты компьютерной системы по одному из четырёх реализованных в нём критериев. Справа на главной странице реализованного приложения располо-

жен список используемых продуктов, обеспечивающих безопасность компьютерной информации. При каждом элементе он имеет поле типа «checkbox», что позволяет использовать в расчётах не все предложенные продукты, а только часть из них. После выбора участвующих в матричной игре атак и средств защиты и нажатия на кнопку «Создать новую игру» приложение автоматически составляет стратегии злоумышленника и администратора, создаёт матрицу игры и выводит её на экран. Здесь появляется возможность выбрать критерий оптимальности стратегии администратора (см. рис. 1).

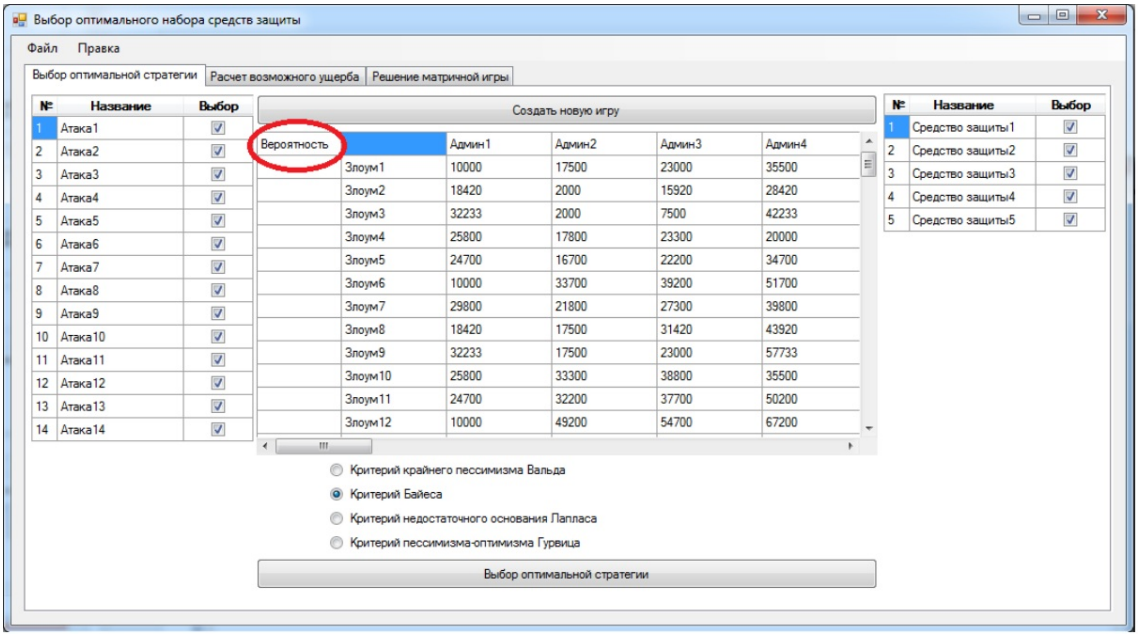

Рис. 1. Матрица игры при выборе критерия Байеса

При выборе администратором критерия Байеса слева от столбца с названиями стратегий злоумышленника появляется колонка «Вероятности» (см. рис. 1), в которую нужно ввести значения вероятностей применения соответствующих стратегий злоумышленника. Сумма значений в этой колонке должна быть равна 1, иначе приложение выдаст сообщение об ошибке и оптимальная стратегия рассчитана не будет. Незаполненные ячейки этого столбца приложение распознает как 0. Если администратор выбирает критерий Гурвица, то слева от названия критерия появляется текстовое поле, в которое нужно ввести коэффициент пессимизма от 0 до 1. При выборе критерия Вальда или Лапласа ввод дополнительных коэффициентов не требуется.

После заполнения колонки «Вероятности» или «Коэффициент пессимизма» и нажатия кнопки «Выбор оптимальной стратегии» приложение выполняет необходимые расчёты и выводит результат в таблицу, расположенную под этой кнопкой (см. рис. 2). В этой таблице содержится информация о найденной оптимальной стратегии администратора: название оптимальной стратегии, критерий по которому она выбиралась, суммарная стоимость всех средств защиты, входящих в эту стратегию, возможный ущерб и суммарные затраты (сумма сто-

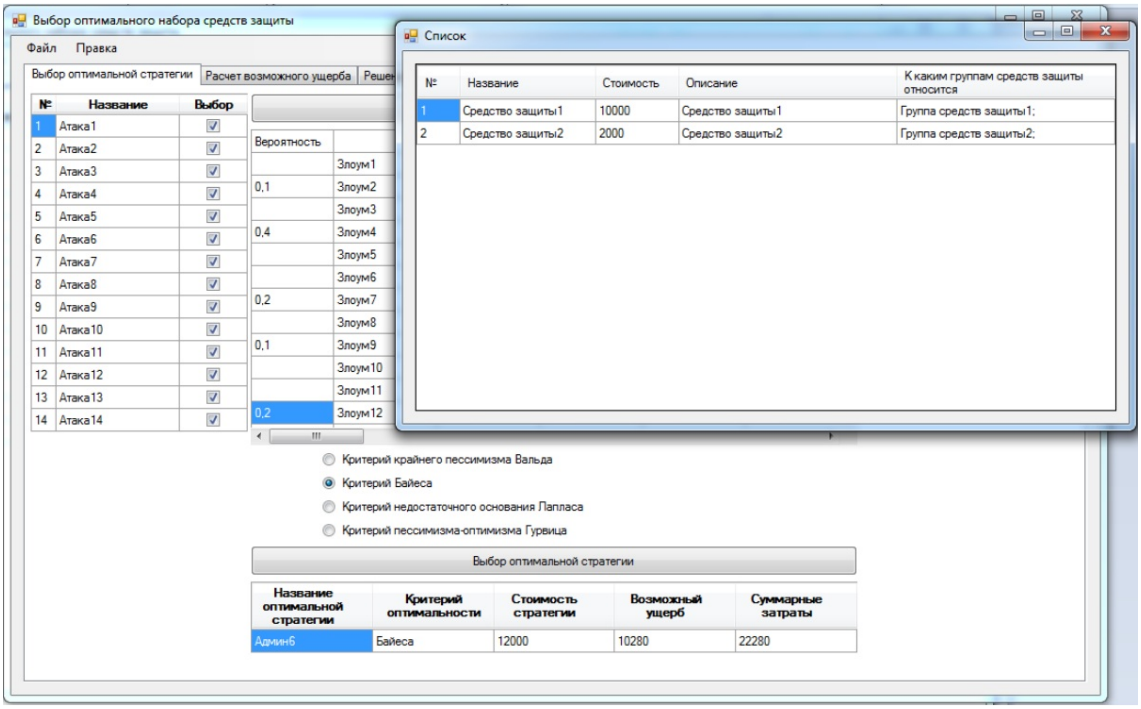

Рис. 2. Результат расчетов оптимальной стратегии администратора по критерию Байеса

имости средств защиты и возможного ущерба). Для просмотра более подробной информации о найденной стратегии администратор может дважды кликнуть по названию стратегии (в таблице результатов или в платёжной матрице игры). В новом окне появится список всех средств защиты, из которых состоит стратегия, и информация о них.

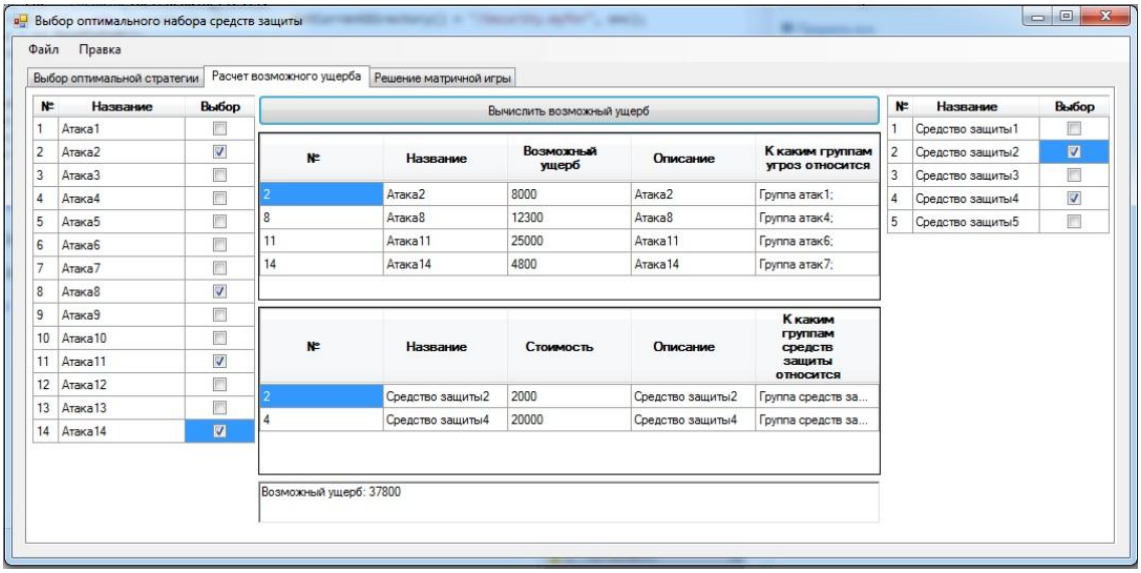

Рис. 3. Окно с результатом расчета возможного ущерба

Для расчёта возможного ущерба нужно открыть вкладку «Расчёт возможного ущерба». Слева на экране на экране будет отображён весь список атак, имеющийся в базе приложения, а справа – список средств защиты. Для удобства выбора конкретного набора средств защиты и атак все стоящие напротив них галочки сняты. Администратору нужно пометить нужные средства защиты и атаки, а затем нажать на кнопку «Вычислить возможный ущерб». После выполнения необходимых вычислений приложение выведет полученный результат на экран (см. рис. 3).

Для решения любой матричной игры по заданной платёжной матрице нужно открыть вкладку «Решение матричной игры». Администратор может заполнить платёжную матрицу вручную или загрузить её из файла. После заполнения матрицы и нажатия кнопки «Решить игру» приложение выполняет необходимые вычисления и выводит полученный результат на экран (см. рис. 4).

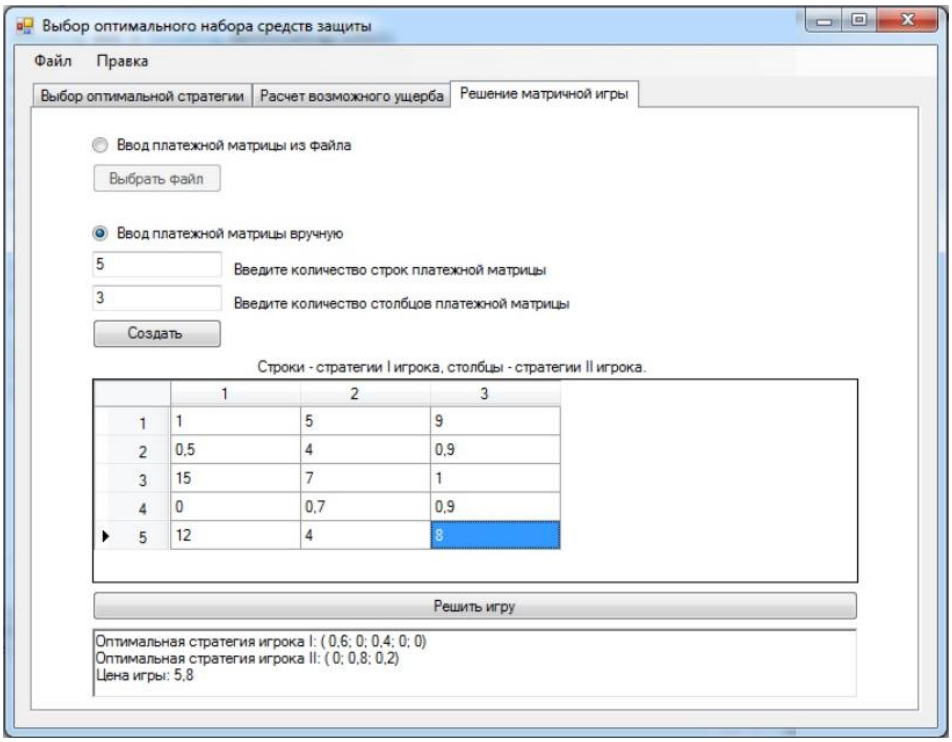

Рис. 4. Вкладка «Решение матричной игры»

Реализованное приложение позволяет изменять список атак и список средств защиты, имеющиеся в базах приложения. Для этого нужно выбрать в меню «Правка», а затем «Изменение списка атак» или «Изменение списка средств защиты». В результате откроется окно, в котором можно будет внести необходимые изменения. На рис. 5 и 6 показаны окна, в которых можно ввести изменения в список атак и в список средств защиты соответственно.

Администратор имеет возможность добавить новое средство защиты или атаку в список или удалить существующее, нажав соответствующую кнопку в появившемся окне приложения. При нажатии на кнопку «Добавить строку»

или «Изменить строку» открывается новое окно для ввода необходимой информации.

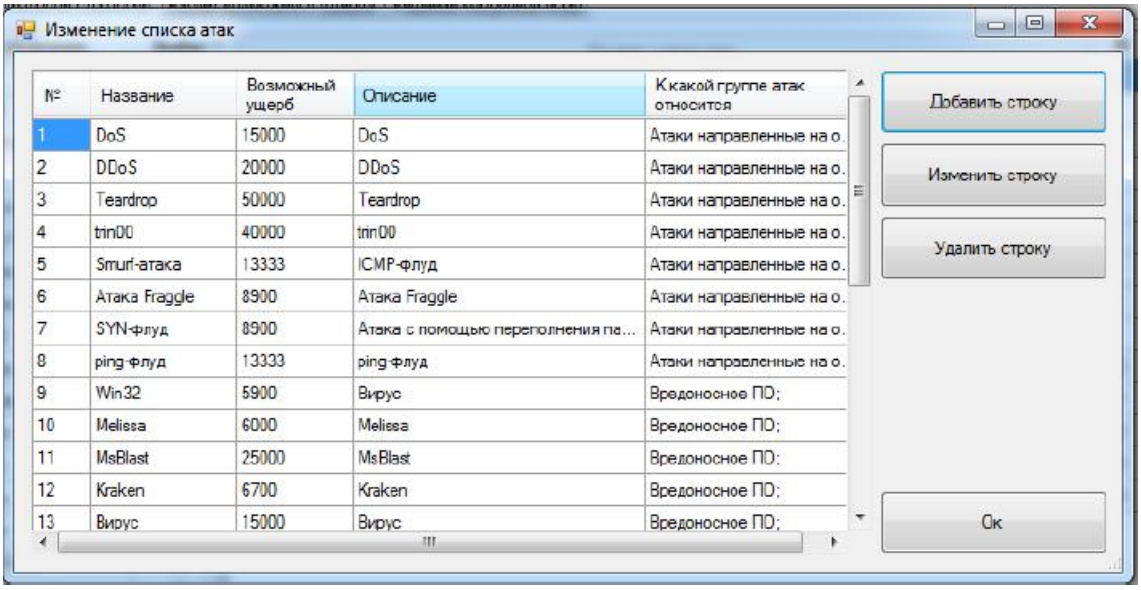

Рис. 5. Окно изменения списка атак

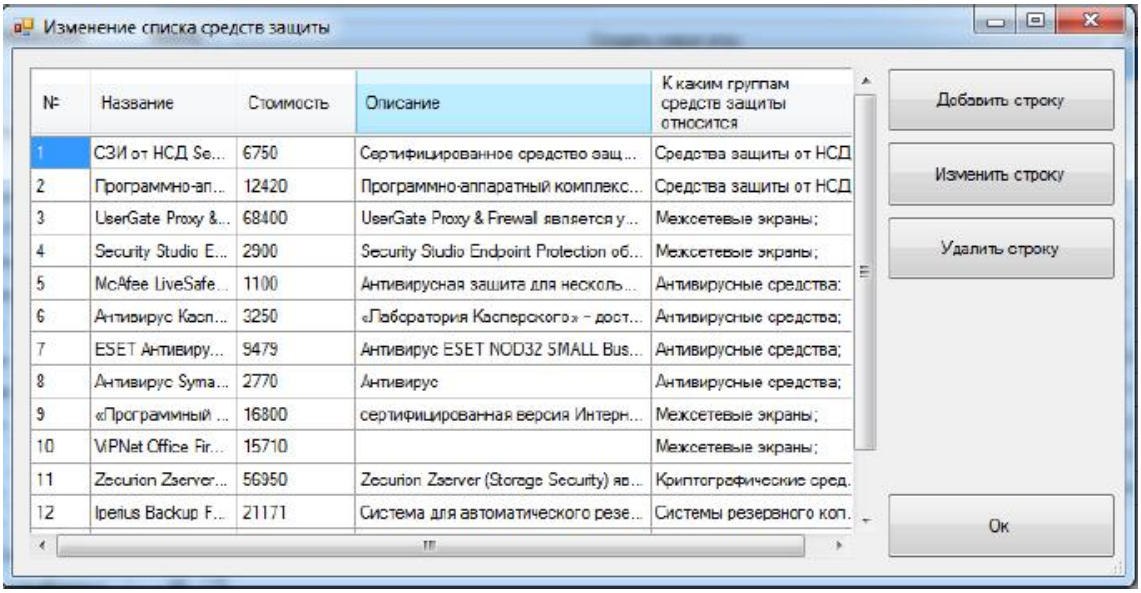

Рис. 6. Окно изменения списка средств защиты

На рис. 7 показаны результаты расчётов оптимальной стратегии администратора безопасности, выполненные при выборе описанных выше критериев. Видно, что оптимальной стратегией администратора по критериям Вальда и Лапласа оказался один и тот же набор программных средств: СЗИ от НСД Secret Net 7, McAfee LiveSafe Promo box и Security Studio Endpoint Protection.

А согласно критериям Байеса и Гурвица можно использовать меньшее количество программных продуктов для защиты компьютерной системы.

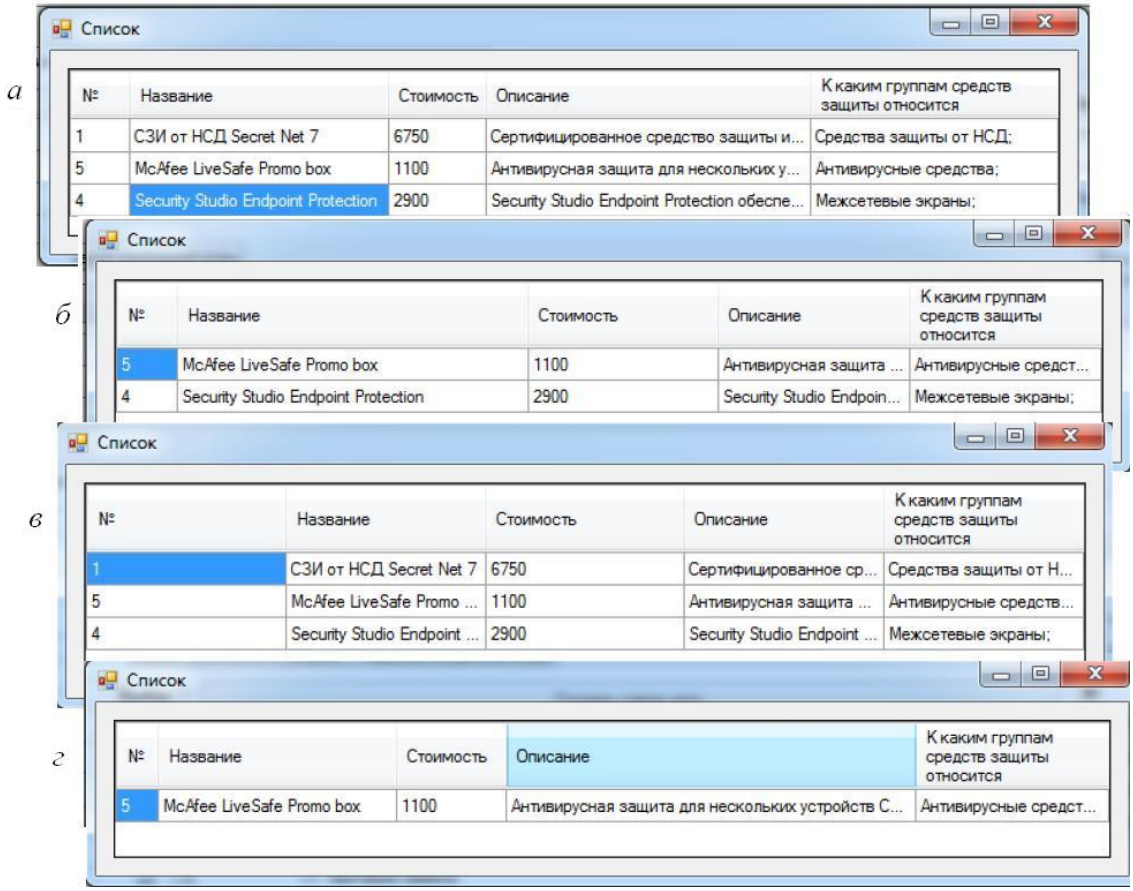

Рис. 7. Результаты расчётов оптимальной стратегии администратора по выбранному критерию: а – Вальда, б – Байеса, в – Лапласа, г – Гурвица

На рис. 8 показаны результаты расчёта оптимальной стратегии при ущербе 10 000 руб. и 100 000 руб. от реализации каждой атаки соответственно. При увеличении величины ущерба от реализации угроз оптимальная стратегия администратора содержит большее число средств защиты.

Приложение создавалось в среде разработки Microsoft VS 2013 с использованием языка программирования C#. Созданное приложение может успешно работать на любом современном компьютере с установленной операционной системой Windows и платформой .NET Framework 4.5 версии и выше. В данном приложении дополнительно реализована возможность шифрования файлов, содержащих списки атак, списки средств защиты и их классификации. Для того, чтобы воспользоваться этой возможностью, нужно включить режим защиты в меню «Файл».

а

Список

№	Название	Стоимость	Описание	К каким группам средств защиты относится
1	СЗИ от НСД Secret Net 7	6750	Сертифицированное средство защиты инфор...	Средства защиты от НСД;
5	McAfee LiveSafe Promo box	1100	Антивирусная защита для нескольких устройс...	Антивирусные средства;
4	Security Studio Endpoint Protection	2900	Security Studio Endpoint Protection обеспечива...	Межсетевые экраны;
14	DeviceLock Endpoint DLP Suite	3300	Программный комплекс DeviceLock Endpoint D...	Системы предотвращения ут...

б

Список

№	Название	Стоимость	Описание	К каким группам средств защиты относится
1	СЗИ от НСД Secret Net 7	6750	Сертифицированное средство защит...	Средства защиты от НСД;
5	McAfee LiveSafe Promo box	1100	Антивирусная защита для нескольки...	Антивирусные средства;
4	Security Studio Endpoint Protection	2900	Security Studio Endpoint Protection об...	Межсетевые экраны;
11	Zecurion Zserver (Storage Security)	56950	Zecurion Zserver (Storage Security) яв...	Криптографические средства ЗИ;
14	DeviceLock Endpoint DLP Suite	3300	Программный комплекс DeviceLock E...	Системы предотвращения утечек ко...

Рис. 8. Результаты расчётов оптимальной стратегии администратора при величине ущерба от каждой атаки 10 000 руб. (а) и 100 000 тыс. руб. (б)

5. Заключение

Применение разработанного на основе описанного игрового подхода программного продукта даст администратору безопасности возможность как оценить эффективность используемого программного обеспечения, так и выбрать оптимальный набор средств защиты компьютерной информации с учётом четырёх различных критериев оптимальности стратегии администратора. В реализованном приложении есть возможность удаления и добавления новых атак и средств защиты, что позволит в дальнейшем расширять и корректировать матрицу 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. Шевченко Д.В. Методы принятия управленческих решений: задания и методические указания для выполнения расчётно-графической работы. Казань : Познание, 2014. 69 с.
4. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: Учебное пособие. Омск : Изд-во ОмГУ, 2013. 160 с.
5. Вахний Т.В., Гуц А.К., Бондарь С.С. Учёт вероятностей хакерских атак в игровом подходе к подбору программных средств защиты компьютерной информации // Математические структуры и моделирование. 2015. № 3(35). С. 91–105.
6. 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.

7. 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.

MATRIX-GAME PROGRAM WITH SELECTION CRITERION FOR DETERMINATION OF OPTIMAL TOOL SET FOR COMPUTER SYSTEM PROTECTION

T.V. Vahniy
Ph.D. (Phys.-Math.), Associate Professor, e-mail: vahniytv@mail.ru
A.K. Guts
Dr.Sc. (Phys.-Math.), Professor, e-mail: guts@omsu.ru
N.Y. Novikov
Student, e-mail: novnicku@gmail.ru

Dostoevsky Omsk State University

Abstract. For finding the most optimal set of tools for computer information protection a software application is developed here based on game theory with various criteria.

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