Математические структуры и моделирование 2018. № 1(45). С. 148–158

УДК 519.83:004.056
DOI: 10.25513/2222-8772.2018.1.148-158

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОГО НАБОРА СРЕДСТВ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СИСТЕМЫ МЕТОДОМ МОНТЕ-КАРЛО

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
И.Ю. Пахотин
студент, e-mail: prakt1k@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В статье представлено программное приложение, позволяющее на основе теории игр находить наиболее оптимальный набор средств защиты компьютерной системы методом Монте-Карло.

Ключевые слова: защита информации, теория игр, хакерские атаки, оптимальная стратегия, программный продукт, метод Монте-Карло.

Введение

Использование теоретико-игрового подхода позволяет обеспечить оптимизацию выбора программных продуктов для защиты компьютерной системы [1–6]. Однако количество возможных стратегий хакера и возможных стратегий администратора безопасности экспоненциально увеличиваются с ростом возможных вариантов атак и средств защиты соответственно. Это приводит к тому, что увеличивается размер платёжной матрицы игры между администратором безопасности и хакером. Кроме того, если решать позиционную игру для всех возможных стратегий хакера и администратора безопасности, то это потребует больших затрат на вычислительные ресурсы, и к тому же на вычисление оптимальной стратегии администратора безопасности потребуется продолжительное время. Поэтому актуально нахождение решения указанной игры методами, которые менее затратны на вычислительные ресурсы.

В данной работе для нахождения наиболее оптимальных вариантов защиты компьютерной системы предлагается построить двухходовую позиционную игру администратора безопасности со злоумышленником и решить её методом имитационного моделирования. На основе описанного подхода было создано программное приложение, которое позволяет рассчитать оптимальный набор средств защиты компьютерной информации методом Монте-Карло.

1. Постановка задачи и игровой подход

Для поиска наиболее оптимального набора средств защиты компьютерной системы можно провести математическую игру двух сторон, одной из которых является система защиты компьютерной информации (I игрок – администратор), а с другой – возможные атаки хакеров (II игрок – злоумышленник). Один из подходов, моделирующий игру хакера и администратора безопасности, основан на теории позиционных игр [2].

Позиционная игра — это последовательная многоходовая игра, которая состоит в последовательном переходе из одного состояния (позиции) в другое состояние (позицию) путём выбора игроками одного из возможных действий в соответствии с правилами игры. Позиционные игры описываются с помощью дерева игры. На рис. 1 представлено дерево двухходовой позиционной игры. Каждая вершина дерева – это позиции игры, ход из одной позиции игры в другую позицию задаётся дугой. Начальной позиции игры соответствует корень дерева R, конечным позициям – листья, из них ходы игроками уже не совершаются. Каждому листу c_{ij} $(i = 1, ..., M;\ j = 1, ..., K)$ приписывается выигрыш.

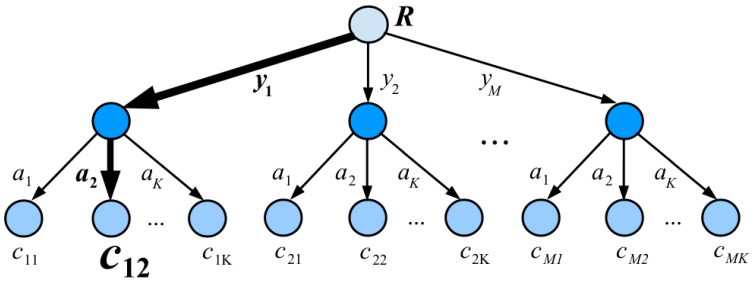

Рис. 1. Дерево двухходовой игры хакера и администратора безопасности

Пусть злоумышленник (игрок II) обладает K стратегиями атаки на компьютерную систему $a_1, a_2, ..., a_K$, каждая такая стратегия a_j $(j = 1, ..., K)$ – это j-я угроза, способная нарушить работу компьютерной системы. Каждому способу атаки a_j $(j = 1, ..., K)$ соответствует ущерб l_j, который терпит администратор в случае успешного осуществления этой j-ой атаки. Администратор безопасности (игрок I) пусть располагает S средствами защиты $d_1, d_2, ..., d_S$, каждое из которых обладает соответствующей ценой $g_1, g_2, ..., g_S$ и эффективностью защиты $e_i = (e_{i1}, e_{i2}, ..., e_{iK})$ $(i = 1, ..., S)$, где e_{ij} – эффективность i-го средства защиты по нейтрализации j-ой угрозы.

Стратегии администратора — это кортежи

$$y_i = (z_{i1}, z_{i2}, ..., z_{iS}),$$

где $z_{ij} = 1$, если задействован способ защиты d_j и $z_{ij} = 0$ – в противном случае.

Имея S средств защиты d_k $(k = 1, ..., S)$, администратор может составить $M = 2^S - 1$ стратегий y_i $(i = 1, ..., M)$, из которых мы исключили кортеж (0, 0, ..., 0), поскольку он представляет полное бездействие администратора.

Ходом администратора является выборка из способов обеспечения защиты информационной системы (разных наборов средств защиты), т. е. выбор стратегии y_i, а ходом злоумышленника — применение способа атаки a_j на компьютерную систему.

Составим платёжную матрицу C, элементами c_{ij} которой (табл. 1) являются потери администратора в том случае, когда он использовал стратегию y_i $(i = 1, ..., M)$, а хакер осуществил атаку a_j $(j = 1, ..., K)$. На дереве игры элементы платёжной матрицы представлены листьями (см. рис. 1).

Элементы платёжной матрицы вычисляются с помощью формулы:

$$c_{ij} = R(y_i, a_j) + G_i,$$

где

$G_i = \sum_{j=1}^{S} z_{ij} g_j$, – затраты администратора на использование средств защиты i-той стратегии y_i;

$R(y_i, a_j) = l_j \sum_{l=1}^{S} (1 - z_{il} e_{lj})$ — остаточный риск атаки a_j при использовании стратегии y_i, т. е. возможный ущерб помноженный на вероятность того, что используемые средства защиты окажутся неэффективны.

Путь от корня R к листу c_{ij} является *партией игры* с исходом игры $F(y_i, a_j) = c_{ij}$. На рис. 1 изображён пример партии, в которой администратор избрал стратегию y_1, а злоумышленник – атаку a_2 .

Процесс игры состоит в том, что администратор выбирает стратегию защиты y_i, злоумышленник выбирает способ атаки a_j, после чего вычисляется исход партии, заключающийся в том, что администратор терпит ущерб равный c_{ij}.

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.

Цель администратора – выбор такой стратегии, которая сводит потери от атак к минимуму, авторы на его стороне, и поэтому цели атакующих хакеров в расчёт не принимаются. В силу этого можно считать, что хакер увлечён желанием нанести как можно больший ущерб атакуемой компьютерной системе. При таком предположении выигрыш хакера будет равен проигрышу администратора безопасности c_{ij}.

Таблица 1. Платежная матрица игры

	a_1	a_2	...	a_K
y_1	c_{11}	c_{12}	...	c_{1K}
y_2	c_{21}	c_{22}	...	c_{2K}
...	...	...	...	...
y_M	c_{M1}	c_{M2}	...	c_{MK}

В качестве стратегий администратора безопасности будем понимать строки y_i $(i = 1, ..., M)$ платёжной матрицы, а в качестве стратегий хакера – её столбцы

a_j $(j = 1, ..., K)$ (табл. 1). Перед своим ходом игроки не знают о ходах друг друга. Для проведения на компьютере игры C надо также знать результаты игры при каждой паре стратегий y_i и a_j.

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 i-ой стратегии администратора число $W_i(C)$, вычисляемое с помощью платёжной матрицы C. Критерий выбора оптимальной стратегии для администратора состоит в том, чтобы взять $W = \min\limits_i W_i(C)$. Тогда оптимальной будет такая стратегия y_{i_0}, для которой $W_{i_0}(C) = W$.

Будем считать, что администратор не имеет никакой информации о том, какую стратегию (способы атаки) выберет злоумышленник, тогда вероятности атак можно считать одинаковыми и равными $1/K$. В таком случае можно воспользоваться критерием недостаточного основания Лапласа [5,7], для которого берём:

$$W_i(C) = \frac{1}{K}\sum_{j=1}^{K} c_{ij}. \tag{1}$$

Использование критерия недостаточного основания Лапласа оправдано, если минимизация риска проигрыша представляется менее существенным фактором принятия решения, чем максимизация среднего выигрыша. Администратор при необходимости может применить и другие критерии [5, 7] к подбору оптимального набора средств защиты.

2. Нахождение оптимальной стратегии администратора безопасности методом Монте-Карло

С увеличением числа S средств защиты растёт и количество $M = 2^S - 1$ вариантов возможных стратегий защиты компьютерной системы. В результате общее количество возможных партий игры администратора безопасности со злоумышленником можно вычислить по формуле:

$$A = KM = K(2^S - 1). \tag{2}$$

Например, если возьмём число возможных атак хакера $K = 10000$, число средств защиты администратора $S = 20$, то число возможных стратегий администратора $M = 1048575$ и количество возможных партий игры будет равно $A = 10485750000$.

Для нахождения оптимальной стратегии администратора нужно вычислить по формуле (1) все $W_i(C)$ для $i = 1, ..., M$. Для этого потребуется провести минимум A сложений, а в приведённом выше примере это более 10 миллиардов сложений. Данный способ расчёта требует больших затрат на вычислительные ресурсы и уже при данных здесь значениях K и S оптимальная стратегия администратора может вычисляться продолжительное время. Если ещё в несколько

раз увеличить значения K и S, то невозможно будет данным способом найти W за разумное время даже с использованием вычислительных машин.

Исходя из этого, актуально нахождение решения рассматриваемой игры методами, которые менее затратны на вычислительные ресурсы. При исследовании сложных систем, подверженных случайным воздействиям, можно использовать имитационное моделирование, которое представляет собой численный метод проведения на ЭВМ вычислительных экспериментов с математической моделью. Результаты поведения рассматриваемой системы, полученные при воспроизведении на имитационной модели, являются случайными реализациями. Для нахождения объективного и устойчивого решения требуется многократное нахождение различных решений с последующей статистической обработкой полученных данных. В настоящее время при имитационном моделировании случайных процессов очень широко используется метод статистических испытаний Монте-Карло [8].

Для приблизительного вычисления значений $W_i(C)$, определяемых в (1), можно для каждой стратегии администратора y_i $(i = 1, ..., M)$ провести по N_{y_i} симуляций (с выбранными случайным образом атаками), после чего для получившихся результатов расчёта убытков $(x_{y_i1}, x_{y_i2}, ..., x_{y_in}, ..., x_{y_iN_{y_i}})$ рассчитать их средние значения для каждой стратегии администратора:

$$\overline{x_{y_i}} = \frac{1}{N_{y_i}} \sum_{j=1}^{N_{y_i}} x_{y_ij}. \tag{3}$$

С ростом значения N_{y_i} математическое ожидание $\overline{x_{y_i}}$ будет стремиться к $W_i(C)$:

$$\mathbf{M}\overline{x_{y_i}} \to W_i(C) \quad \text{при} \quad N_{y_i} \to \infty.$$

Критерием выбора оптимальной стратегии администратора может служить выбор стратегии y_{i_0}, для которой

$$\overline{x_{y_{i_0}}} = \min_i \overline{x_{y_i}},$$

т. е. стратегии, для которой среднее значение результатов симуляций убытков (ущерба от атак и затрат на средства защиты) минимально.

Пусть $N = \sum\limits_{i=1}^{M} N_{y_i}$ – общее количество симуляций. Тогда общее количество операций сложения, которые нужно выполнить для расчёта $\overline{x_{y_i}}$ равно N_{y_i}, а общее количество операций сложения для приблизительного нахождения W равно N. Если $N < A$, т. е. меньше количества возможных исходов игры, то мы получаем выигрыш по времени.

3. Оптимизация симуляций

Если количество симуляций для всех стратегий администратора y_i установить одинаковым, т. е. все значения N_{y_i} $(i = 1, ..., M)$ равными, то данный способ будет неоптимальным.

Например, установив общее количество симуляций N, на шаге n гораздо лучше динамически принимать решение, для какой стратегии проводить очередную симуляцию. Нужно каким-то образом отдавать предпочтения тем стратегиям y_i, для которых значение $\overline{x_{y_i}}$ на шаге n меньше. В таком случае минимальные значения $\overline{x_{y_i}}$ будут быстрее сходиться к своему математическому ожиданию, и мы будем экономить на вычислениях. Мы укажем ниже более эффективный алгоритм выбора стратегий y_i.

4. Реализуемый алгоритм USB1

Для минимизации потерь администратора применим алгоритм UCB1 (Upper-Confidence-Bound) [9] к нашей задаче:

Пусть N – требуемое количество симуляций и $N > M$.

1. Шаг $n = 1$. Проведём M симуляций, по одной симуляции для каждой стратегии администратора y_i.

2. Шаг n, пока $n < N$.

На шаге n проводим симуляцию x_{y_i} для стратегии y_i, для которой минимальна величина

$$\overline{x_{y_i}} - b\sqrt{\frac{2\ln n}{n_{y_i}}}, \tag{4}$$

где $\overline{x_{y_i}}$ – средние убытки компьютерной системы при использовании администратором стратегии y_i (см. (3));

n_{y_i} – количество уже проведённых симуляций для стратегии y_i;

n – номер текущей симуляции;

b – константа, используемая для установки нужного баланса между шириной и глубиной поиска. Чем она больше, тем чаще будут рассматриваться варианты, для которых средние убытки компьютерной системы не являются минимальными на текущий момент.

На рис. 2 изображены графики радикала $\sqrt{\frac{2\ln n}{n_{y_i}}}$ при различных значениях n_{y_i}. Алгоритмический смысл данного радикала состоит в том, что без него на шаге n мы бы каждый раз просто выбирали стратегию с минимальным значением $\overline{x_{y_i}}$. Но так как этот радикал растёт у стратегий, для которых мы не проводим симуляций, то время от времени мы будем проводить симуляции у стратегий, не показывающих минимальный результат на данный момент. Это позволяет сгладить ситуации, когда нам не повезло и для «хороших» стратегий были проведены симуляции с «плохим» результатом.

5. Описание программного продукта и анализ результатов расчёта

В данной статье мы представляем программный продукт [10], который по введённым значениям стоимости средств защиты и ущерба от применения атак

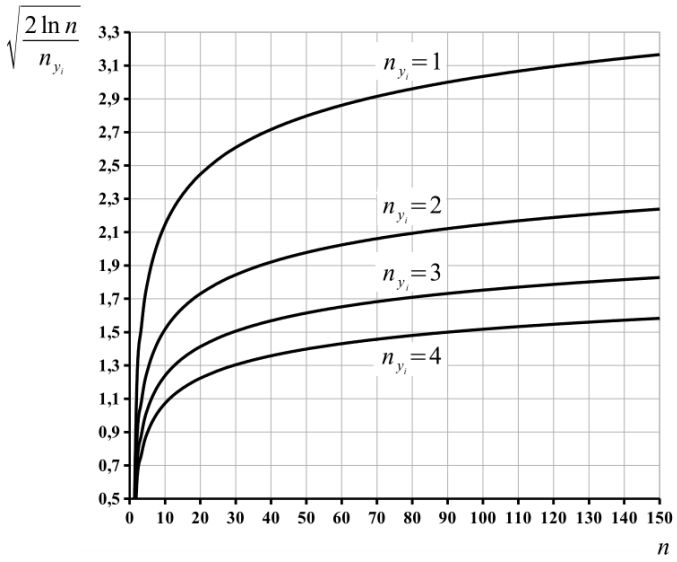

Рис. 2. Зависимость величины радикала от номера текущей симуляции n для различных значений количества проведенных симуляций i-ой стратегии администратора

позволяет рассчитать оптимальный набор средств защиты компьютерной системы методом Монте-Карло с использованием алгоритма UCB1.

Приложение создавалось в среде разработки IntelliJ IDEA с использованием языка программирования Java. В качестве Фреймворка для автоматической сборки был использован Maven, для разработки графического интерфейса на Java использована библиотека Swing.

На рис. 3 показано главное окно программного приложения, предоставляющее доступ к другим окнам.

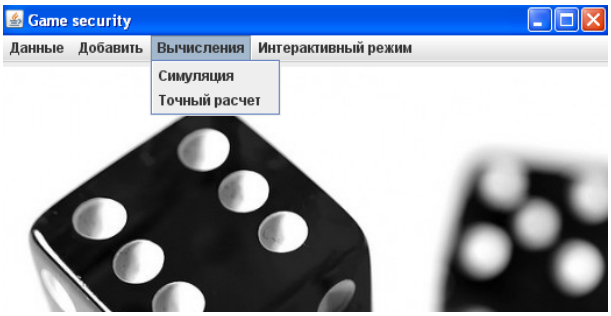

Рис. 3. Интерфейс меню программного приложения

Созданное программное приложение на основе набора введённых средств защиты $(d_1, d_2, ..., d_S)$ генерирует список из всех возможных стратегий администратора y_i $(i = 1, ..., M)$. Пользователь имеет возможность добавлять новые способы атаки на компьютерную систему и новые средства защиты. В программном приложении можно получить как точное решение задачи, так и решение методом Монте-Карло. Общее количество симуляций является суммой

значения поля «Количество симуляций» (см. рис. 4) и количества стратегий администратора.

После проведения необходимых расчётов программное приложение сортирует стратегии администратора в порядке увеличения средних значений затрат на средства защиты и ущерба от атак.

При выборе вида вычисления «Симуляция» (см. рис. 3) программным приложением производятся расчёты для нахождения значений $\overline{x_{y_i}}$, которые с увеличением количества симуляций приближаются к значениям математического ожидания убытков администратора при выборе соответствующих стратегий. Оптимизация симуляций производилась введением коэффициента смены стратегий (КСС), который является значением b из формулы (4). Этот коэффициент отвечает за то, насколько часто алгоритм будет проводить симуляции для стратегий, у которых на текущий момент убытки не принимают минимального значения [9].

На рис. 4 показаны результаты работы программного приложения при количестве симуляций 50000 и $KCC = 5000$. В таблицу с лучшим результатом выводится три стратегии с наименьшими средними убытками и с наибольшим количеством симуляций (N_{y_i}).

Программное приложение было запущено на случайно сгенерированных данных с абстрактными способами атаки и методами защиты (см. рис. 5). На данных малого размера расчёт оптимальных стратегий администратора по методу Монте-Карло существенно проигрывает точному расчёту. Но интерес представляют ситуации, когда количество методов защиты и способов атаки являются большими числами, причём количество способов атак много больше возможных стратегий администратора. На таких данных алгоритм может иметь большое преимущество перед точным расчётом.

Было произведено моделирование на основе случайных данных, когда количество методов защиты равно 7, а способов атак 10 000. Программное приложение было запущено по несколько раз на количестве симуляций 100, 500, 1000, 5000 и 50 000. При малом числе симуляций полученный методом Монте-Карло результат отличался от точных расчётов. На 5000 симуляциях почти во всех случаях программное приложение точно находило одну из двух лучших стратегии, и она была на первом месте в таблице «Лучший результат». На 50000 симуляциях программное приложение всегда точно определяло две лучшие стратегии в правильном порядке (см. рис. 4 и рис. 6).

На 50000 симуляций потребовалось провести $50000 + 2^7 = 50127$, а не $10000(2^7 - 1) = 1270000$ сложений чисел, что составляет 0,04 от исходного количества. Таким образом, удалось добиться существенного выигрыша по времени вычисления оптимального набора средств защиты компьютерной информации.

В рамках данной работы критерием выбора оптимальной стратегии администратора безопасности был использован критерий недостаточного основания Лапласа, предполагающий, что все атаки равновероятны. В случае, когда атаки неравновероятны и администратору известны их вероятности, можно использовать критерий Байеса [5–7].

Более подробно программный продукт описан в [10].

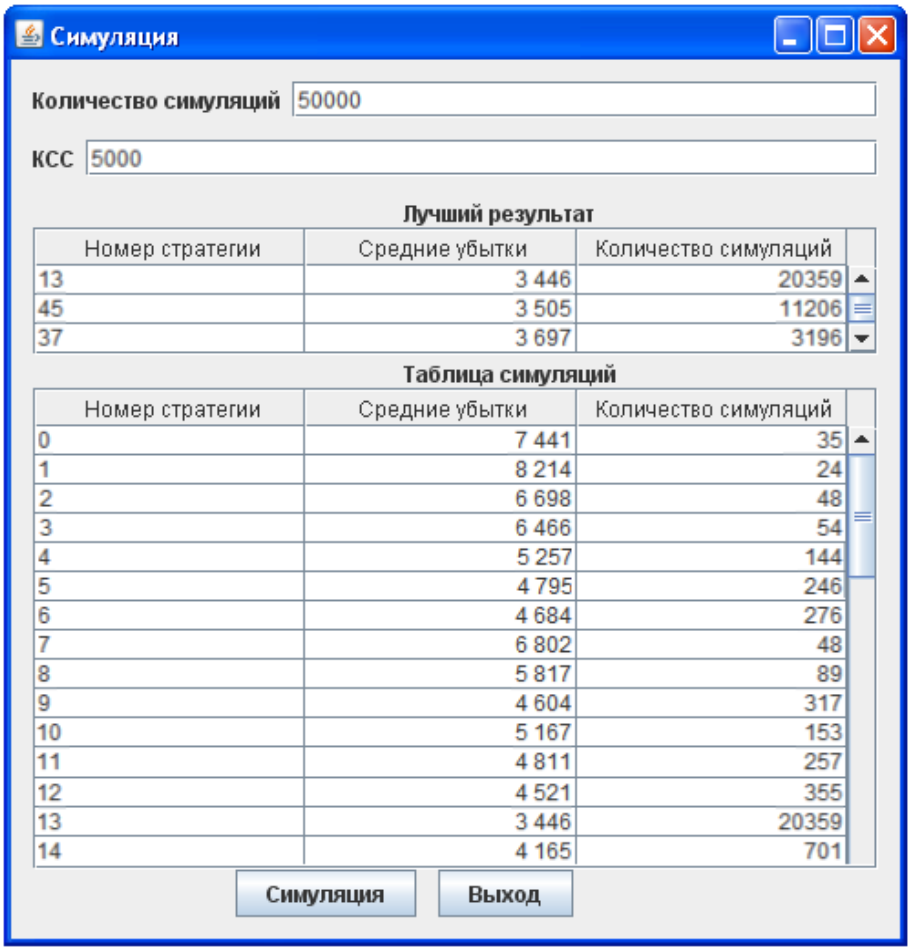

Рис. 4. Результат нахождения оптимальных стратегий администратора методом Монте-Карло при количестве симуляций 50 000

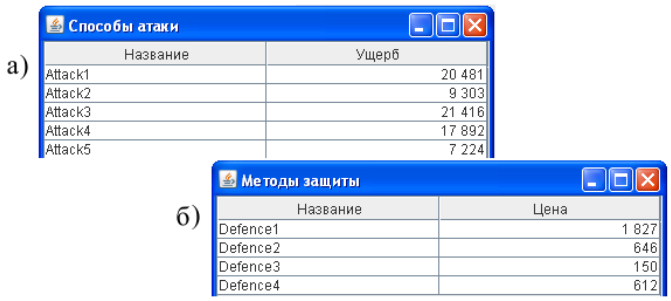

Рис. 5. Добавление в игру абстрактных способов атаки (а) и методов защиты (б)

6. Заключение

Разработанное программное приложение находит оптимальный набор средств защиты компьютерной системы, решая двухходовую позиционную игру администратора безопасности со злоумышленником методом статистических испытаний Монте-Карло. Сравнение полученных результатов с точными расчё-

№	Номер стратегии	Средние убытки
1	13	3 437
2	45	3 459
3	43	3 741
4	37	3 774
5	41	4 259
6	14	4 325
7	11	4 454
8	5	4 521
9	29	4 563
10	12	4 588
11	6	4 623
12	44	4 628
13	38	4 649
14	77	4 662
15	46	4 765

Рис. 6. Результаты точных расчётов убытков (ущерба от атак и затрат на средства защиты) для разных стратегий администратора

тами показало, что при огромном количестве возможных атак хакеров и выборе оптимальной стратегии администратора из большого количества средств защиты данный подход позволяет добиться существенного выигрыша по времени нахождения решения.

Литература

1. Матричные игры / Под. ред. Н.Н. Воробьёва. М. : ФМ, 1961. 280 с.
2. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие. Омск : Изд-во ОмГУ, 2013. 160 с.
3. 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.
4. 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.
5. Вахний Т.В., Гуц А.К., Новиков Н.Ю. Матрично-игровая программа с выбором критерия для определения оптимального набора средств защиты компьютерной системы // Математические структуры и моделирование. 2016. № 2(38). С. 103–115.
6. 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.
7. Шевченко Д.В. Методы принятия управленческих решений: задания и методические указания для выполнения расчётно-графической работы. Казань : Познание, 2014. 69 с.
8. Ермаков С.М., Михайлов Г.А. Статистическое моделирование. М. : Физматлит, 1982. 296 с.

9. Finite-time Analysis of the Multiarmed Bandit Problem. URL: `https://homes.di.unimi.it/~cesabian/Pubblicazioni/ml-02.pdf` (дата обращения: 07.01.2017).
10. Пахотин Ю.И. Применение стохастических методов к защите информации: выпускная квалификационная работа. Омск: ОмГУ, 2017. 51 с.

DETERMINING THE OPTIMAL SET OF TOOLS FOR COMPUTER SYSTEM SECURITY BY MONTE-CARLO METHOD

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
I.Yu. Pahotin
Student, e-mail: prakt1k@mail.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The article presents a software application that allows based on game theory to find the most optimal set of tools for computer information protection by Monte-Carlo method.

Keywords: information security, theory of games, hacker attacks, optimal strategy, software product, Monte-Carlo method.

Дата поступления в редакцию: 10.02.2018