Математические структуры и моделирование 2022. № 1 (61). С. 105–114

УДК 519.83:004.056
DOI 10.24147/2222-8772.2022.1 .105-114

ИТЕРАТИВНОЕ РЕШЕНИЕ БИМАТРИЧНОЙ ИГРЫ ДЛЯ ОПТИМИЗАЦИИ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СИСТЕМЫ

Т.В. Вахний
к.ф.-м.н., доцент, e-mail: vahniytv@mail.ru
С.В. Вахний
студент, e-mail: vakhniysv@mail.ru

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

Аннотация. В статье для решения биматричной игры между злоумышленником и администратором безопасности при огромных размерах платёжных матриц игроков предлагается использовать менее затратный на вычислительные ресурсы приближённый итеративный метод, алгоритм которого построен на основе метода Брауна–Робинсона.

Ключевые слова: информационная безопасность, компьютерная система, биматричные игры, итеративные методы, оптимальная стратегия, программный продукт.

Введение

При построении систем защиты информации можно применять теоретико-игровые методы, позволяющие анализировать взаимодействие между администратором безопасности системы и злоумышленниками [1–3]. Целью администратора безопасности является выбор такой стратегии защиты, которая будет сводить потери от атак к минимуму, а цели атакующих хакеров часто в расчёт не принимаются. В силу этого предполагается, что злоумышленник увлечён желанием нанести как можно больший ущерб атакуемой компьютерной системе, тогда его выигрыш можно приравнять проигрышу администратора безопасности. В результате цели игроков полагают прямо противоположными и для анализа их взаимодействия достаточно составить одну общую платёжную матрицу и найти решение матричной игры [1–4].

Нанесение хакером ущерба обычно является скорее следствием его действий, а не самой целью. В биматричных играх предполагается, что игроки (администратор безопасности и злоумышленник) имеют разные интересы и для каждого из них составляется своя платёжная матрица [1]. Нахождение решений (наиболее оптимальных стратегий игроков) матричных и биматричных игр с платёжными матрицами небольших размеров не занимает много времени. Однако постоянно увеличивающееся количество способов атак и средств защиты приводит к тому, что экспоненциально растёт количество возможных стратегий хакеров и стратегий администратора безопасности (т. е. различных соче-

таний программных средств) соответственно. В результате решение подобных матричных и биматричных игр с платёжными матрицами огромных размеров представляет собой трудоёмкий и громоздкий процесс, требующий достаточно продолжительного времени [2]. Поэтому становятся всё более актуальными разработка и применение методов их приближённого решения, которые менее затратны на вычислительные ресурсы [2, 3].

В данной работе для нахождения наиболее оптимальных вариантов защиты компьютерной системы предлагается построить биматричную игру администратора безопасности со злоумышленником и решить её приближённым итеративным методом, алгоритм которого построен на основе метода Брауна–Робинсона [4].

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 безопасности), а с другой – возможные атаки хакеров (II игрок – злоумышленник). Один из подходов, моделирующий игру хакера и администратора безопасности, основан на проведении биматричной игры, в которой интересы игроков не совпадают и не являются противоположными.

Биматричная игра – это конечная игра двух игроков с ненулевой суммой, в которой выигрыши каждого игрока задаются платёжными матрицами отдельно для каждого игрока. В каждой из них строки соответствуют стратегиям одного игрока (программное средство или набор из программных средств), а столбцы – стратегиям другого игрока, а на их пересечении в первой платёжной матрице стоит цена игры для администратора, а во второй платёжной матрице – цена игры для злоумышленника.

Если администратор для обеспечения безопасности системы может выбирать из S средств защиты, и при этом их можно использовать одновременно, то у него будет $N = 2^S - 1$ вариантов стратегий. Аналогично, если злоумышленник имеет L способов атаки, то у него будет $M = 2^L - 1$ вариантов вредоносных стратегий.

Таблица 1. **Платёжная матрица** A

	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}

Таблица 2. **Платёжная матрица** B

	y_1	y_2	...	y_M
x_1	b_{11}	b_{12}	...	b_{1M}
x_2	b_{21}	b_{22}	...	b_{2M}
...	...	...	...	...
x_N	b_{N1}	b_{N2}	...	b_{NM}

Ходом администратора безопасности является использование одной из N стратегий защиты компьютерной системы x_i $(i = 1, 2, ..., N)$, а ходом злоумыш-

ленника – применение одной из M стратегий атаки y_j $(i = 1, 2, ..., M)$ на компьютерную систему. Последовательно перебирая все стратегии игроков, можно заполнить две таблицы, в одной из них указывая ущерб администратора a_{ij} (см. табл. 1), а во второй – прибыль b_{ij} злоумышленника (см. табл. 2) соответственно при выборе стратегии защиты x_i $(i = 1, 2, ..., N)$ и способа атаки y_j $(i = 1, 2, ..., M)$. Из таблиц 1 и 2 можно выписать платёжные матрицы A и B, содержащие N строк и M столбцов с элементами a_{ij} и b_{ij}, соответственно:

$$A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1M} \\ a_{21} & a_{22} & ... & a_{2M} \\ ... & ... & ... & ... \\ a_{N1} & a_{N2} & ... & a_{NM} \end{pmatrix}; \quad B = \begin{pmatrix} b_{11} & b_{12} & ... & b_{1M} \\ b_{21} & b_{22} & ... & b_{2M} \\ ... & ... & ... & ... \\ b_{N1} & b_{N2} & ... & b_{NM} \end{pmatrix}.$$

Здесь элементы a_{ij} платёжной матрицы администратора безопасности A вычисляются следующим образом:

$$a_{ij} = R(x_i, y_j) + G_i,$$

где G_i – затраты администратора безопасности на приобретение и использование средств защиты, необходимых для реализации i-й стратегии x_i, $R(x_i, y_j)$ – величина ущерба от атаки y_j при использовании стратегии защиты x_i.

Аналогично элементы b_{ij} платёжной матрицы злоумышленника B вычисляются по формуле:

$$b_{ij} = P(x_i, y_j) - F_j,$$

где F_j – затраты злоумышленника на использование атаки y_j, $P(x_i, y_j)$ – величина прибыли от атаки y_j при использовании администратором стратегии защиты x_i.

Биматричная игра является одноходовой. Процесс игры состоит в том, что администратор выбирает стратегию защиты x_i, злоумышленник выбирает стратегию атаки y_j, после чего вычисляется исход игры, заключающийся в том, что администратор терпит ущерб, равный a_{ij}, а злоумышленник получает прибыль b_{ij}. Цель администратора безопасности – выбор такой стратегии, т. е. набора программных средств защиты, который сводит потери от атак и затраты на покупку средств защиты к минимуму, а цель атакующего – выбор такой стратегии, которая даст ему наибольший выигрыш.

2. Критерии выбора оптимальных стратегий игроков

Осмотрительное поведение администратора безопасности заключается в том, чтобы минимизировать свой возможный максимальный ущерб. Поэтому его оптимальную стратегию в простейшем случае можно найти из условия минимакса [1]. Поставим в соответствие каждой i-й стратегии администратора число $W_i(A)$, вычисляемое с помощью его платёжной матрицы A. Критерий выбора оптимальной стратегии x_{i0} для администратора состоит в том, чтобы взять

$$W_{i_0}(A) = \min_i \max_j a_{ij}. \tag{1}$$

Если злоумышленник ориентируется на самые неблагоприятные условия, то он стремится максимизировать свой возможный минимальный выигрыш. Поэтому его оптимальную стратегию в простейшем случае можно найти из условия максимина [1]. Поставим в соответствие каждой j-й стратегии злоумышленника число $W_j(B)$, вычисляемое с помощью его платёжной матрицы B. Критерий выбора оптимальной стратегии y_{j0} для злоумышленника состоит в том, чтобы взять

$$W_{j_0}(A) = \max_j \min_i b_{ij}. \tag{2}$$

Минимаксные стратегии игроков уместны в тех случаях, когда они не столько хотят выиграть, сколько не хотят проиграть. Хотя администратор и злоумышленник могут выбрать для себя и другие критерии для подбора наиболее оптимальных для них наборов программных средств [5].

Решение биматричной игры сводится к отысканию ситуаций равновесия и равновесных (оптимальных) стратегий игроков. Выбор одним из игроков неоптимальной для него стратегии приведёт к ухудшению его результатов игры и улучшению их у противника.

3. Сложности нахождения точного решения биматричной игры

С увеличением участвующих в игре средств защиты S и атак L, растёт общее количество стратегий игроков N и M, размер их платёжных матриц, а также число возможных партий игры $C = NM = (2^S - 1)(2^L - 1)$. Например, если число возможных стратегий злоумышленника $M = 1000$, число выбираемых средств защиты $S = 25$, то число возможных стратегий администратора будет $N = 33554431$, а количество возможных партий игры $C = 33554431000$! Тогда для нахождения оптимальной стратегии администратора безопасности нужно провести минимум $2C$ сложений, а в приведённом примере это более 67 миллиардов. В результате данный способ расчёта требует больших затрат на вычислительные ресурсы, и уже при заданных здесь относительно небольших значениях M и S оптимальная стратегия администратора может вычисляться продолжительное время. Если ещё в несколько раз увеличить значения M и S, то невозможно будет данным способом найти точное решение биматричной игры за разумное время даже с использованием вычислительных машин.

Исходя из этого, актуально нахождение решения рассматриваемой игры методами, которые будут менее затратны на вычислительные ресурсы, например приближённым итеративным методом.

4. Описание алгоритма приближённого решения биматричной игры итеративным методом

В данной работе для нахождения приближённого решения биматричной игры итеративным методом предлагается многократно фиктивно разыгрывать игру с платёжными матрицами двух игроков (администратора безопасности и злоумышленника). При этом платёжные матрицы A и B составляют только из чистых стратегий игроков. У администратора безопасности каждая чистая стратегия состоит только из одного программного средства, а у злоумышленника – из одного способа атаки. Таким образом, в данном методе платёжные матрицы A и B будут иметь гораздо меньший размер $S \times L$.

В первой партии (при одном повторении игры) оба игрока могут использовать любые известные критерии [5] для нахождения своих чистых стратегий, а в k-й партии каждый игрок выбирает ту чистую стратегию, которая максимизирует его ожидаемый выигрыш или минимизирует проигрыш против наблюдаемого эмпирического вероятностного распределения противника за все его предыдущие $(k-1)$ партий. При итерационном решении биматричной игры свои оптимальные чистые стратегии злоумышленник выбирает по своей платёжной матрице B, после чего его ходы соответствующим образом переносятся на платёжную матрицу администратора A. Данный метод позволяет находить приближённое решение биматричной игры и из чистых стратегий выстраивает оптимальные смешанные стратегии обоих игроков. При этом наиболее оптимальная стратегия администратора безопасности будет выстраиваться с учётом не только собственной выгоды, но и интересов злоумышленника.

Алгоритм итеративного решения биматричной игры:

• Шаг $k = 0$. Игроки используют начальные чистые стратегии x_{i_0} и y_{j_0}, которые определяются из условий (1) и (2).

• Шаг $k = 1$. Выбор чистых стратегий x_{i_1} и y_{j_1} осуществляется исходя из накопленного выигрыша на предыдущей итерации:

$$x_{i_1} : \min_i b_{ij_0} = \underline{v^1}; \qquad y_{j_1} : \max_j a_{i_0 j} = \overline{v^1}.$$

• Шаг $k+1$. Выбор чистых стратегий $x_{i_{k+1}}$ и $y_{j_{k+1}}$ осуществляется исходя из накопленного выигрыша на предыдущих итерациях:

$$x_{i_{k+1}} : \min_i \sum_j b_{ij_k} \eta_j^k / k = \underline{v^k}; \qquad y_{j_{k+1}} : \max_j \sum_i a_{ij_k} \xi_i^k / k = \overline{v^k},$$

где ξ_i^k и η_j^k – количество выборов чистых стратегий x_i и y_j за k шагов.

Цены игры администратора безопасности и злоумышленника будут равны $\frac{\overline{v^{k+1}}}{k+1}$ и $\frac{\underline{v^{k+1}}}{k+1}$ соответственно. Итеративный процесс следует продолжать до тех пор, пока за некоторое количество последних партий не будет повторяться чистая стратегия администратора безопасности при достижении некоторой предварительно задаваемой точности результатов значений игры.

Смешанные стратегии игроков выстраивают из чистых стратегий, которые участвовали в описанном алгоритме.

Чем больше будет сыграно партий игроками, тем ближе к точному значению приближается решение биматричной игры. Однако для оптимизации компьютерной безопасности наибольший интерес представляет не цена игры при оптимальной стратегии администратора, т. е. не конкретная величина наименьшего ущерба от атак при наименьших затратах на средства защиты, а именно сама оптимальная смешанная стратегия администратора безопасности, т. е. набор программных средств, при котором эта минимальная цена игры достигается.

5. Применение описанного алгоритма

Рассмотрим применение описанного алгоритма для решения задачи с платёжными матрицами небольшой размерности. Пусть у злоумышленника есть возможность купить и использовать две чистые стратегии y_1, y_2, а администратор может выбирать из трёх чистых стратегий x_1, x_2 и x_3. В случае успешной реализации стратегия y_1 может принести злоумышленнику прибыль 100 у.е. (условных единиц), а стратегия y_2 – 110 у.е., для их приобретения нужно заплатить 2 у.е. и 1 у.е. соответственно. При этом бесплатная чистая стратегия администратора x_1 защищает от атак y_1 и y_2 на 90 %, чистая стратегия x_2 стоит 5 у.е. и защищает от атаки y_1 на 80 %, чистая стратегия x_3 стоит 1 у.е., защищает от атаки y_1 на 85 % и от атаки y_2 на 99 %. Требуется определить, какие программные средства из x_1, x_2, x_3 нужно выбрать администратору для наиболее эффективной защиты компьютерной системы при наименьших затратах на их приобретение, а также какая стратегия злоумышленника будет для него наиболее оптимальной.

Проведём биматричную игру администратора со злоумышленником, найдём её точное решение и сравним его с приближённым решением, полученным описанным в данной работе итеративным методом.

Сначала для игроков нужно составить две платёжные матрицы A и B. У злоумышленника будут возможны 3 стратегии: y_1, y_2 и стратегия y_3, заключающаяся в использовании программных средств для проведения одновременно обеих атак y_1 и y_2. В свою очередь у администратора будет возможность выбирать из 7 стратегий: x_1, x_2, x_3, $x_4 = x_1 + x_2$, $x_5 = x_1 + x_3$, $x_6 = x_2 + x_3$, $x_7 = x_1 + x_2 + x_3$.

Последовательно перебирая все стратегии игроков, заполним две таблицы, в одной из них указывая ущерб администратора a_{ij} (см. табл. 3), а во второй – прибыль b_{ij} злоумышленника (см. табл. 4), соответственно, при выборе стратегии защиты $x_i (i = 1, \ldots, 7)$ и способа атаки $y_j (j = 1, \ldots, 3)$.

Для нахождения точного решения биматричной игры воспользуемся минимаксными критериями (1) и (2). Тогда из платёжной матрицы A для администратора: $W_{i0}(A) = \min\{21,\ 135,\ 17.1,\ 26,\ 12.1,\ 22.1,\ 17.1\} = 12.1$, откуда следует, что его оптимальной i_0-й стратегией будет x_5, которая заключается в использовании программных средств x_1 и x_3. Из платёжной матрицы B для злоумышленника: $W_{j0}(B) = \max\{8,\ 0.1,\ 8.1\} = 8.1$, откуда следует, что его оптимальной j_0-й стратегией будет y_3, которая заключается в использовании обеих атак y_1 и y_2.

Таблица 3. **Платёжная матрица** A

	y_1	y_2	y_3
x_1	10	1	**21**
x_2	25	115	**135**
x_3	16	2.1	**17.1**
x_4	15	16	**26**
x_5	11	2.1	**12.1**
x_6	21	7.1	**22.1**
x_7	16	7.1	**17.1**

Таблица 4. **Платёжная матрица** B

	y_1	y_2	y_3
x_1	**8**	10	18
x_2	18	109	127
x_3	13	**0.1**	13.1
x_4	**8**	10	18
x_5	**8**	**0.1**	**8.1**
x_6	13	**0.1**	13.1
x_7	**8**	**0.1**	**8.1**

Если администратор безопасности и злоумышленник выберут свои оптимальные стратегии x_5 и y_3, то цена игры для них будет 12.1 у.е. (ущерб администратора) и 8.1 у.е. (прибыль злоумышленника).

Таблица 5. **Платёжная матрица** A

	y_1	y_2
x_1	10	**11**
x_2	25	**115**
x_3	**16**	2.1

Таблица 6. **Платёжная матрица** B

	y_1	y_2
x_1	**8**	10
x_2	18	109
x_3	13	**0.1**

Теперь найдём приближённое решение данной задачи итеративным методом. Для этого составим платёжные матрицы A и B, используя только чистые стратегии игроков. Последовательно перебирая стратегии игроков, так же заполним две таблицы, в одной из них указывая ущерб администратора a_{ij} (см. табл. 5), а во второй – прибыль b_{ij} злоумышленника (см. табл. 6), соответственно, при выборе стратегии защиты $x_i (i = 1, 2, 3)$ и способа атаки $y_j (j = 1, 2)$.

Для нахождения начальных чистых стратегий x_{i_0} и y_{j_0} воспользуемся минимаксными критериями (1) и (2). Из платёжной матрицы A определим $W_{i0}(A) = \min\limits_i \{11,\ 115,\ 16\} = 11$, откуда следует, что для администратора безопасности $x_{i_0} = x_1$. Аналогично из платёжной матрицы B определим $W_{i0}(B) = \max\limits_j \{8,\ 0.1\} = 8$, откуда следует, что для злоумышленника $y_{j_0} = y_1$. Результаты расчётов каждой партии k запишем в табл. 7.

В первой партии игры (при $k = 1$) в 7–8-й столбцы табл. 7 из платёжной матрицы A записываются возможные исходы игры для администратора безопасности при выборе им стратегии $x_{i_0} = x_1$ (из первой строки матрицы A в табл. 5), из них выбирается максимальное значение. Чистая стратегия злоумышленника, при которой цена игры для администратора будет максимальна, принимается за оптимальную y_{j_1} (цена игры для администратора равна 11 у.е. при стратегии злоумышленника y_2). В 4–6-й столбцы табл. 7 из матрицы B

Таблица 7. **Выигрыши игроков**

k	Выбор игрока 1	Выбор игрока 2	Выигрыш игрока 1			Выигрыш игрока 2		$\overline{v^k}/k$	$\underline{v^k}/k$
			x_1	x_2	x_3	y_1	y_2		
1	x_1	y_1	**8**	18	13	10	**11**	11	8
2	x_1	y_2	18	127	**13.1**	20	**22**	$22/2 = 11$	$13.1/2 = 6.55$
3	x_3	y_2	28	236	**13.2**	**36**	24.1	$36/3 = 12$	$13.2/3 = 4.4$
4	x_3	y_1	36	254	**26.2**	**52**	26.2	$52/4 = 13$	$26.2/4 = 6.55$
5	x_3	y_1	44	272	**39.2**	**68**	28.3	$68/5 = 13.6$	$39.2/5 = 7.84$
6	x_3	y_1	**52**	290	52.2	**84**	30.4	$84/6 = 14$	$52/6 \approx 8.67$
7	x_1	y_1	**60**	308	65.2	**94**	41.4	$94/7 \approx 13.4$	$60/7 \approx 8.57$
8	x_1	y_1	**68**	326	78.2	**104**	52.4	$104/8 = 13$	$68/8 = 8.5$
9	x_1	y_1	**76**	344	91.2	**114**	63.4	$114/9 = 12.7$	$76/9 = 8.44$
10	x_1	y_1	**84**	362	104.2	**124**	74.4	**12.4**	**8.4**
...	...	...	...	...	...	...	...	...	...

записываются возможные исходы игры для хакера при выборе им стратегии $y_{j_0} = y_1$ (из первого столбца матрицы B в табл. 6). Стратегия администратора безопасности, при которой цена игры будет минимальна для злоумышленника, выбирается в качестве оптимальной для администратора безопасности, и $x_{i_1} = x_1$. В последние два столбца таблицы записывают цены игры для игроков.

Во второй партии игры (при $k = 2$) в 7–8-й столбцы табл. 7 из платёжной матрицы A записывается сумма соответствующих значений возможных исходов игры для администратора безопасности при выборе им стратегии $x_{i_1} = x_1$ и значений исходов игры первой партии (из предыдущей строки), из полученных сумм выбирается максимальное значение, по которому определяется следующая оптимальная чистая стратегия злоумышленника $y_{j_2} = y_2$. Аналогично в 4–6-й столбцы табл. 7 из матрицы B записывается сумма возможных исходов игры для хакера при выборе им стратегии $y_{j_1} = y_2$ и значений исходов игры первой партии (из предыдущей строки), из полученных сумм выбирается минимальное значение, по которому определяется оптимальная чистая стратегия администратора безопасности $x_{i_2} = x_3$. При расчёте цен игры для игроков нужно найденные суммы разделить на номер партии игры k, полученные значения заносятся в два последних столбца табл. 7. Аналогичные расчёты производятся для следующих партий игры.

Как видно из табл. 7, уже после проведения 10 партий (при $k = 10$) становится понятно, что оптимальная **смешанная** стратегия администратора безопасности состоит в использовании программных средств защиты x_1 и x_3 (см. второй столбец табл. 7), а оптимальной смешанной стратегией злоумышлен-

ника является использование обеих атак y_1 и y_2 (см. третий столбец в табл. 7). При этом приближённое решение биматричной игры (после 10 партий при выборе оптимальных стратегий игроков ущерб администратора 12.4 у.е. и прибыль злоумышленника 8.4 у.е.) с ростом числа партий приближается к точному решению (ущерб администратора 12.1 у.е. и прибыль злоумышленника 8.1 у.е.).

6. Заключение

В матричных играх у игроков имеет место строгое соперничество, поскольку выигрыш одного игрока в точности равен проигрышу другого, а в биматричных играх интересы игроков могут быть любыми, даже похожими. Поэтому анализ результатов расчётов биматричных игр может быть полезен администратору безопасности в принятии более верных решений в вопросах оптимизации защиты компьютерной системы. Предложенный в данной статье итеративный алгоритм даст выигрыш во времени нахождения решения биматричных игр с платёжными матрицами огромных размеров по сравнению с нахождением точного решения традиционными способами.

Литература

1. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: Учебное пособие. Омск : Изд-во ОмГУ, 2013. 160 с.
2. Вахний Т.В., Гуц А.К., Пахотин И.Ю. Определение оптимального набора средств защиты компьютерной системы методом Монте-Карло // Математические структуры и моделирование. 2018. № 1(45). С. 148–158.
3. Вахний Т.В., Зиновьев С.А., Бесценный И.П. Игровой подход к защите компьютерных систем и алгоритм «Thompson Sampling» // Математическое и компьютерное моделирование [электронный ресурс]: сборник материалов VII Международной научной конференции, посвящённой памяти С.С. Ефимова (Омск, 22 ноября, 2019 г.). Омск: Изд-во Омского государственного университета, 2020. С. 160–162. URL: `http://fkn.omsu.ru/nauka/Conf/2019/VII-MCM-Conf-2019.pdf` (дата обращения: 01.03.2022).
4. Петросян Л.А., Зенкевич Н.А., Шевкопляс Е.В. Теория игр: учебник. СПб. : БХВ-Петербург, 2012. 432 с.
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.

ITERATIVE SOLUTION OF A BIMATRIC GAME TO OPTIMIZE THE PROTECTION OF A COMPUTER SYSTEM

T.V. Vakhniy
Ph.D.(Phys.-Math.), Associate Professor, e-mail: vahniytv@mail.ru
S.V. Vakhniy
Student, e-mail: vakhniysv@mail.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The article suggests to solve a bimatric game between an attacker and a security administrator with huge sizes of players' payment matrices, to use an approximate iterative method that is less expensive for computing resources, the algorithm of which is based on the Brown–Robinson method.

Keywords: Information security, computer system, bimatric games, iterative methods, optimal strategy, software product.

References

1. Guts A.K. and Vakhnii T.V. Teoriya igr i zashchita komp'yuternykh sistem: Uchebnoe posobie. Omsk, Izd-vo OmGU, 2013, 160 p. (in Russian)
2. Vakhnii T.V., Guts A.K., and Pakhotin I.Yu. Opredelenie optimal'nogo nabora sredstv zashchity komp'yuternoi sistemy metodom Monte-Karlo. Matematicheskie struktury i modelirovanie, 2018, no. 1(45), pp. 148–158. (in Russian)
3. Vakhnii T.V., Zinov'ev S.A., and Bestsennyi I.P. Igrovoi podkhod k zashchite komp'yuternykh sistem i algoritm "Thompson Sampling". Matematicheskoe i komp'yuternoe modelirovanie [elektronnyi resurs]: sbornik materialov VII Mezhdunarodnoi nauchnoi konferentsii, posvyashchennoi pamyati S.S. Efimova (Omsk, 22 noyabrya, 2019 g.), Omsk, Izd-vo Omskogo gosudarstvennogo universiteta, 2020, pp. 160–162. URL: `http://fkn.omsu.ru/nauka/Conf/2019/VII-MCM-Conf-2019.pdf` (01.03.2022). (in Russian)
4. Petrosyan L.A., Zenkevich N.A., and Shevkoplyas E.V. Teoriya igr: uchebnik. Saint Petersburg, BKhV-Peterburg, 2012, 432 p. (in Russian)
5. Vakhnii T.V., Guts A.K., and Novikov N.Yu. Matrichno-igrovaya programma s vyborom kriteriya dlya opredeleniya optimal'nogo nabora sredstv zashchity komp'yuternoi sistemy. Matematicheskie struktury i modelirovanie, 2016, no. 2(38), pp. 103–115. (in Russian)

Дата поступления в редакцию: 14.03.2022