Математические структуры и моделирование
2025. № 1 (73). С. 116–124

УДК 519.83:004.056
DOI 10.24147/2222-8772.2025.1.116-124

РЕШЕНИЕ БИМАТРИЧНОЙ ИГРЫ С УЧЁТОМ ИЕРАРХИЧЕСКОГО НЕРАВЕНСТВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ И ЗЛОУМЫШЛЕННИКА

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 предложена математическая модель для проведения биматричной игры между администратором безопасности компьютерной системы и злоумышленником с учётом их иерархического неравенства. Сравнение полученных наиболее вероятных наилучших результатов игроков позволяет численно проверить возможность увеличения выигрыша игрока при повышении его иерархической ступени.

Ключевые слова: компьютерная система, кибербезопасность, биматричная игра, иерархическая игра, оптимальная стратегия.

Введение

Теоретико-игровой подход активно используется для организации безопасности компьютерных систем, позволяя оптимизировать выбор методов и средств защиты [1–5]. Обычно рассматриваются игровые модели принятия решений, в которых положение игроков является равноправным, т. е. понятие оптимальности стратегии не зависит от номера игрока. Однако существуют ситуации, в которых участники конфликтной ситуации не являются равноправными, что может выражаться в определённом порядке выбора решений, различной информированности, возможности влиять на выбор других участников и т. д. Для моделирования таких ситуаций можно воспользоваться теорией иерархических игр. Иерархические игры – это модели конфликтных ситуаций с неравноправными участниками, в которых исследование проводится с точки зрения управляющего (ведущего) игрока [6, 7].

В данной статье предлагается решить биматричную игру с учётом иерархического неравенства администратора безопасности и злоумышленника, сделав одного из игроков управляющим, и сравнить полученные результаты с решением аналогичной биматричной игры, в которой не учитывается иерархическое неравенство игроков. Сопоставление полученных гарантированных наилучших результатов игроков позволит численно проверить, есть ли возможность увеличения выигрыша игрока при повышении его иерархической ступени.

1. Математическая модель биматричной игры

Один из подходов, моделирующих игру администратора безопасности и атакующего злоумышленника, основан на проведении биматричной игры, в которой интересы игроков не совпадают и не являются противоположными, а выигрыши задаются платёжными матрицами отдельно для каждого игрока [3, 4]. В каждой из матриц строки соответствуют стратегиям одного игрока (программное средство или набор из программных средств), а столбцы – стратегиям другого игрока. На их пересечении в первой платёжной матрице A стоит цена игры для злоумышленника, а во второй платёжной матрице B – цена игры для администратора безопасности. Проведение биматричной игры позволяет определить наиболее выигрышные стратегии для каждого игрока.

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

Ходом злоумышленника является использование одной из N стратегий атаки x_i ($i = 1, 2, ..., N$) на компьютерную систему, а ходом администратора безопасности – применение одной из M стратегий защиты y_j ($i = 1, 2, ..., M$). Последовательно перебирая все стратегии игроков, можно заполнить две таблицы, в одной из них указывая прибыль злоумышленника a_{ij} (см. табл. 1), а во второй – ущерб b_{ij} администратора (см. табл. 2), соответственно, при выборе атаки x_i ($i = 1, 2, ..., N$) и способа защиты y_j ($i = 1, 2, ..., M$).

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}

Из табл. 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 злоумышленника A вычисляются по формуле:

$$a_{ij} = P(x_i, y_j) - V_i,$$

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

Аналогично элементы b_{ij} платёжной матрицы администратора безопасности B вычисляются следующим образом:

$$b_{ij} = R(x_i, y_j) + Q_j,$$

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

Биматричная игра является одноходовой. Процесс игры состоит в том, что злоумышленник выбирает стратегию атаки x_i, а администратор выбирает стратегию защиты y_j, после чего вычисляется исход игры, заключающийся в том, что злоумышленник получает прибыль a_{ij}, а администратор терпит ущерб, равный b_{ij}. Цель атакующего – выбор такой стратегии, которая даст ему наибольший выигрыш, а 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. Решение биматричной игры сводится к отысканию равновесных (оптимальных) стратегий игроков [1].

2. Критерии выбора оптимальных стратегий

Скорее всего злоумышленник осуществляет атаку на компьютерную систему с целью извлечь из этого какую-то выгоду. При этом он может позволить себе рисковать, поскольку в любом случае администратор безопасности вряд ли собирается нанести ему материальный ущерб. От выбора стратегии злоумышленника зависит величина его выигрыша, поэтому он может быть как азартно увлечён получить наибольшую прибыль от атаки, так и играть осмотрительно, чтобы получить хоть какую-то гарантированную пользу от осуществления атаки [3].

Если злоумышленник ориентируется на самые неблагоприятные условия, то он стремится максимизировать свой возможный минимальный выигрыш, и в простейшем случае его оптимальную стратегию можно найти **из условия максимина** [1]. Поставим в соответствие каждой i-ой стратегии злоумышленника число $W_i(A)$, вычисляемое с помощью его платёжной матрицы A. Критерий выбора оптимальной стратегии x_{i0} для осторожного злоумышленника состоит в том, чтобы взять

$$W_{i_0}(A) = \max_i \min_j a_{ij}. \tag{1}$$

Если злоумышленник, стремясь получить наибольший выигрыш, играет азартно, то для выбора его оптимальной стратегии можно использовать **критерий крайнего оптимизма** [3]. Этот критерий подходит для азартного злоумышленника, так как для него обычно потери в игре малозначимы, и он может «рискнуть» понадеяться на самый крупный выигрыш из-за неудачной стратегии защиты компьютерной системы организации. В таком случае для каждой стратегии злоумышленника по его

платёжной матрице A определяется наилучший достижимый результат как максимальный элемент в строке, а наиболее подходящей для него считается та стратегия, для которой этот результат наибольший:

$$W_{i_0}(A) = \max_i \max_j a_{ij}. \tag{2}$$

Поскольку при неудачном выборе стратегии защиты ущерб от атаки злоумышленника может оказаться существенным или фатальным для организации, то от администратора безопасности компьютерной системы следует ожидать, прежде всего, осмотрительное поведение, чтобы минимизировать возможный максимальный ущерб. Поэтому оптимальную стратегию администратора, в простейшем случае, можно найти **из условия минимакса** [1]. Поставим в соответствие каждой j-ой стратегии администратора число $W_j(B)$, вычисляемое с помощью его платёжной матрицы B, тогда критерий выбора его оптимальной стратегии y_{j0} состоит в том, чтобы взять

$$W_{j_0}(B) = \min_j \max_i b_{ij}. \tag{3}$$

Максиминная и минимаксная стратегии игроков уместны в тех случаях, когда они не столько хотят выиграть, сколько не хотят проиграть. Применение критерия крайнего оптимизма редко позволяет получить максимально возможный выигрыш, но злоумышленник может себе позволить такую стратегию игры. При необходимости злоумышленник и администратор безопасности могут выбрать для себя и другие критерии для подбора наиболее оптимальных для них наборов программных средств [3, 4].

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

3. Учёт иерархического неравенства злоумышленника и администратора безопасности

В биматричной игре игроки принимают решения одновременно и не знают о выборе своих противников. Однако часто игроки принимают решения последовательно, и к моменту принятия решения одного из игроков уже становится известно, как повёл себя другой игрок. Это приводит к необходимости построения игровых моделей, учитывающих последовательность принятия решений игроками, а также информационную асимметрию. В теории игр для этого используются различные модели с «неравенством» игроков – как в смысле различной очередности хода, так и в смысле разной степени осведомлённости о поведении противников. Такой класс теоретико-игровых моделей описывает **иерархические игры** [6, 7].

Рассмотрим, как может быть описана одношаговая иерархическая игра, на примере взаимодействия злоумышленника и администратора безопасности компьютерной системы в предположении, что ведущая роль принадлежит злоумышленнику.

Такая постановка задачи возможна, если имеем дело с опытным злоумышленником, прекрасно осведомлённым о способах защиты информационного ресурса, которыми располагает администратор безопасности. К тому же именно злоумышленник делает первым ход, организуя атаку на компьютерную систему, и ему же принадлежит инициатива в противостоянии игроков [6].

Множество стратегий злоумышленника обозначим X, а множество стратегий администратора безопасности компьютерной системы – Y. В теории иерархических игр говорится, что интересы злоумышленника характеризует функция выигрыша $F(x_i, y_j)$, интересы администратора – аналогичная функция $G(x_i, y_j)$, поэтому иерархическая игра может быть задана совокупностью $\Gamma = \{X, Y, F(x_i, y_j), G(x_i, y_j)\}$, где $i = 1, 2, ..., N; j = 1, 2, ..., M$. Значения функций выигрыша игроков $F(x_i, y_j)$ и $G(x_i, y_j)$ будем определять из составленных платёжных матриц A и B соответственно. Таким образом, биматричную игру с учётом иерархического неравенства игроков зададим совокупностью $\Gamma = \{X, Y, A, B\}$.

Сначала злоумышленник выбирает некоторую стратегию $x_{i_0} \in X$ и начинает атаку, т. е. совершает свой выбор до того, как это сделает второй игрок. При этом злоумышленнику важно учесть интересы администратора безопасности компьютерной системы, так как итог их взаимодействия зависит именно от него, делающего завершающий ход. Далее администратор безопасности, узнав стратегию злоумышленника x_{i_0}, выбирает свою стратегию защиты $y_{j_0} \in Y$, которая позволит ему минимизировать ущерб от предпринятой злоумышленником атаки. Итогом игры является нахождение наилучшего гарантированного результата злоумышленника $a_{i_0 j_0}$ и цены игры (ущерба от атаки) для администратора безопасности $b_{i_0 j_0}$.

При проведении биматричной игры с учётом иерархического неравенства игроков будем считать, что злоумышленник обладает полной информацией о ресурсах атакуемой компьютерной системы, и поэтому можно считать, что ему также известна функция выигрыша администратора безопасности $G(x_i, y_j)$, где $i = 1, 2, ..., N; j = 1, 2, ..., M$. Злоумышленник понимает, что администратор будет выбирать стратегию из множества $Y(x_{i_0})$, он не может знать его конкретного выбора $y_j \in Y(x_{i_0})$ $(j = 1, 2, ..., M)$, но может ожидать, что будет выбрана такая стратегия защиты y_{j_0}, которая позволит уменьшить ущерб от атаки x_{i_0} на компьютерную систему.

Для получения наибольшей прибыли от атаки злоумышленнику нужно предварительно рассмотреть несколько гипотез о выборе предпочтительных стратегий защиты при реализации предполагаемых стратегий атаки. Анализ размера получаемого при этом выигрыша даст злоумышленнику возможность сделать наиболее удачный для него выбор стратегии атаки x_{i_0}.

4. Сравнение решений биматричной игры с учётом и без учёта иерархического неравенства игроков

1) Решение биматричной игры при осторожном злоумышленнике

Рассмотрим решение биматричной игры с платёжными матрицами небольшого размера A и B (см. табл. 3 и 4) для случая, когда атакующий злоумышленник и администратор безопасности компьютерной системы крайне осторожны. Тогда

их оптимальные стратегии можно найти из условий максимина (1) и минимакса (3) соответственно.

Таблица 3. **Платёжная матрица A**

	y_1	y_2	y_3	y_4
x_1	7	4	**2**	4
x_2	7	7	**3**	6
x_3	5	**3**	8	8
x_4	6	**4**	5	5

Таблица 4. **Платёжная матрица B**

	y_1	y_2	y_3	y_4
x_1	3	**6**	**8**	3
x_2	3	3	4	**8**
x_3	**7**	2	5	6
x_4	3	1	4	2

При использовании критериев максимина (1) и минимакса (3) оцениваются значения ячеек платёжных матриц A и B. В каждой строке платёжной матрицы злоумышленника A выделим ячейки с наименьшими значениями выигрыша, а в платёжной матрице администратора безопасности B в каждом столбце выделим ячейки с наибольшими значениями ущерба. Согласно формулам (1) и (3) получается $W_{i_0=4}(A) = \max(2,3,3,4) = 4$ и $W_{j_0=2}(B) = \min(7,6,8,8) = 6$, поэтому для злоумышленника и администратора безопасности лучшими стратегиями будут x_4 и y_2 соответственно. В таком случае выигрыш злоумышленника будет 4 у. е., а ущерб администратора безопасности компьютерной системы – 1 у. е. (см. в табл. 3 и 4).

2) Решение биматричной игры при азартном злоумышленнике

Рассмотрим решение биматричной игры с теми же платёжными матрицами небольшого размера A и B (см. табл. 3 и 4), но для случая, когда администратор безопасности осторожен, а злоумышленник играет азартно. Тогда их оптимальные стратегии можно найти из условий (3) и (2) соответственно.

В каждой строке платёжной матрицы злоумышленника A выделим ячейки с наибольшими значениями выигрыша, а в платёжной матрице администратора безопасности B в каждом столбце выделим ячейки с наибольшими значениями ущерба (см. в табл. 5 и 6).

Таблица 5. **Платежная матрица A**

	y_1	y_2	y_3	y_4
x_1	**7**	4	2	4
x_2	**7**	**7**	3	6
x_3	5	3	**8**	**8**
x_4	**6**	4	5	5

Таблица 6. **Платежная матрица B**

	y_1	y_2	y_3	y_4
x_1	3	**6**	**8**	3
x_2	3	3	4	**8**
x_3	**7**	2	5	6
x_4	3	1	4	2

Согласно формулам (2) и (3) получается $W_{i_0=3}(A) = \max(7,7,8,6) = 8$ и $W_{j_0=2}(B) = \min(7,6,8,8) = 6$, поэтому для злоумышленника и администратора лучшими стратегиями будут x_3 и y_2 соответственно. Тогда выигрыш злоумышленника составит 3 у. е., а ущерб администратора безопасности компьютерной системы – 2 у. е. Как бы ни стремился злоумышленник увеличить свой выигрыш, такой подход

к выбору оптимальной стратегии не может гарантированно обеспечить ему лучший результат игры.

3) Решение иерархической игры при ведущем злоумышленнике

В биматричной игре с учётом иерархического неравенства игроков будем считать, что ведущим (управляющим) игроком является злоумышленник, который делает ход первым и имеет полную информацию об интересах ведомого игрока – администратора безопасности компьютерной системы.

Рассмотрим несколько гипотез о выборе предпочтительных стратегий защиты при реализации предполагаемых стратегий атаки (см. табл. 7 и 8):

– при выборе злоумышленником стратегии x_1 администратору безопасности выгодно выбрать стратегию защиты y_1 или y_4 (так как $W_{j_0=1}(B) = W_{j_0=4}(B) = \min(3, 6, 8, 3) = 3$), в результате чего злоумышленник получит выигрыш 7 или 4 у. е. соответственно;

– если же злоумышленник выберет стратегию атаки x_2, то администратору безопасности актуально выбрать стратегию защиты y_1 или y_2 (так как $W_{j_0=1}(B) = W_{j_0=2}(B) = \min(3, 3, 4, 8) = 3$), в результате выигрыш злоумышленника составит 7 у. е.;

– в случае выбора злоумышленником стратегии x_3 или x_4, администратор безопасности скорее всего выберет стратегию защиты y_2 (так как $W_{j_0=2}(B) = \min(7, 2, 5, 6) = 2$ и $W_{j_0=2}(B) = \min(3, 1, 4, 2) = 1$), поэтому злоумышленнику стоит ожидать совсем небольшой выигрыш – 3 или 4 у. е. соответственно.

Таблица 7. **Платёжная матрица A**

	y_1	y_2	y_3	y_4
x_1	**7**	4	2	**4**
x_2	**7**	**7**	3	6
x_3	5	**3**	8	8
x_4	6	**4**	5	5

Таблица 8. **Платёжная матрица B**

	y_1	y_2	y_3	y_4
x_1	**3**	6	8	**3**
x_2	**3**	**3**	4	8
x_3	7	**2**	5	6
x_4	3	**1**	4	2

Проанализировав возможный размер предполагаемого выигрыша при различных стратегиях атаки, злоумышленнику становится понятно, что наиболее удачной для него будет стратегия x_2. В таком случае выигрыш злоумышленника составит 7 у. е., а ущерб администратора безопасности – 3 у. е. Таким образом, при повышении иерархической ступени у атакующего злоумышленника появляется шанс существенно увеличить свой выигрыш.

Кроме того, если злоумышленник владеет ещё и информацией о системе безопасности компании, например о том, что в данный момент используется стратегия защиты y_2 и в ближайшее время её менять не планируется, то для получения наибольшего выигрыша злоумышленнику остаётся выбрать наилучшую для него стратегию атаки x_2.

4) Иерархическая игра при ведущем администраторе безопасности

При построении системы защиты и после её внедрения в компании администратору безопасности необходимо регулярно анализировать информацию об атаках на

компьютерные системы, изучать новые угрозы, а также из огромного количества современных средств защиты выбирать наиболее подходящие для понижения риска потери конфиденциальности, целостности и доступности информации. Изучение возможностей атакующих злоумышленников позволит администратору безопасности повысить свою иерархическую ступень в противостоянии со злоумышленником.

Администратор безопасности может попробовать составить платёжную матрицу злоумышленника, рассмотреть гипотезы о выборе предпочтительных стратегий атаки при реализации предполагаемых стратегий защиты и на основании этого определить наилучшую стратегию защиты компьютерной системы. Но в любом случае даже самый опытный администратор безопасности не может позволить себе быть неосторожным, опираясь лишь на результаты решения иерархической игры, в которой он выступал в качестве ведущего игрока. К тому же невозможно в одной платёжной матрице собрать интересы различных злоумышленников. Однако проведение подобных игр и анализ их результатов поможет администратору безопасности обратить внимание на дополнительные программные средства защиты, что может пригодиться для построения более надёжной системы безопасности компьютерной системы.

5. Заключение

В статье даётся описание математической модели для проведения биматричной игры между администратором безопасности компьютерной системы и злоумышленником с учётом их иерархического неравенства в смысле различной очерёдности хода и разной степени осведомлённости. На основе сравнения полученных наиболее вероятных наилучших результатов игроков было показано, что повышение иерархической ступени злоумышленника может позволить ему увеличить выигрыш от атаки. Таким образом численно была подтверждена необходимость скрывать данные как о важнейших ресурсах компьютерной системы компании, так и об используемых методах и средствах её защиты.

Литература

1. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие. Омск: ОмГУ, 2013. 160 с.
2. Вахний Т.В., Константинов П.В. Создание сервиса для анализа защищённости компьютерных систем на основе теоретико-игрового подхода и базы знаний MITRE ATT&CK // Математические структуры и моделирование. 2024. № 2 (70). С. 80–86.
3. Вахний Т.В., Вахний С.В. Решение биматричной игры с применением различных критериев для выбора стратегий администратора безопасности и злоумышленника // Математические структуры и моделирование. 2023. № 3 (67). С. 111–120.
4. Вахний Т.В., Вахний С.В. Оптимизация выбора наилучшей стратегии защиты от вредоносных атак на основе решения биматричной игры с учётом рисков // Математические структуры и моделирование. 2024. № 1 (69). С. 103–109.

5. Гуц А.К. Выявление цены психологической ошибки администратора компьютерной сети в оценке квалификации злоумышленников // Омские научные чтения: материалы Всероссийской научно-практической конференции. Омск: ОмГУ, 2017. С. 319–321.
6. Вахний Т.В., Гуц А.К. Иерархические игры и защита компьютерных систем // Омские научные чтения: материалы Второй Всероссийской научной конференции. Омск: ОмГУ, 2018. С. 174–175.
7. Васин А.А., Морозов В.В. Теория игр и модели математической экономики: учебное пособие. М.: МАКС Пресс, 2005. 272 с.

THE SOLUTION OF A BIMATRIC GAME TAKING INTO ACCOUNT THE HIERARCHICAL INEQUALITY OF THE SECURITY ADMINISTRATOR AND THE ATTACKER

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 proposes a mathematical model for conducting a bimatrical game between a computer system security administrator and an attacker, taking into account their hierarchical inequality. Comparing the most likely best results of the players obtained allows us to numerically check the possibility of increasing the player's winnings with an increase in his hierarchical level.

Keywords: computer system, cybersecurity, bimatric game, hierarchical game, optimal strategy.

Дата поступления в редакцию: 13.11.2024