Математические структуры и моделирование
2025. № 2 (74). С. 131–137

УДК 519.83:004.056
DOI 10.24147/2222-8772.2025.2.131-137

ТЕОРИЯ ИГР В КИБЕРПРОСТРАНСТВЕ: РЕФЛЕКСИВНЫЙ ПОДХОД К МОДЕЛИРОВАНИЮ ВЗАИМОДЕЙСТВИЯ АДМИНИСТРАТОРА И ЗЛОУМЫШЛЕННИКА

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

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

Аннотация. Предложена расширенная модель биматричной игры, учитывающая различные уровни стратегической рефлексии администратора безопасности и злоумышленника.

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

Введение

В эпоху цифровых технологий кибербезопасность и защита данных приобретают критическое значение для успеха бизнеса. Последствия успешной кибератаки могут выйти далеко за рамки утечки данных и финансовых потерь, затронув операционную устойчивость, репутацию и даже само существование организации. Для эффективной борьбы с киберугрозами необходимо понимать возможные причины, лежащие в основе изменений в тактиках злоумышленника. В этой связи теоретико-игровые модели предлагают удобный инструмент для анализа взаимодействия между администратором безопасности и злоумышленником, позволяя оптимизировать выбор методов и средств защиты для построения надёжной системы безопасности, минимизирующей экономические риски компании [1–5].

В данной статье для моделирования стратегического взаимодействия в киберпространстве предлагается построить биматричную игру администратора безопасности со злоумышленником и решать её с введением рангов рефлексии для каждого игрока. Сопоставление полученных наилучших гарантированных результатов игроков позволит проанализировать, как учёт стратегической рефлексии влияет на выбор оптимальных стратегий, а также численно проверить, есть ли возможность увеличения выигрыша игрока при повышении его ранга рефлексии и может ли игнорирование этой способности привести к неоптимальным решениям. Предложенный подход будет полезен как для анализа применяемых, так и для поиска более эффективных стратегий защиты компьютерных систем от хакерских атак.

1. Постановка задачи и игровой подход

Один из подходов, моделирующий игру администратора безопасности и атакующего злоумышленника, основан на проведении биматричной игры, в которой интересы игроков не совпадают, а выигрыши задаются разными платёжными матрицами [2–4]. В этих матрицах строки соответствуют стратегиям одного игрока (программное средство или набор из программных средств), столбцы – стратегиям другого игрока, на их пересечении в первой матрице A стоит цена игры для администратора безопасности, а во второй матрице B – цена игры для злоумышленника. Проведение биматричной игры позволяет определить наиболее выигрышные стратегии для каждого игрока.

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.

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

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 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.

В биматричной игре игроки выбирают свои стратегии однократно, одновременно и независимо друг от друга. 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}. Решение биматричной игры сводится к поиску равновесных (оптимальных) стратегий игроков [2–4].

2. Критерии выбора оптимальных стратегий администратора безопасности и злоумышленника

В биматричной игре администратор безопасности стремится выбрать такую стратегию, которая позволит ему свести к минимуму наносимый компьютерной системе ущерб от реализации атак злоумышленника при минимизации финансовых затрат на покупку средств защиты. Поставим в соответствие каждой стратегии администратора x_i число $W_i(A)$, вычисляемое с помощью его платёжной матрицы A. Критерий выбора оптимальной стратегии x_{i_0} для администратора состоит в том, чтобы взять

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

В свою очередь, злоумышленник стремится выбрать такую стратегию, которая позволит ему максимизировать свой возможный выигрыш от реализации тех или иных угроз. Если при этом он ориентируется на самые неблагоприятные условия, то ему нужно максимизировать свой возможный минимальный выигрыш. В таком случае критерий выбора оптимальной стратегии y_{j_0} для злоумышленника состоит в том, чтобы взять

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

Таким образом, $W_{i_0}(A)$ и $W_{j_0}(B)$ – это наилучшие гарантированные результаты администратора безопасности и злоумышленника соответственно.

Минимаксная (1) и максиминная (2) стратегии уместны в тех случаях, когда администратор и злоумышленник не столько хотят выиграть, сколько не хотят проиграть [2]. Хотя они могут выбрать для себя и другие критерии для подбора наиболее оптимальных для них наборов программных средств [4–6].

3. Учёт стратегической рефлексии игроков

Взаимодействие администратора безопасности и злоумышленника в киберпространстве похоже на динамичную игру, в которой каждая сторона адаптирует свои стратегии, пытаясь предугадать действия оппонента. Классические биматричные игры являются полезным инструментом для моделирования таких сценариев, но они пренебрегают важным аспектом – стратегической рефлексией, т. е. способностью игроков думать о мыслях друг друга.

Дополним математическую модель биматричной игры введением рангов рефлексии для каждого игрока. Будем считать, что игрок с нулевым рангом рефлексии знает только собственную платёжную матрицу и действует, исходя из своей гарантированной наилучшей стратегии, не учитывая возможные действия оппонента, а игрок с ненулевым рангом рефлексии, равным k, предполагает, что его противник обладает чуть более низким рангом рефлексии, равным $k-1$. Это позволяет ему выбирать оптимальную стратегию, основываясь не только на своей платёжной матрице, но и на анализе наиболее вероятных действий второго игрока [7]. При этом расчёт ожидаемых выигрышей и выбор стратегий производится им рекурсивно на основе уже рассчитанных стратегий оппонента на уровне $k-1$.

В предложенной модели биматричной игры администратор безопасности и злоумышленник могут иметь разные уровни стратегической рефлексии, что позволяет моделировать сценарии, где один из них более искусен в анализе поведения оппонента.

4. Решение биматричной игры при задании у администратора безопасности и злоумышленника различных рангов рефлексии

Решение биматричной игры без учёта рефлексии игроков

Рассмотрим решение биматричной игры администратора безопасности и злоумышленника с платёжными матрицами небольшого размера A и B (табл. 3 и 4) для случая, когда игроки не пытаются предугадать наилучшие стратегии друг друга. Будем считать, что они играют осторожно, поэтому их оптимальные стратегии будем находить из условий минимакса (1) и максимина (2) соответственно.

Таблица 3. Платёжная матрица A

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

Таблица 4. Платёжная матрица B

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

В каждой строке платёжной матрицы администратора безопасности A выделим ячейки с наибольшими значениями ущерба, а в платёжной матрице злоумышлен-

ника B в каждом столбце выделим ячейки с наименьшими значениями выигрыша от атаки. Согласно формулам (1) и (2) получается, что наилучшие гарантированные результаты игроков равны $W_{i_0=2}(A) = \min(7, 6, 8, 8) = 6$ и $W_{j_0=4}(B) = \max(2, 3, 3, 4) = 4$. Поэтому для администратора безопасности и злоумышленника лучшими стратегиями будут x_2 и y_4 соответственно. При выборе игроками этих стратегий ущерб администратора безопасности будет составлять 3 у. е., а выигрыш злоумышленника – 4 у. е. (табл. 3 и 4).

Решение биматричной игры с ненулевым рангом рефлексии у злоумышленника

Рассмотрим, как изменится решение биматричной игры с теми же платёжными матрицами A и B (табл. 3 и 4), когда у злоумышленника будет ненулевой уровень рефлексии $k_B = 1$. В таком случае злоумышленник может догадаться, что администратор безопасности выберет стратегию защиты x_2. Тогда $W_{j_0=2}(B) = \max(4, 7, 3, 4) = 7$, поэтому для злоумышленника лучшей стратегией будет y_2. При выборе игроками этих стратегий ущерб администратора безопасности будет 4 у. е., а выигрыш злоумышленника – 7 у. е. Таким образом, повышение уровня рефлексии злоумышленника позволило ему увеличить выигрыш на 3 у. е. по сравнению с предыдущей ситуацией, когда его уровень рефлексии был нулевым. При этом ущерб администратора безопасности увеличился на 1 у. е.

Решение биматричной игры с ненулевым рангом рефлексии у администратора безопасности

Рассмотрим решение биматричной игры с теми же платёжными матрицами A и B (табл. 3 и 4), когда у администратора безопасности ненулевой уровень рефлексии $k_A = 1$. В таком случае администратор может догадаться, что злоумышленник выберет стратегию y_4. Тогда $W_{i_0=4}(A) = \min(3, 3, 4, 2) = 2$, поэтому для администратора лучшей стратегией будет x_4. При выборе игроками этих стратегий ущерб администратора безопасности будет 2 у. е., а выигрыш злоумышленника – 5 у. е. Таким образом, повышение уровня рефлексии администратора безопасности позволило ему уменьшить ущерб на 1 у. е. по сравнению с ситуацией, когда уровни рефлексии у обоих игроков были нулевыми.

Решение биматричной игры с учётом рефлексии обоих игроков

Рассмотрим решение биматричной игры с теми же платёжными матрицами A и B (табл. 3 и 4), но когда у администратора безопасности и злоумышленника ненулевые уровни рефлексии, равные $k_A = 2$ и $k_B = 1$ соответственно. В таком случае администратор может догадаться, что злоумышленник догадается, что администратор выберет стратегию x_4, на основании чего он выберет стратегию y_3. Тогда $W_{i_0=3}(A) = \min(7, 2, 1, 6) = 1$, поэтому для администратора лучшей стратегией будет x_3. При выборе игроками этих стратегий ущерб администратора безопасности составит 1 у. е., а выигрыш злоумышленника – 8 у. е. Таким образом, дальнейшее повышение уровня рефлексии администратора безопасности позволило ему уменьшить ущерб на 2 у. е. по сравнению с ситуацией, когда уровни рефлексии у обоих игроков были нулевыми.

Если же администратор безопасности будет считать, что у злоумышленника уровень рефлексии $k_B = 1$, а на самом деле он будет нулевым, то злоумышленник выберет стратегию y_4, а администратор – x_3. При выборе игроками этих стратегий ущерб

администратора безопасности составит 4 у. е., а выигрыш злоумышленника – 5 у. е. Таким образом, если ранг рефлексии игрока превышает ранг рефлексии противника больше, чем на 1, то повышение ранга рефлексии не гарантирует ему улучшения исхода игры.

Проведённый анализ решений биматричной игры, моделирующей стратегическое взаимодействие администратора безопасности и злоумышленника с учётом рефлексивности их мышления, показал, что повышение ранга рефлексии даёт игроку преимущество, если его ранг рефлексии будет на единицу выше, чем у противника.

Заключение

В статье продемонстрировано решение рефлексивной биматричной игры, моделирующей стратегическое взаимодействие администратора безопасности и злоумышленника. Анализ полученных решений показал, что более высокий ранг рефлексии обычно даёт игроку преимущество, но при этом оптимальный ранг рефлексии зависит от ранга рефлексии противника. В частности, игрок, чей ранг рефлексии на единицу выше, как правило, выигрывает, в то время как при большей разнице в рангах повышение ранга рефлексии не гарантирует игроку улучшения его исхода игры.

Перспективным направлением дальнейших исследований является разработка алгоритмов для автоматического определения уровней рефлексии игроков на основе анализа их поведения в реальных сценариях и дополнительное проведение игры рангов игроков [7].

Литература

1. 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.
2. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учеб. пособие. Омск: Изд-во ОмГУ, 2013. 160 с.
3. Вахний Т.В., Вахний С.В. Итеративное решение биматричной игры для оптимизации защиты компьютерной системы // Математические структуры и моделирование. 2022. № 1 (61). С. 105–114.
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. 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. Шевченко Д.В. Методы принятия управленческих решений: задания и методические указания для выполнения расчётно-графической работы. Казань: Познание, 2014. 69 с.
7. Новиков Д.А., Чхартишвили А.Г. Рефлексия и управление: математические модели. М.: Изд-во физ.-математ. лит., 2013. 412 с.

GAME THEORY IN CYBERSPACE: A REFLEXIVE APPROACH TO MODELING THE INTERACTION BETWEEN AN ADMINISTRATOR AND AN 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. This article offers an extended bimatric game model that takes into account different levels of strategic reflection between the security administrator and the attacker.

Keywords: Computer system, cybersecurity, bimatric game, reflection of the players, optimal strategy.

Дата поступления в редакцию: 27.02.2025