Математические структуры и моделирование
2024. № 1 (69). С. 103–109

УДК 519.83:004.056
DOI 10.24147/2222-8772.2024.1.103-109

ОПТИМИЗАЦИЯ ВЫБОРА СТРАТЕГИИ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ АТАК НА ОСНОВЕ РЕШЕНИЯ БИМАТРИЧНОЙ ИГРЫ С УЧЁТОМ РИСКОВ

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 описано решение биматричной игры между администратором безопасности и атакующим злоумышленником в два этапа. На первом этапе предлагается применять критерии оптимальности, учитывающие цену игры, а на втором этапе – критерии, учитывающие риски игроков. Такой подход помогает находить наилучшую стратегию защиты от атак злоумышленника среди стратегий с одинаковой ценой игры.

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

Введение

В современном мире цифровая трансформация охватывает почти все сферы деятельности, от бизнеса и образования до здравоохранения и государственного управления. Новейшие технологии, такие как искусственный интеллект, большие данные и интернет вещей, открывают огромные возможности для создания новых продуктов и услуг. Благодаря этому глобальная цифровизация позволяет компаниям стать более эффективными, инновационными и адаптивными, что является ключевым фактором успешной конкуренции на рынке. В связи с этим вопросы кибербезопасности и сохранности данных к кибератакам выходят на первый план. Непрекращающийся рост числа атак, их усложнение и изощрённость побуждают к созданию большого количества средств защиты, и построение надёжной системы безопасности становится всё более сложной задачей.

Стохастической природе проблем защиты компьютерных систем соответствуют математические методы принятия решений в условиях неопределённости, в частности методы теории игр. Использование теоретико-игрового подхода позволяет анализировать взаимодействие между администратором безопасности и атакующим злоумышленником, на основе чего обеспечить оптимизацию выбора программных продуктов для построения наилучшей системы безопасности компании [1–3].

В данной статье для оптимизации защиты компьютерной системы компании предлагается построить биматричную игру администратора безопасности со злоумышленником и предусмотреть нахождение её решения в два этапа. При этом на

первом этапе в расчётах следует применять критерии оптимальности, традиционно учитывающие цену игры, а на втором этапе – критерии, учитывающие риски игроков. Такой подход может быть полезен для нахождения наилучшей стратегии защиты от атак злоумышленника среди стратегий с одинаковой ценой игры.

1. Постановка задачи и игровой подход

Один из подходов, моделирующих игру администратора безопасности и атакующего злоумышленника, основан на проведении биматричной игры, в которой интересы игроков не совпадают и задаются разными платёжными матрицами. В платёжных матрицах 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 администратора безопасности, а во второй платёжной матрице B – цена игры для злоумышленника. Проведение биматричной игры позволяет определить наиболее выигрышные стратегии для каждого игрока.

Если администратор для обеспечения безопасности компьютерной системы компании может выбирать из S программных средств защиты, и при этом их можно устанавливать 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 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 x_i ($i = 1, 2, ..., N$), а ходом злоумышленника – применение одной из M стратегий атаки y_j ($j = 1, 2, ..., M$) на компьютерную систему компании. 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 и способа атаки y_j. 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 вычисляются следующим образом:

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

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

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

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

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

Биматричная игра 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. Решение биматричной игры сводится к отысканию равновесных (оптимальных) стратегий игроков x_{i_0} и y_{j_0}. Выбор одним из игроков любой другой стратегии вероятнее всего приведёт к ухудшению его результатов игры и улучшению их у противника.

В учебной литературе биматричная игра описывается как одноходовая [1,4]. Однако при выборе из большого количества программных продуктов у нескольких найденных наилучших стратегий администратора безопасности цена игры может оказаться одинаковой. Для таких случаев предлагается предусмотреть второй этап для уточнения решения биматричной игры. На первом этапе нужно найти наилучшие стратегии игроков и проверить, есть ли среди них такие, которые мало отличаются по цене игры. Если таковые найдутся, то предлагается построить новые платёжные матрицы из найденных на первом этапе наилучших стратегий игроков и уточнить решение биматричной игры, используя в этот раз критерии оптимальности, основанные на оценке степени удачности применений стратегий, т. е. величины риска. Риск рассчитывается как разность между ценой игры при выборе стратегии в условиях, когда заранее не известна стратегия второго игрока, и в условиях, когда она заранее известна [4].

2. Построение матриц рисков для администратора безопасности и злоумышленника

Матрица рисков для администратора безопасности R строится по столбцам его платёжной матрицы A. В каждом столбце нужно найти наименьшее значение, это значение по очереди вычесть из всех значений в данном столбце и результат записать в те же позиции. Элементы матрицы рисков для администратора безопасности рассчитывают по формуле: $r_{ij} = a_{ij} - \min\limits_{j} a_{ij}$. Они показывают, насколько больше

может быть ущерб компьютерной системе по сравнению с минимально возможным значением для каждого типа атаки злоумышленника из-за неверного выбора стратегии защиты.

Аналогично матрица рисков для атакующего злоумышленника строится по строкам его платёжной матрицы B. В каждой строке нужно найти наибольшее значение, из этого значения по очереди вычесть все значения в данной строке и результат записать в те же позиции. Элементы матрицы рисков для злоумышленника рассчитывают по формуле: $v_{ij} = \max\limits_{i} b_{ij} - b_{ij}$. Они показывают, насколько меньше может быть выигрыш по сравнению с максимально возможным значением.

3. Критерии выбора оптимальных стратегий игроков

3.1. Критерии оптимальности стратегий для первого этапа игры

Оптимальную стратегию администратора безопасности, который осмотрительно играет и стремится минимизировать свой возможный максимальный ущерб, в простейшем случае можно найти из условия **минимакса** [1]. В таком случае критерий выбора оптимальной стратегии x_{i0} для администратора состоит в том, чтобы из его платёжной матрицы A взять следующее число:

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

Если атакующий злоумышленник также 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]. Тогда критерий выбора оптимальной стратегии y_{j0} для злоумышленника состоит в том, чтобы из его платёжной матрицы B взять следующее число:

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

Минимаксная (1) и максиминная (2) стратегии игроков уместны в тех случаях, когда они не столько хотят выиграть, сколько не хотят проиграть. Хотя администратор безопасности и атакующий злоумышленник могут выбрать для себя и другие критерии для подбора наиболее оптимальных для них наборов программных средств, с помощью которых они смогут реализовать свои лучшие стратегии игры [3].

3.2. Критерии оптимальности стратегий для второго этапа игры

Необходимость в проведении второго этапа биматричной игры возникает, если на первом этапе найдено несколько наилучших стратегий игроков, имеющих одинаковую цену игры. В таком случае можно предположить, что на втором этапе игры второй игрок выбирает свою стратегию случайным образом, и воспользоваться теорией статистических решений [4]. Тогда среди найденных стратегий поиск наилучшей можно проводить, используя критерии оптимальности, основанные на оценке

степени удачности многократных применений стратегии, т. е. на оценке величины риска. Если оба игрока играют осторожно, то в простейшем случае для поиска их лучших стратегий наиболее подходит **критерий Сэвиджа (минимального максимального риска)** [4].

Согласно критерию Сэвиджа для администратора безопасности в каждой строке его матрицы рисков R определяется максимальный элемент, лучшей считается та стратегия, для которой этот результат наименьший. Таким образом, на втором этапе биматричной игры критерий выбора оптимальной стратегии x_{i0} для администратора безопасности состоит в том, чтобы из его матрицы рисков R взять следующее число:

$$W_{i_0}(R) = \min_i \max_j r_{ij}. \tag{3}$$

Аналогично для злоумышленника в каждом столбце его матрицы рисков V определяется максимальный элемент и лучшей считается та стратегия, для которой этот результат наименьший. Критерий выбора оптимальной стратегии y_{j0} для злоумышленника на втором этапе биматричной игры состоит в том, чтобы из его матрицы рисков V взять следующее число:

$$W_{j_0}(V) = \min_j \max_i v_{ij}. \tag{4}$$

Критерий минимаксного риска Сэвиджа предполагает, что оптимальной является та стратегия игрока, при которой величина риска для него в наихудшем случае минимальна.

4. Проведение второго этапа биматричной игры для уточнения лучших стратегий игроков

Рассмотрим на простом примере второй этап решения биматричной игры для случая, когда на первом этапе были найдены лучшие стратегии x_1, x_2, x_3 для администратора безопасности и y_1, y_2, y_3 – для злоумышленника. Составим из этих стратегий новые платежные матрицы A и B (см. табл. 3 и 4).

Таблица 3. Платёжная матрица A

	y_1	y_2	y_3
x_1	4	**10**	4
x_2	**10**	5	7
x_3	3	5	**10**

Таблица 4. Платёжная матрица B

	y_1	y_2	y_3
x_1	4	9	**2**
x_2	8	**2**	3
x_3	**2**	3	7

Будем считать, что администратор безопасности и атакующий злоумышленник крайне осторожны. Тогда их оптимальные стратегии можно найти из условий минимакса (1) и максимина (2) соответственно. При использовании этих критериев оцениваются значения ячеек платёжных матриц A и B, но, как видно, для рассматриваемой биматричной игры этого оказывается недостаточно для однозначного определения лучших стратегий игроков.

Для того чтобы составить матрицу рисков R администратора безопасности, нужно в каждом столбце его платёжной матрицы A найти наименьшее значение, по очереди вычесть его из всех значений в данном столбце и результат записать в те же позиции (см. табл. 5). Матрица рисков V злоумышленника строится по строкам его платёжной матрицы B. В каждой строке нужно найти наибольшее значение, из этого значения по очереди вычесть все значения в данной строке и результат записать в те же позиции (см. табл. 6).

Таблица 5. Матрица рисков R

	y_1	y_2	y_3
x_1	1	**5**	0
x_2	**7**	0	3
x_3	0	0	**6**

Таблица 6. Матрица рисков V

	y_1	y_2	y_3
x_1	**5**	0	**7**
x_2	0	**6**	5
x_3	**5**	4	0

После этого в каждой строке матрицы рисков R администратора безопасности и каждом столбце матрицы рисков V злоумышленника нужно определить максимальный элемент. Лучшей по критерию Сэвиджа считается та стратегия, для которой этот результат будет наименьшим. В нашем случае, согласно формулам (3) и (4), получается $W_{i_0=1}(R) = 5$ и $W_{j_0=1}(V) = 5$, поэтому лучшими стратегиями для администратора безопасности и атакующего злоумышленника будут x_1 и y_1 соответственно. Таким образом, если администратор безопасности и злоумышленник выберут стратегии x_1 и y_1, то цена игры для каждого них будет по 4 у.е. (см. табл. 3 и 4). Если же выбрать менее удачные согласно критерию Сэвиджа стратегии, например x_2 и y_3, то можно убедиться, что оба игрока сыграют хуже, так как цена игры для администратора безопасности составит 7 у.е. (больший ущерб), а для злоумышленника – 3 у.е. (меньшая прибыль).

5. Заключение

В статье продемонстрировано преимущество решения биматричной игры между администратором безопасности и атакующим злоумышленником в два этапа. Возможность проведения второго этапа игры в большинстве случаев позволяет выявить наиболее выигрышные стратегии игроков среди нескольких с одинаковой ценой игры, найденных на первом этапе. На основе предложенного подхода можно создать программное приложение, которое позволит администратору анализировать и оптимизировать подбор программных средств для построения системы безопасности компании.

Литература

1. Гуц А.К., Вахний Т.В. Теория игр и защита компьютерных систем: учебное пособие. Омск: Изд-во ОмГУ, 2013.

2. 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.
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. Шевченко Д.В. Методы принятия управленческих решений: задания и метод. указания для выполнения расчёт.-граф. работы. Казань: Познание, 2014.

OPTIMIZING THE CHOICE OF A STRATEGY TO PROTECT AGAINST MALICIOUS ATTACKS BASED ON A RISK-BASED BIMATRIC GAME SOLUTION

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 describes the solution of a bimatric game between a security administrator and an attacking attacker in two stages. At the first stage, it is proposed to apply optimality criteria that take into account the price of the game, and at the second stage, criteria that take into account the risks of the players. This approach helps to find the best strategy to protect against malicious attacks among strategies with the same price of the game.

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

Дата поступления в редакцию: 27.02.2024