Математические структуры и моделирование 2023. № 3 (67). С. 111–120

УДК 519.83:004.056
DOI 10.24147/2222-8772.2023.3.111-120

РЕШЕНИЕ БИМАТРИЧНОЙ ИГРЫ С ПРИМЕНЕНИЕМ РАЗЛИЧНЫХ КРИТЕРИЕВ ДЛЯ ВЫБОРА СТРАТЕГИЙ 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 описано решение биматричной игры с применением разных критериев для выбора стратегий администратора безопасности и злоумышленника. Анализ результатов подобных расчётов может быть полезен в вопросах оптимизации защиты компьютерной системы.

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

1. Введение

В последние несколько лет вопросы кибербезопасности чрезвычайно важны в реализации бизнес-целей различных организаций и учреждений, потеря или изменение информации которых может привести не только к урону их репутации, но и к огромным убыткам или даже прекращению деятельности и банкротству. При этом в мире постоянно увеличивается количество способов атак и средств защиты, в результате чего построение надёжной системы защиты становится всё более сложной задачей. Использование теории игр позволяет обеспечить оптимизацию выбора программных продуктов для построения наилучшей системы безопасности организации при минимизации финансовых затрат [1–4].

Целью администратора безопасности является выбор такой стратегии защиты, которая будет сводить потери от атак к минимуму, а интересы атакующего злоумышленника часто в расчёт не принимаются, и предполагают, что его цель прямо противоположная – нанести наибольший ущерб компьютерной системе. Поэтому для анализа их взаимодействия обычно составляют одну общую платёжную матрицу и находят решение матричной игры. Но игра, в которой выигрыш одного игрока – это проигрыш другого, т. е. игра с нулевой суммой, не всегда адекватно отражает ситуацию противостояния администратора безопасности и злоумышленника. У них разные меры ценности информации и представления об успехе. Поэтому полезно проводить не только матричные, но и биматричные игры, в которых выигрыши задаются отдельными платёжными матрицами для каждого игрока [1, 5].

В данной статье для нахождения наиболее оптимальных вариантов защиты компьютерной системы предлагается построить биматричную игру администратора безопасности со злоумышленником и решать её, используя для выбора стратегий игроков разные критерии [3, 6].

2. 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 не являются противоположными, а выигрыши задаются платёжными матрицами отдельно для каждого игрока [1, 2]. 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 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 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 злоумышленника – 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 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:

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

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. Решение биматричной игры сводится к отысканию равновесных (оптимальных) стратегий игроков [1].

3. Критерии для выбора стратегий администратора

Во время построения системы защиты и после её внедрения администратору безопасности необходимо постоянно анализировать новости, которые касаются атак на компьютерные системы, уметь выделять новые угрозы и оценивать риски, связанные с этими угрозами, а также из огромного количества современных средств защиты выбирать наиболее подходящие для понижения риска потери конфиденциальности, целостности и доступности информации. При этом он стремится выбрать такую стратегию, которая позволит свести к минимуму наносимый компьютерной системе ущерб от реализации тех или иных угроз.

Поставим в соответствие каждой i-й стратегии администратора безопасности число $W_i(A)$, вычисляемое с помощью его платёжной матрицы A. Критерий выбора оптимальной стратегии для администратора состоит в том, чтобы взять $W_{i_0} = \min\limits_i W_i(A)$. Для нахождения числа $W_i(A)$ можно использовать различные критерии к выбору наиболее подходящей стратегии администратора [3].

Поскольку при неудачном выборе стратегии ущерб от атаки злоумышленника может оказаться существенным или фатальным для организации, то от администратора безопасности следует ожидать прежде всего осмотрительное поведение, изучение существующих угроз безопасности и интерес к тому, какие из них наиболее часто реализуются. При таком подходе для выбора наилучшей стратегии администратора безопасности подойдут критерии Вальда, Байеса, Лапласа и Сэвиджа [6].

1) Критерий крайнего пессимизма Вальда ориентирует игрока на самые неблагоприятные для него условия и, следовательно, на крайне осторожное поведение при выборе стратегии. Согласно этому критерию за оптимальную принимается такая стратегия, которая в наихудших условиях гарантирует минимальный ущерб от атаки злоумышленника. Следовательно, согласно критерию Вальда $W_i(A) = \max\limits_j a_{ij}$, и администратор безопасности выбирает такую стратегию, при которой наибольший ущерб от атаки является наименьшим среди всех возможных стратегий защиты. То есть по критерию Вальда оптимальной для администратора безопасности будет стратегия, определяемая **из условия минимакса** [1]:

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

Выбирая стратегию по критерию Вальда, можно твёрдо рассчитывать на полученный при её определении результат даже при самом плохом стечении обстоятельств. Критерий Вальда уместен в тех случаях, когда администратор безопасности не столько хочет, чтобы ущерб компьютерной системе был самым минимальным из возможных, сколько не хочет, чтобы он оказался огромным.

2) Критерий математического ожидания Байеса предполагает, что администратору безопасности известны вероятности p_j, с которыми злоумышленник применяет свои стратегии. Полагают, что $W_i(A) = \sum\limits_j p_j a_{ij}$, и оптимальной является стратегия администратора, при которой:

$$W_{i_0}(A) = \min_i W_i(A) = \min_i \sum_j p_j a_{ij}. \tag{2}$$

Вероятности реализации атак p_j могут быть определены по результатам статистических исследований. Можно изучить статистику хакерских атак за определённый промежуток времени, например по данным портала Sicherheitstacho (https://www.sicherheitstacho.eu/start/main). Также полезно установить систему обнаружения хакерских атак (IDS), которая позволит самостоятельно набрать статистику, с помощью которой можно выявить наиболее распространённые типы атак и вычислить вероятности p_j стратегий злоумышленника [4].

Использование критерия Байеса позволяет повысить значимость защиты компьютерной системы от наиболее частых атак. Такая стратегия может хорошо подойти для ситуаций многократной повторяемости, когда лучший средний результат приведёт к лучшему общему итогу.

3) Критерий недостаточного основания Лапласа можно использовать администратору безопасности при наличии неполной информации о вероятностях реализации атак или одинаковых вероятностях всех стратегий злоумышленника. Если

предположить, что все атаки равновероятны, т. е. $p_j = 1/M$, где M – количество стратегий атакующего злоумышленника, то от критерия Байеса перейдём к критерию Лапласа. Согласно критерию Лапласа $W_i(A) = \frac{1}{M}\sum\limits_j a_{ij}$, и для администратора безопасности оптимальная стратегия может быть определена следующим образом:

$$W_{i_0}(A) = \min_i W_i(A) = \frac{1}{M}\min_i \sum_j a_{ij}. \tag{3}$$

Использование критерия Лапласа оправдано, если минимизация риска представляется менее существенным фактором принятия решения, чем минимизация среднего ущерба от атак.

4) Критерий Сэвиджа (минимального максимального риска) основан на применении в расчётах матрицы (таблицы) рисков. Матрица рисков для администратора безопасности 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 рассчитывают по формуле: $r_{ij} = a_{ij} - \min\limits_j a_{ij}$. Они показывают, на сколько больше может быть ущерб компьютерной системе, по сравнению с минимально возможным значением, для каждого типа атаки злоумышленника из-за неверного выбора стратегии защиты. Далее в каждой строке матрицы рисков определяется наибольший результат (максимальный элемент в строке). Лучшей по критерию Сэвиджа считается та стратегия, для которой этот результат наименьший:

$$W_{i_0}(A) = \min_i W_i(A) = \min_i \max_j r_{ij}. \tag{4}$$

Критерий Сэвиджа наиболее соответствует ситуации, в которой администратору важнее не рисковать, нежели гнаться за минимально возможным ущербом от атаки в надежде на неудачный выбор стратегии злоумышленника.

4. Критерии для выбора стратегий злоумышленника

Скорее всего злоумышленник осуществляет атаку на компьютерную систему с целью извлечь из этого какую-то выгоду, при этом он может рисковать, так как в любом случае администратор безопасности не может 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. Единственное, что может его немного останавливать в игре, так это материальные затраты на новые программные средства для атаки. Поэтому для выбора стратегии игры злоумышленника лучше подойдёт другой набор критериев, нежели тот, который был у администратора безопасности [6].

1) Критерий крайнего пессимизма Вальда может выбрать злоумышленник, если он ориентируется на самые неблагоприятные условия, т. е. стремится максимизировать свой возможный минимальный выигрыш. В таком случае его оптимальную стратегию 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, тогда критерий выбора оптимальной стратегии y_{j0} для злоумышленника состоит в том, чтобы взять:

$$W_{j_0}(B) = \max_j W_j(B) = \max_j \min_i b_{ij}. \tag{5}$$

Максиминная стратегия злоумышленника уместна в тех случаях, когда он не столько хочет выиграть, сколько не хочет проиграть, т. е. когда ему нужен гарантированный положительный результат даже при самых неблагоприятных условиях игры.

2) Критерий крайнего оптимизма наилучшим образом подходит для ситуации, в которой злоумышленник настроен крайне оптимистично и рассчитывает на наибольший успех. Этот критерий хорошо подходит для азартного злоумышленника, так как для него обычно потери в игре мало значимы, и он может запросто «рискнуть» понадеяться на самый крупный выигрыш из-за неудачной стратегии защиты компьютерной системы организации.

В критерии крайнего оптимизма для каждой стратегии злоумышленника по платёжной матрице B определяется наибольший достижимый результат как максимальный элемент в столбце $W_j(B) = \max_i b_{ij}$. Лучшей по критерию оптимизма считается та стратегия, для которой этот результат наибольший:

$$W_{j_0}(B) = \max_j W_j(B) = \max_j \max_i b_{ij}. \tag{6}$$

Применение критерия крайнего оптимизма редко позволяет получить максимально возможный выигрыш, но злоумышленник может себе позволить такую стратегию игры.

3) Критерий пессимизма-оптимизма Гурвица является регулируемым компромиссом между критериями крайнего пессимизма и крайнего оптимизма. Согласно этому критерию стратегию игры злоумышленника можно определить следующим образом:

$$W_{j_0}(B) = \max_j(c \cdot \min_i b_{ij} + (1-c) \cdot \max_i b_{ij}), \tag{7}$$

где c – коэффициент пессимизма, который может принимать любые значения от 0 до 1.

Значение $c = 1$ соответствует крайнему пессимизму для злоумышленника, в таком случае уравнение (7) преобразуется к условию максимина (5). Значение $c = 0$ соответствует крайнему оптимизму (критерий азартного игрока), когда злоумышленником делается ставка на самый большой возможный выигрыш, и уравнение (7) преобразуется в уравнение (6). Коэффициент пессимизма выбирается из субъективных соображений администратора безопасности.

4) Критерий минимального риска может быть использован для выбора стратегии злоумышленника, если он не стремится к случайному наибольшему выигрышу. Матрица рисков для злоумышленника строится по строкам 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: $r_{ij} = \max\limits_{i} b_{ij} - b_{ij}$, они показывают, на сколько меньше может быть выигрыш по сравнению с максимально возможным значением.

Оптимальная стратегия злоумышленника может быть определена не только по минимальному значению среди максимальных значений элементов в столбцах матрицы рисков (по аналогии с тем, как было описано для администратора безопасности):

$$W_{j_0}(B) = \min_j W_j(B) = \min_j \max_i r_{ij}, \tag{8}$$

но и по минимальному в столбцах суммарному значению элементов матрицы рисков:

$$W_{j_0}(B) = \min_j W_j(B) = \min_j \sum_i r_{ij}. \tag{9}$$

Данный критерий для выбора стратегии подходит злоумышленнику, если он не собирается гнаться за максимально возможным выигрышем в надежде на то, что администратор безопасности выберет неудачную стратегию защиты.

5. Решение биматричной игры при задании у игроков разных критериев выбора оптимальной стратегии

Рассмотрим решение биматричной игры с платёжными матрицами небольшого размера при использовании для игроков разных критериев выбора оптимальной стратегии. 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 условных единиц (у.е.), 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.

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) при выборе стратегии защиты $x_i (i = 1, \ldots, 7)$ и способа атаки $y_j (j = 1, \ldots, 3)$.

Таблица 3. Платёжная матрица A

	y_1	y_2	y_3
x_1	**10**	11	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

Найдём решение биматричной игры, используя для выбора оптимальной стратегии администратора **критерий Сэвиджа** (4), а для выбора стратегии злоумышленника – **критерий крайнего оптимизма** (6).

Для того чтобы составить матрицу рисков администратора, нужно в каждом столбце его платёжной матрицы A найти наименьшее значение (см. в табл. 3), по очереди вычесть его из всех значений в данном столбце и результат записать в те же позиции (см. табл. 5). После этого в каждой строке матрицы рисков нужно определить максимальный элемент. Лучшей по критерию Сэвиджа считается та стратегия, для которой этот результат наименьший. В нашем случае $W_{i_0}(A) = 1$ и наилучшей стратегией администратора безопасности будет x_5, которая заключается в использовании программных средств x_1 и x_3.

Таблица 5. Матрица рисков

	y_1	y_2	y_3
x_1	0	**8.9**	**8.9**
x_2	15	112.9	**122.9**
x_3	**6**	0	5
x_4	5	**13.9**	**13.9**
x_5	**1**	0	0
x_6	**11**	5	10
x_7	**6**	5	5

Согласно критерию крайнего оптимизма для каждой стратегии злоумышленника по платёжной матрице B нужно определить наибольший достижимый результат как максимальный элемент в столбце (см. табл. 4), и лучшей считается та стратегия, для которой этот результат наибольший. В нашем случае $W_{j_0}(B) = 127$ и наилучшей

стратегией злоумышленника будет стратегия y_3, которая заключается в использовании программных средств y_1 и y_2.

Таким образом, если администратор безопасности и злоумышленник выберут 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).

Для проведения биматричной игры между администратором безопасности и атакующим злоумышленником с платёжными матрицами больших размеров удобно создать и использовать программный продукт, в котором реализована возможность задавать критерии для выбора стратегий игроков [3]. Тогда по введённым значениям стоимости средств защиты и ущерба от применения всех возможных пар «атака – защита» можно будет рассчитывать как оптимальный набор средств защиты компьютерной системы, так и наиболее выигрышную стратегию злоумышленника.

6. Заключение

В статье продемонстрировано решение биматричной игры между администратором безопасности и злоумышленником, когда для каждого игрока применялся свой критерий выбора оптимальной стратегии. На основе предложенного подхода можно создать программное приложение, которое позволит администратору безопасности более тонко учитывать различные нюансы при выборе программных продуктов для построения наиболее надёжной системы защиты при минимизации финансовых затрат на их приобретение.

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., Вахний С.В. Итеративное решение биматричной игры для оптимизации защиты компьютерной системы // Математические структуры и моделирование. 2022. № 1 (61). С. 105–114.
3. 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.
4. 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.
5. Кремлев А.Г. Основные понятия теории игр : учебное пособие. Екатеринбург : Изд-во Ур. ун-та, 2016. 144 с.
6. Шевченко Д.В. Методы принятия управленческих решений : задания и методические указания для выполнения расчётно-графической работы. Казань : Познание, 2014. 69 с.

THE SOLUTION OF A BIMATRIC GAME USING VARIOUS CRITERIA FOR CHOOSING THE STRATEGIES 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 describes the solution of a bimatric game using different criteria for choosing the strategies of a security administrator and an attacker. Analysis of the results of such calculations can be useful in optimizing the protection of a computer system.

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

Дата поступления в редакцию: 14.08.2023

Авторам

Предоставляемые данные и документы

Автор предоставляет в редакцию:

- рукопись статьи в формате LaTeX (см. требования к оформлению);
- список из трёх экспертов по тематике статьи, давших согласие написать рецензию на представленную работу[1];
- экспертное заключение о возможности открытого опубликования.

Лицензирование

Согласно ГК РФ ст. 1286 лицензионный договор с автором для публикации в периодических изданиях может быть заключён в устной форме. Сам факт получения рукописи статьи редколлегией журнала «Математические структуры и моделирование» является акцептом (принятием) лицензионного договора.

Все статьи в журнале «Математические структуры и моделирование» публикуются под лицензией Creative Commons Attribution 4.0 International (CC-BY). Текст лицензии находится по адресу `https://creativecommons.org/licenses/by/4.0/legalcode`.

Требования к оформлению рукописи

К публикации принимаются рукописи объёмом не более 16 страниц.

Авторам необходимо предоставить следующую информацию на русском и английском языках:

- название статьи;
- список авторов с указанием
  - фамилии, имени и отчества,
  - учёного звания,
  - учёной степени,
  - должности,
  - места работы или учёбы,
  - действующего адреса электронной почты;
- аннотация (абстракт) объёмом от 100 до 250 слов;
- список ключевых слов.

Автор также указывает УДК (универсальный десятичный код) статьи. Его можно подобрать по тематике статьи в справочнике `http://msm.univer.omsk.su/udc/`.

Библиографические ссылки оформляются согласно ГОСТ 7.0.5–2008.

Рукопись статьи представляется в редакцию по электронной почте в двух форматах – pdf и tex. Статья должна быть набрана с использованием макропакета LaTeX и стиля msmb.cls, предоставляемого редакцией `http://msm.univer.omsk.su/files/msmb.zip`. Рекомендуется установить компилятор MiKTeX, так как именно им пользуются в редакции.

Отклонения в оформлении рукописи от приведённых правил позволяют редколлегии принять решение о снятии статьи с публикации. Статья может быть отклонена по причинам несоответствия тематике журнала или в связи с низким уровнем качества научного исследования.

В статье запрещается переопределять стандартные команды и окружения.

Нумеруемые формулы необходимо выделять в отдельную строку.

Нумерация только арабскими цифрами в порядке возрастания с единицы. Нумеровать следует только те формулы, на которые в тексте имеются ссылки.

Запрещается использовать в формулах буквы русского алфавита. Если без них никак не обойтись, то следует использовать команду `\mbox{...}`.

[1] Необходимы полные данные экспертов (место работы, учёная степень, должность), с указанием способа связи с ними (e-mail, телефон). Редколлегия может обратиться к одному из экспертов из предложенного списка с просьбой написать рецензию или может назначить рецензента из собственного списка.