ИГРОВАЯ ЗАДАЧА ВЫБОРА ЗАЩИЩАЕМЫХ ОБЪЕКТОВ И ИССЛЕДОВАНИЕ АЛГОРИТМА ПОИСКА СЕДЛОВОЙ ТОЧКИ НА ОСНОВЕ МОДИФИКАЦИИ МЕТОДА БРАУНА-РОБИНСОНА

Быков А.Ю.[1], Гришунин М.В.[2], Крыгин И.А.[3]

Представлена игровая постановка задачи выбора объектов для защиты и нападения двух игроков с учетом ограниченных ресурсов защитника и нападающего. Постановка задачи является антагонистической игрой с конечными стратегиями, каждый игрок должен решить свою задачу булевого программирования с ограничениями на ресурсы при фиксированном решении другого игрока. Игра может быть сведена к матричной игре большой размерности. Для поиска седловой точки в смешанных стратегиях может быть применен метод Брауна-Робинсона, но он требует явного построения матрицы игры, при большой размерности матрицы ее построение требует много памяти. Предложена модификация метода без явного построения матрицы игры, на начальных шагах алгоритма решается задача булева программирования для каждого игрока, на последующих шагах для снижения вычислительной трудоемкости решение ищется среди найденных ранее решений. В качестве критерия завершения решений задач булевого программирования предложено ограничение на число шагов алгоритма, на которых подряд получены не новые решения. В ходе экспериментов выявлено, что максимальное число таких шагов за-висит от числа полученных различных решений алгоритмом, экспериментально получены оценки коэффициента корреляции между этими параметрами. Представлен пример решения задачи.

Ключевые слова: *информационная безопасность, теория игр, матричная игра, игра с нулевой суммой, сме-шанная стратегия, дискретная оптимизация, булевое программирование.*

DOI: *10.21681/2311-3456-2019-2-2-12*

Введение

При решении различных задач защиты информации в условиях ограниченных ресурсов часто используется подход на основе теории игр. Рассмотрим некоторые примеры.

В [1] совместно используются эволюционная теория игр и марковский процесс принятия решений для построения многоступенчатой марковской эволюционной модели игры с целью анализа сетевой атаки и защиты с учетом ограничений. Модель, основанная на некооперативной эволюционной теории игр, может выполнять динамический анализ и дедукцию для многоступенчатого процесса сетевой атаки и защиты. Предложен метод решения многоступенчатого игрового равновесия на основе расчета одноступенчатого эволюционного игрового равновесия. Приведен алгоритм поиска оптимальной стратегии защиты многоступенчатых эволюционных игр.

В [2] рассматривается теоретико-игровая совместная оптимизация соотношения качества обслуживания сети QoS (quality of service) и безопасности в мобильных сетях. Игроками являются мобильное пользовательское оборудование и обслуживающие его базовые станции. Таким образом, пользовательское оборудование получает сбалансированный набор QoS и уровней безопасности, в то время как базовые станции максимизируют использование своих полос пропускания.

В [3] рассматриваются расширенные постоянные угрозы (Advanced persistent threats – APTs) и применяется кумулятивная теория перспектив (cumulative prospect theory – CPT) для изучения взаимодействия между киберсистемой и атакующим. Каждый из них принимает субъективные решения, выбирая свой интервал сканирования и интервал атаки. Используется показатель ожидаемой полезности при неопределенной продолжительности атаки в игре с чистой стратегией нападающего и смешанной стратегией защитника. Получены равновесия по Нэшу в игре обнаружения APTs.

В [4] рассматривается процесс защиты от сетевых атак в режиме реального времени с учетом случайных факторов. Используются совместно модели дифференциальных игр и марковский метод принятия решений. В качестве критерия принятия решений используется многоступенчатое равновесие игры, разработан оптимальный алгоритм выбора стратегии защиты.

В [5] используется модель игры для идентификации источника данных с последовательностью обучающих данных, в которой часть данных повреждена злоумышленником. Защитник стремится решить, была ли создана тестовая последовательность некоторым дискретным источником без памяти, статистика которого ему известна благодаря наблюдению обучающей последовательности. Злоумышленник может тестовую последовательность изменить. Рассматривается поиск равновесного состояния, проводится анализ предельной различимости любых двух источников в зависимости от допустимого искаже-

1 Быков Александр Юрьевич, доцент, кандидат технических наук, МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: abykov@bmstu.ru

2 Гришунин Максим Вадимович, аспирант МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: grishunin-mv@ya.ru

3 Крыгин Иван Александрович, аспирант МГТУ им. Н.Э. Баумана, Москва, Россия. E-mail: krygin.ia@gmail.com

ния и доли поврежденных выборок, введенных в обучающую последовательность.

Работа [6] посвящено тому, как пользователя социальной сети стимулировать защищать свои конфиденциальные данные с помощью настроек безопасности профиля. Предложена теоретическая игровая структура для моделирования взаимодействия пользователей, которое влияет на решения пользователей использовать настройки безопасности. Для моделирования отношений между сообществами пользователей вводится эволюционная динамика, в которой взаимодействия пользователей могут происходить только среди тех пользователей, у которых есть хотя бы одно общее сообщество. Анализируется выбор пользовательских стратегий, заключающийся в том, чтобы использовать особую защиту или нет, на основе предложенной теоретической структуры эволюционной игры внутри сообщества.

В [7] исследуется облачная федерация (Cloud federation) – объединение провайдеров для удовлетворения растущих волн спроса на их ресурсы и услуги. Могут существовать недобросовестные провайдеры, которые присоединяются к федерациям, чтобы уничтожить их изнутри или исключить некоторых сильных конкурентов. В модели игры используется принцип максимина, для обнаружения недобросовестных провайдеров администратором, ответственным за создание и управление федерациями. Недобросовестные провайдеры стараются минимизировать возможность их обнаружения.

В [8] рассматриваются стратегии защиты от фишинговых атак с учетом стоимости их реализации. Рассматривается игра, в которой защитник выбирает стратегии защиты, а нападающий стратегии нападения. Учитывается как возможный ущерб от атак, так и стоимость реализации стратегий защиты.

В [9] теория игр применяется для относительно новых периферийных вычислений мультисервисного доступа (multiaccess edge computing – MEC) применительно к беспроводным сетям. MEC предлагает облачные сервисы на периферии сети, стремясь уменьшить задержку обслуживания и повысить другие показатели, например, безопасность. Рассматриваются игры многих игроков с разными интересами. В статье приводится обзор различных моделей подобных игр.

В [10] рассматриваются вопросы безопасности в социальных сетях. Для экономического анализа используется статическая теория игр для анализа конечных стратегий, используемых атакующим и защитником, где оба участника стремятся оптимизировать ущерб и свои затраты на атаку/защиту. В рамках динамического подхода используется цепь Маркова для разработки динамической модели дерева атаки-защиты, позволяющей на каждую атаку предложить соответствующую контрмеру.

В [11] рассматривается игра защитника и нападающего с разными показателями и с учетом их выигрышей и затрат, при решении происходит упрощение и игра сводится к матричной игре. Используются принципы принятия решений максимин и минимакс, ищется седловая точка в чистых стратегиях, если она существует.

В [12] содержится обзор публикаций по использованию теории игр в информационной безопасности. Рассматриваются задачи: выбор оптимальной стратегии защиты узловой системы обнаружения вторжений, выбор оптимального набора средств защиты для информационной системы, выбор средств защиты от DoS и DDoS атак, обеспечение безопасности в мобильных сетях MANET, распределение ресурсов между объектами в распределенной информационной системе, поиск оптимального набора средств защиты информации для информационной системы. Для каждого случая предлагаются свои модели.

В [13] предложена игра многих игроков: пользователи СЗИ и нарушители, модель носит общий характер, алгоритмы решения не предложены.

В [14] рассматриваются стохастические игровые ситуации с участием двух сторон, преследующих противоположные цели. Принимаемые решения направлены на достижение максимальной полезности, учитываются информированности игроков, предлагается принцип гарантированного результата.

В [15] приведен обзор литературы по игровым моделям, применяемым для моделирования обманных систем, например, когда незаконный сервер маскируется под законный.

Ниже рассмотрим дискретную игровую задачу с нулевой суммой выбора объектов для защиты или выбора защищаемых активов, нападающий выбирает эти же объекты или активы для проведения атак. Подобные задачи в непрерывной форме были представлены в [16, 17]. При этом каждый игрок решает свою задачу математического программирования, системы ограничений задают ограничения на ресурсы игроков.

Похожая задача в дискретной форме представлена в [18], но было введено только одно ограничение – ограничение на стоимость защиты и нападения, и не ставилась задача поиска седловой точки. Впервые рассматриваемая в статье задача представлена в [19], кратко изложены основы алгоритма. В дискретной игровой задаче каждый игрок должен решать свою задачу булевого программирования с ограничениями на ресурсы. В общем виде точные алгоритмы решения подобных задач имеют экспоненциальную трудоемкость. В [20] рассматривают некоторые аспекты экспоненциальных алгоритмов применительно к криптографии. Описанная ниже модификация алгоритма направлена на снижение вычислительной трудоемкости решения задачи.

1. Постановка задачи выбора игроками объектов или активов для атаки и для защиты

1.1. Исходные данные

$Z=\{z_1,z_2,\ldots,z_m\}$ – множество защищаемых объектов или активов, $M=\{1,2,\ldots,m\}$ – множество индексов этих объектов.

$R=\{r_1,r_2,\ldots,r_l\}$ – множество ограниченных ресурсов стороны защиты, $L=\{1,2,\ldots,l\}$ – множество индексов этих ресурсов.

$N=\{n_1,n_2,\ldots,n_s\}$ – множество ограниченных ресурсов стороны нападения, $S=\{1,2,\ldots,s\}$ – множество индексов этих ресурсов.

Параметры элементов множеств и отношений между ними

Таблица 1.

Возможный вариант представления матрицы игры

Решения нападающего	Решения защитника					
	[1,1,0,0,0]	[1,0,1,0,0]	[1,0,0,0,1]	[0,1,1,0,0]	[0,1,0,0,1]	[0,0,0,1,1]
[1,0,0,0,1]	1660	1660	593	3190	2120	2120
[0,1,0,0,0]	385	3740	3740	385	385	3740
[0,0,1,1,0]	5940	2990	5940	2990	5940	4730
[0,0,0,1,1]	3330	3330	2260	3330	2260	1060

$w_i \geq 0,\ \forall\, i \in M$ – возможный ущерб при нарушении безопасности i-го защищаемого объекта (стоимость объекта).

$p_{пр\,i} \in [0,1], \forall i \in M$ – вероятность (или возможность) предотвращения атаки на i-ый объект при его защите.

$a_{ki} \geq 0, \forall k \in L, i \in M$ –значение k-го ограниченного ресурса, используемого для обеспечения защиты i-го объекта.

$b_k \geq 0, \forall k \in L$ – максимальное значение k-го ограниченного ресурса, выделенное на защиту.

$c_{ki} \geq 0, \forall k \in S, i \in M$ –значение k-го ограниченного ресурса стороны нападения, используемого для атаки на i-ый объект.

$d_k \geq 0, \forall k \in S$ – максимальное значение k-го ограниченного ресурса стороны нападения, выделенного на проведение атак.

Ограниченными ресурсами могут быть денежные средства, выделяемые на защиту или нападение, вычислительные ресурсы, ресурсы оперативной памяти и другие ресурсы, могут измеряться в различных единицах измерения, в том числе, в нормированных единицах.

1.2. Искомые параметры

Введем переменную $x_i \in \{0,1\}, \forall i \in M$, $x_i = 1$, если i-й объект защищается защитником, $x_i = 0$ - в противном случае. Переменные образуют вектор $X = [x_1, x_2, ..., x_m]^T$. Для стороны нападения введем переменную $y_i \in \{0,1\}, \forall i \in M$, $y_i = 1$ если i-й объект подвергается атаке нападающим, $y_i = 0$ - в противном случае. Переменные образуют вектор $Y = [y_1, y_2, ..., y_m]^T$.

1.3. Показатели игроков

Для игры с нулевой суммой показатели качества двух игроков определяются ущербом стороны защиты. Средний ущерб

$$U(X,Y) = U_{max}(Y) - U_{np}(X,Y) = \sum_{i \in M} w_i y_i - \sum_{i \in M} p_{pr\,i} w_i x_i y_i, \quad (1)$$

где $U_{max}(Y) = \sum_{i \in M} w_i y_i$ – максимальный ущерб, который может быть нанесен стороной нападения при отсутствии защиты;

$U_{np}(X,Y) = \sum_{i \in M} p_{pr\,i} w_i x_i y_i$ – предотвращенный ущерб стороной защиты.

Сторона защиты желает этот показатель минимизировать, а сторона нападения максимизировать. Каждый из игроков решает задачу линейного булевого программирования при фиксированном решении другого игрока.

1.4. Ограничения

Система ограничений на использование ограниченных ресурсов стороной защиты, задающая множество допустимых альтернатив , имеет вид:

$$\Delta_{don}^{(x)} : \left\{ \sum_{i \in M} a_{ki} x_i \leq b_k, \forall k \in L \right. \quad (2)$$

Система ограничений на использование ограниченных ресурсов стороной нападения, задающая множество допустимых альтернатив , имеет вид:

$$\Delta_{don}^{(y)} : \left\{ \sum_{i \in M} c_{ki} y_i \leq d_k, \forall k \in S \right. \quad (3)$$

Будем полагать, что системы ограничений (2) и (3) не позволяют выбрать защитником и нападающим решения, состоящее из всех единиц (полная защита или полное нападение), так как в этом случае, такие решения являются оптимальными, и задача становится тривиальной.

2. Алгоритмы решения задачи

2.1. Прямой алгоритм метода Брауна-Робинсона

Построим платежную матрицу игры в явном виде. Для этого необходимо перебрать все допустимые решения защитника, удовлетворяющие ограничениям (2), и все допустимые решения нападающего, удовлетворяющие ограничениям (3). Пусть решения защитника в матрице задают столбцы, а решения нападающего задают строки. Элементами матрицы являются значения показателя (1) в условных единицах при заданных решениях защитника и нападающего. Например, если размерности векторов и равны 5, возможный вариант матрицы представлен в (табл.1).

Для сокращения матрицы игры можно сразу исключить доминируемые строки и столбца. Например, если решение нападающего [0,0,0,1,1] является допустимым, то допустимыми являются решения нападающего, получаемые из исходного решения заменой 1 на 0, например, решения [0,0,0,0,1], [0,0,0,1,0], [0,0,0,0,0]. Но эти решения не дадут выигрыш нападающему, больший, чем решение [0,0,0,1,1] при любых решениях защитника, то есть эти решения являются доминируемыми решением [0,0,0,1,1] и их можно исключить из матрицы. Аналогично

можно поступить для защитника. Таким образом, в (табл. 1) присутствуют решения с максимальным числом единиц: в этих решения при замене любого 0 на 1 получаем недопустимое по ограничениям (2) или (3) решение. Решения с максимальным числом единиц для защитника нападающего можно получить различными алгоритмами, например, алгоритмом неполного перебора на основе идей метода Балаша [21], или другими алгоритмами.

При прямом методе Брауна-Робинсона игра состоит их последовательных партий, каждый игрок выбирает чистую стратегию, оптимизирую свой показатель, при этом учитывается усредненный выигрыш другого игрока за все предыдущие ходы. Самый первый ход первый игрок делает произвольно, но рекомендуется по критерию максимина или минимакса в зависимости от игрока. Усредненное значение показателя для защитника (минимакс) определяет верхнюю цену игры, усердное значение показателя для нападающего (максимин) определяет нижнюю цену игры. Критерий остановки – разность между верней и нижней ценами игры меньше заданного небольшого значения, задающего погрешность. Недостаток метода – сходимость приближенных решений к точному решению происходит достаточно медленно. Достоинство – трудоемкость метода при увеличении размеров матрицы игры возрастает незначительно, в отличие от метода сведения игры к задаче линейного программирования.

2.2. Модифицированный алгоритм на основе метода Брауна-Робинсона

В модификации алгоритма не будем строить матрицу игры в явном виде. На каждом из шагов алгоритма будем последовательно решать оптимизационные задачи для защитника и нападающего. При решении оптимизационной задачи для одного из игроков решение другого фиксировано и задает усредненный выигрыш или проигрыш, полученный на предыдущих шагах. Для расчета суммарного выигрыша или проигрыша введем вещественные вектора размерности : . Для расчета среднего решения для игроков будем использовать также вещественные вектора размерности : . Рассмотрим первоначально прямой подход. Решения оптимизационных задач сохраняются в списках решений игроков для последующего расчета частот появления этих решений.

Шаг0.Полагаем $X_{сум}=[0,0,...,0]^T$, $Y_{сум}=[0,0,...,0]^T$, $X_{сред}=[0,0,...,0]^T$ $Y_{сред}=[1,1,...,1]^T$, $k_x=0$ – число полученных решений защитником, $k_y=0$ – число полученных решений нападающим. $Y_{сред}$ – будем считать начальным решением нападающего, это решение является недопустимым. Создаем два списка: список найденных решений защитника и список найденных решений нападающего, изначально эти списки пустые. В списках хранится найденные решения игроков, для каждого найденного решения задан счетчик, содержащий значение сколько раз это решение встретилось.

Шаг i-ый (i=1,3,5 нечетный шаг). Решаем задачу защитника - минимизация показателя (1) при решении нападающего $Y_{сред}$ и ограничениях (2) любым методом дискретного программирования, находит оптимальный вектор $F_з^{(i)}=U\left(X^{(i)},Y_{сред}\right)$ и оптимальное значение показателя , полагаем $k_x=k_x+1$. Если найденное решение находится в списке решений защитника, то счетчик для этого решения увеличивается на 1. Если решения нет в списке, то помещаем его в список, значение счетчика для этого решения равно 1.

$$X_{сум}=X_{сум}+X^{(i)},\ X_{сред}=X_{сум}/k_x.$$

Шаг (i+1)-ый (четный шаг). Решаем задачу нападающего - максимизация показателя (1) при решении защитника $X_{сред}$ и ограничениях (3), находит оптимальный вектор $Y^{(i)}$ и оптимальное значение показателя $F_н^{(i)}=U\left(X_{сред},Y^{(i)}\right)$, полагаем $k_y=k_y+1$. Если найденное решение находится в списке решений нападающего, то счетчик для этого решения увеличивается на 1. Если решения нет в списке, то помещаем его в список, значение счетчика для этого решения равно 1.

$Y_{сум}=Y_{сум}+Y^{(i)},\ Y_{сред}=Y_{сум}/k_y$. Проверяем критерий остановки: если $\left|F_з^{(i)}-F_н^{(i)}\right|<\xi$, то переходим к заключительному шагу, в противном случае полагаем i=i+2 и переходим снова к нечетному шагу.

Шаг заключительный. Для каждого из решений, находящихся в списках защитника и нападающего, определяем частоты их повторений, для этого значение счетчика решения делим на k_x – для защитника и на k_y – для нападающего.

Основной недостаток предложенного алгоритма заключается в том, что на каждом шаге требуется решать задачу булевого программирования для поиска решений для игроков, что требует существенных вычислительных ресурсов. Но, как показали эксперименты, число решений, получаемых алгоритмом, частоты появления которых не равны 0, намного меньше, чем общее число допустимых решений с максимальным числом единиц в матрице игры. Причем новые решения обычно получаются на начальных итерациях алгоритма, потом решения начинают повторяться. Поэтому алгоритм можно модифицировать так. В случае если получено N решений, которые уже есть в списках защитника и нападающего (на N шагах не получено новых решений, возможны разные значения для защитника и нападающего), то задачу булевого программирования можно не решать, а искать решение в существующем списке решений, размерность которого относительно невелика способом перебора.

Ниже рассмотрим эксперименты с применением генераторов псевдослучайных чисел для получения исходных данных, в том числе и для определения N в зависимости от размерности задачи, а также пример решения задачи.

3. Эксперименты и пример решения задачи

3.1. Эксперименты с алгоритмом на исходных данных, полученных с помощью генераторов псевдослучайных чисел

Рассмотрим результаты тестирования алгоритмов на исходных данных, сгенерированных генераторами псевдослучайных чисел (ГПСЧ). В качестве критерия остановки использовалось достижение 0.01 % относительной погрешности в оценке значения показателя качества (от-

Таблица 2.
Результаты экспериментов с алгоритмом задач для исходных данных, полученных ГПСЧ

#№п/п	Число объектов m	Исходная размерность матрицы игры	Размерность матрицы игры после исключения доминируемых строк (столбцов)	Параметры для нападающего			Параметры для защитника			Общее число шагов
				Число решений в списке	Максимальный интервал между новыми решениями	№ шага последнего нового решения	Число решений в списке	Максимальный интервал между новыми решениями	№ шага последнего нового решения	
1	8	50 x 40	27 x 32	17	28	49	17	263	425	796414
	8	35 x 32	26 x31	9	45	59	7	8	16	322978
	8	40 x 31	20 x 30	5	8	13	7	9	16	31298
	10	144 x 136	140 x 136	17	106	252	12	11556	11639	606669
	10	126 x 134	118 x 134	15	182	317	32	986	1832	915478
	10	101 x 129	48 x 66	7	54	91	7	30	45	655536
	15	2237 x 3178	1222 x 3178	28	2406	3191	31	2972	3338	1356679
	15	2740 x 2944	1634 x 2944	42	11595	12423	98	19038	43121	1060669
	15	2085 x 2417	312 x 1223	16	39	126	20	2203	2576	309317
	20	59201 x 82320	———	41	126	395	55	5204	12018	446527
	20	59174 x 78813	———	53	484	1199	53	567	1545	552266
	20	58237 x 56109	———	94	1284	2287	89	12484	16086	260941

ношение модуля разности между показателями игроков к минимальному модулю показателя). Результаты тестирования представлены в (табл. 2), в этой таблице приведены следующие данные:

– число объектов m, для каждого значения m проверено по три испытания с разными исходными данными;
– размерность матрицы игры при получении решений с максимальным числом единиц;
– размерность этой матрицы при исключении доминируемых строк и столбцов путем попарного сравнения их;
– число разных решений, полученных защитником и нападающим (возможно, некоторые решения можно из смешанных стратегий исключить из-за низкой частоты их появления);
– максимальный интервал между полученными новыми решениями для каждого из игроков (интервал измеряется числом шагов алгоритма, на которых были получены решения из существующего списка);
– номер последнего шага алгоритма, на котором получено новое решение для каждого из игроков, которого нет в списке полученных решений;
– общее число шагов алгоритма для достижения заданной точности, под шагом понимается решение двух оптимизационных задач защитником и нападающим (число решений защитника и нападающего для получения заданной точности).

В (табл. 2) для случая, когда число защищаемых объектов 20 (m = 20) матрица игры не построена в явном виде из-за нехватки оперативной памяти, поэтому в столбце с размерностью сокращенной матрицы (путем удаления доминируемых строк и столбцов) данные отсутствуют. Задача булева программирования решалась на каждом шаге методом Балаша [21]. При числе защищаемых объектов 20 (m = 20) время решения составляло порядка нескольких часов (от 1 до 5). Из таблицы видно, что число полученных решений может быть на порядки меньше, чем число допустимых решений.

Рассмотрим способы сокращения времени решения: будем использовать параметр N (отдельно для защитника и нападающего), если на N шагах подряд не было получено новое решение, то задачу булевого программирования не решаем, а ищем максимум или минимум,

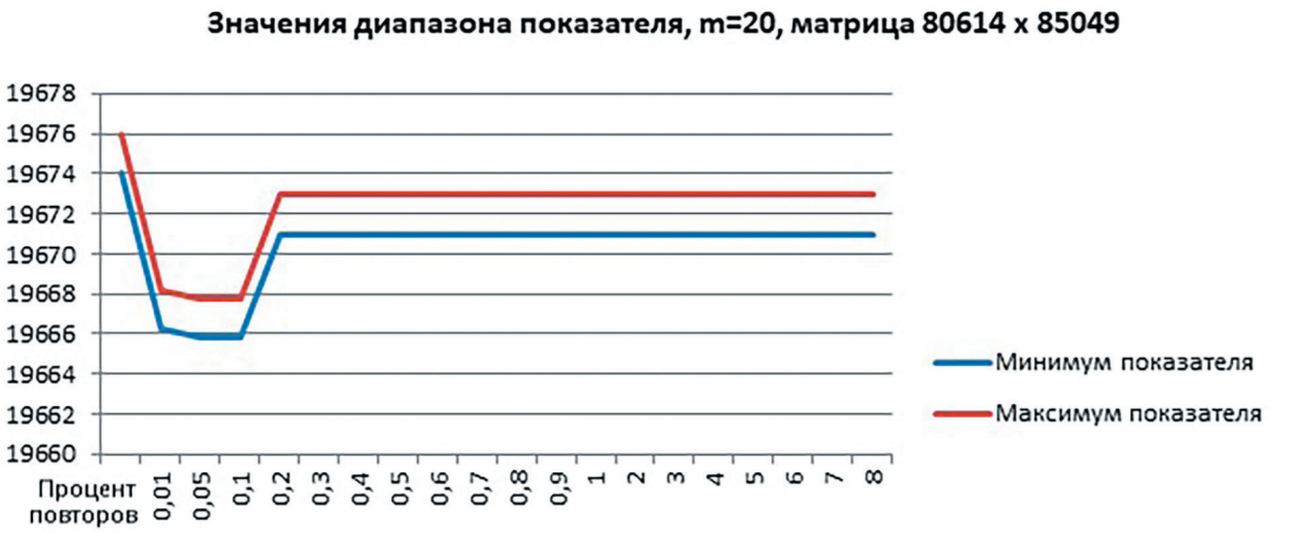

Рис.1. Значения диапазона показателя при m=20, размерность матрицы 80614 x 85049

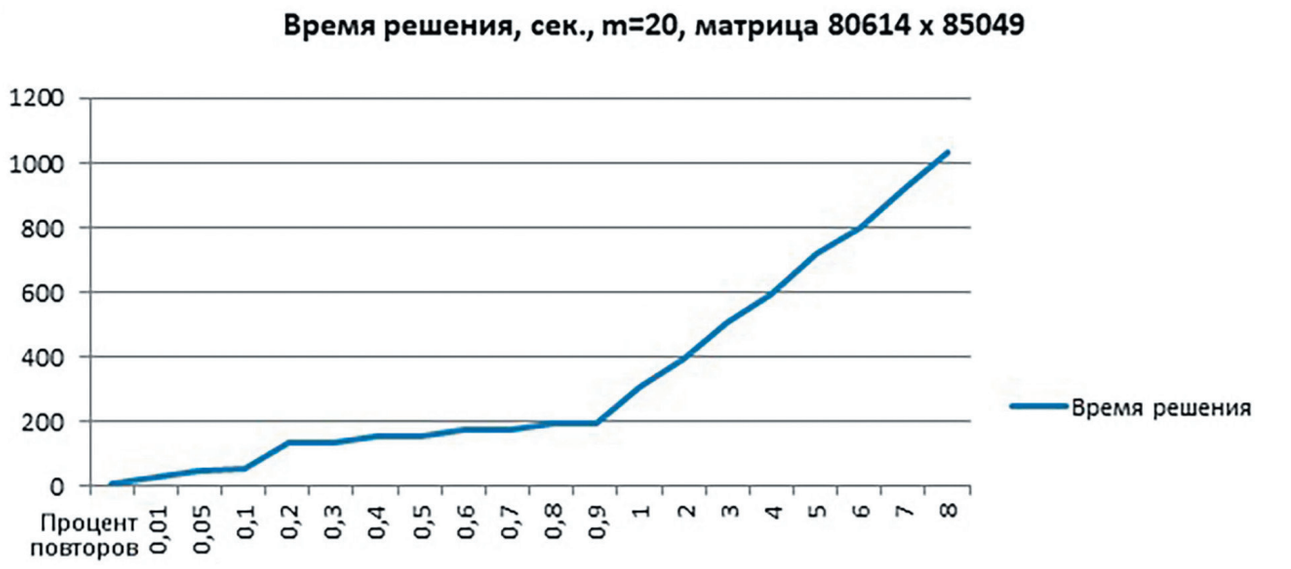

Рис.2. Время решения задачи при m=20, размерность матрицы 80614 x 85049

просматривая список уже найденных решений. Этот параметр связан с максимальным интервалом между новыми решениями, приведенным в (табл. 2) и имеющим существенный разброс. Учитывая данные (табл. 2) и опираясь на здравый смысл, можно предположить, что этот интервал зависит (с большим разбросом) от числа допустимых решений (исходной размерности матрицы игры). Параметр N будем задавать в процентах от числа допустимых решений, если число допустимых решений 1000, процент равен 10, то при 100 случаях подряд получения повторных решений (уже полученных ранее), решение задачи булевого программирования прекращается, поиск решения осуществляется в списке уже полученных решений. Эксперименты проводились на ноутбуке с процессором Intel(R) Core(TM) i3-6006U CPU @ 2.00GHz, 2000 МГц, ядер: 2, логических процессоров: 4, оперативной памятью 4 ГБ, операционная система Windows 10, среда разработки Microsoft Visual Studio, язык программирования Си++. Погрешность в оценке показателя была задана 0.01 %. Исходные данные сформированы с помощью ГПСЧ.

На (рис. 1) представлены значения верхней и нижней оценки показателя качества выбора игроков (значения диапазона показателя) в зависимости от заданного процента повторов для случая, когда m=20. На (рис. 2) представлена зависимость времени решения задачи от процента повторов для этого же случая. Для других размерностей графики имели качественно аналогичный вид.

Из представленных графиков можно сделать вывод о том, что при увеличении параметра N от минимального значения к максимальному, при некотором значении параметра N значения показателя игроков практически перестает изменяться. На начальном этапе значения показателя не стабильно. Из графика зависимости времени решения задач от N можно сделать вывод о том, что вычислительная сложность зависит от N полиномиально, так как общее число решаемых задач булева программирования зависит полиномиально от N.

Проведены эксперименты для проверки зависимости максимального числа повторных решений подряд и числа различных решений, составляющих смешанную стратегию игрока и имеющих оценку вероятности больше 0,

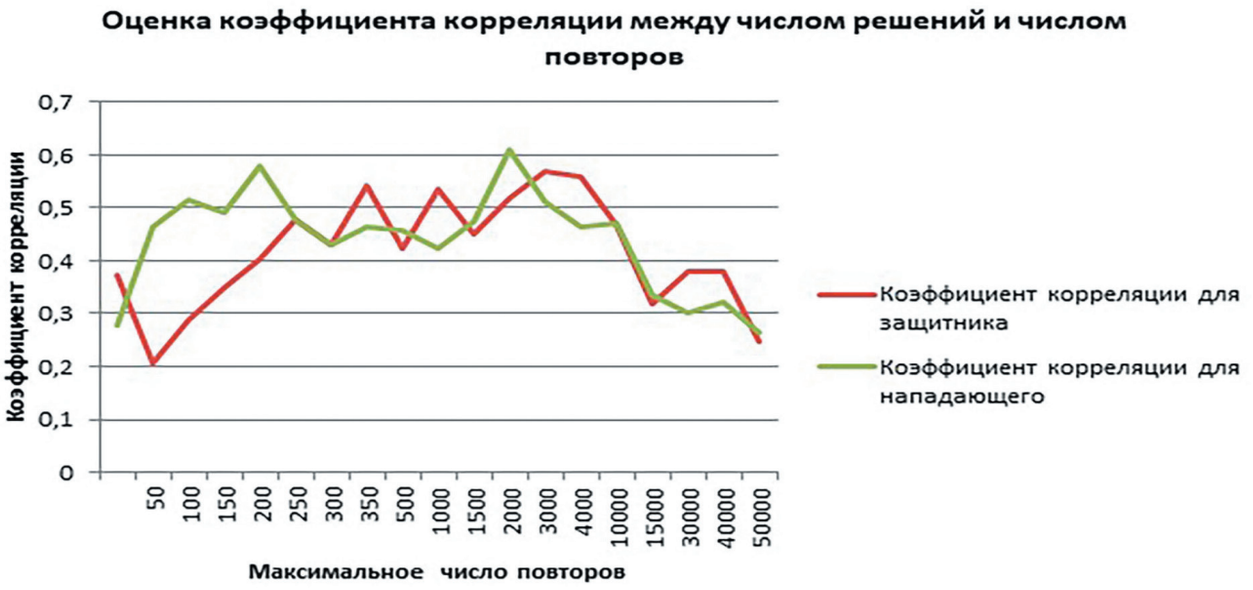

Рис.3. Зависимости оценки коэффициента корреляции между числом решений и максимальным числом повторов от ограничения на максимальное число повторов

т.е. которые были получены алгоритмом. Если исходные данные генерируются с помощью ГПСЧ, то можно рассматривать эти два параметра как случайные величины (псевдослучайные величины в программе). Проводились оценки коэффициента корреляции между максимальным числом повторных решений, получаемым алгоритмом подряд, и числом различных решений, входящих в смешанную стратегию с ненулевой вероятностью. Эксперименты проводились для числа объектов m=10, для получения оценки коэффициента корреляции решались 100 задач с разными исходными данными. При этом было введено ограничение на максимальное число повторов, при достижении которого новое решение искалось в списке существующих решений (полученное алгоритмом максимальное число повторов не может превышать заданное ограничение). На (рис. 3) представлены графики зависимости для защитника и нападающего коэффициента корреляции от ограничения на максимальное число повторов.

Из графиков на (рис. 3) можно сделать вывод о том, что корреляция положительная. При небольшом и, напротив, большом значении ограничения на число максимальных повторов значение коэффициента корреляции снижается. При большом значение ограничения на максимальное число повторов снижение корреляции можно объяснить тем, что новое решение с большим числом повтором появляется не часто, и сразу вносит искажение в расчет из-за относительно большого «выброса». Например, при ограничении 100000, максимальное число повторов в одной задаче для защитника составило 95685, предыдущее максимальное число повторов до появления этого числа было 18, а число различных решений защитника в э той задачи было 13.

Учитывая взаимосвязь максимального числа повторяющихся решений подряд и числа полученных решений с ненулевой вероятностью в смешанной стратегии игрока. Можно предложить следующую модификацию, описанного в подразделе 2.2 алгоритма.

Начальное целое значение $N=\lambda>0$ (отдельно для защитника и нападающего), при появлении каждого нового решения, которого еще не было в списке значение N изменяется: $N=N+\lambda$. Выбор λ зависит от требований точности и наличия вычислительных ресурсов, в большинстве случаях для получения оценок показателя, которые затем при увеличении N практически не изменялись достаточно $\lambda=3$ или $\lambda=4$. Отдельные задачи потребовали $\lambda=7$.

3.2. Пример решения задачи

Рассмотрим пример решения задачи в случае, когда 8 объектов защиты, например, узлов сети. Значения ущерба и вероятности защиты объектов (табл.3).

У защитника и нападающего по 4 вида ресурсов, примеры параметров ограничений для защитника и нападающего (табл.4). Параметры первого ограничения для защитника и нападающего приведены без нормировки, например, это может быть стоимость, остальные параметры

Таблица 3.
Значение ущерба и вероятностей защиты объектов

Номер объекта	1	2	3	4	5	6	7	8
Значения w_i, в у.е.	4000	10000	3000	9000	5000	9500	10000	8000
Значения $p_{пр\,i}$	0.80	0.99	0.70	0.95	0.85	0.90	0.50	0.92

Таблица 4.

Параметры системы ограничений на ресурсы защитника и нападающего

Параметры ограничений защитника									
№ ограничения	Значения коэффициентов в левых частях ограничений для защитника, a_{ki}								Значения b_k
1	100	1000	200	900	400	500	1200	1100	3000
2	0.03	0.30	0.05	0.15	0.30	0.30	0.35	0.10	0.70
3	0.05	0.20	0.20	0.25	0.30	0.10	0.33	0.35	0.60
4	0.01	0.05	0.02	0.05	0.02	0.01	0.01	0.01	0.20
Параметры ограничений нападающего									
№ ограничения	Значения коэффициентов в левых частях ограничений для нападающего, c_{ki}								Значения d_k
1	50	600	60	500	100	120	1000	550	1500
2	0.02	0.20	0.05	0.25	0.35	0.30	0.30	0.15	0.80
3	0.02	0.30	0.30	0.35	0.40	0.15	0.35	0.30	0.80
4	0.15	0.10	0.20	0.05	0.20	0.10	0.10	0.10	0.50

Таблица 5.

Результаты решения задачи точным алгоритмом

№ п/п	Решение	Оценка вероятности
Решения для защитника (значение показателя 15031.8)		
1	1 1 1 0 0 1 0 0	0.472
2	1 0 1 1 0 1 0 0	0.374
3	1 1 0 0 0 0 1 0	0.033
4	1 0 0 0 0 1 1 0	0.120
Решения для нападающего (значение показателя 15031.8)		
1	0 0 0 1 0 0 1 0	0.319
2	1 1 0 0 0 1 0 1	0.319
3	0 0 0 1 0 1 0 1	0.050
4	1 0 0 0 1 0 1 0	0.312

Таблица 6.

Результаты решения задачи предложенным алгоритмом

№ п/п	Решение	Оценка вероятности
Решения для защитника (достигнутое значение показателя 15031.326)		
1	1 1 1 0 0 1 0 0	0.472
2	0 0 0 1 0 0 1 0	0.000
3	1 0 1 1 0 1 0 0	0.349
4	1 0 0 0 0 1 0 1	0.000
5	1 1 0 0 0 0 1 0	0.008
6	1 0 0 0 0 1 1 0	0.146
7	1 1 0 1 0 0 0 0	0.025
Решения для нападающего (достигнутое значение показателя 15032.822)		
1	0 0 0 1 0 0 1 0	0.317
2	1 1 0 0 0 1 0 1	0.318
3	0 0 0 1 0 1 0 1	0.051
4	1 0 0 0 1 0 1 0	0.313

представлены в нормированном виде (значение от 0 до 1), это могут быть ресурсы вычислительных средств, оперативной памяти, ресурсы каналов передачи данных и т.п.

Решение задачи точным методом, основанным на сведении игры к задаче линейного программирования [21], представлены (табл. 5).

Результаты решения задачи предложенным алгоритмом представлены (табл.6). При этом для критерия остановки использовалось достижение 0.01 % относительной погрешности в оценке значения показателя качества.

В (табл.6) некоторые оценки вероятностей решений имеют нулевые значения, это означает, что это решение появлялось на некоторых шагах алгоритма, но оценка вероятности для него менее 0.001, данным решением можно пренебречь, можно также пренебречь решением с вероятностью 0.008, тогда остаются по 4 решения у защитника и нападающего. Решение задачи точным алгоритмом на основе сведения к задаче линейного программирования продемонстрировало подобные результаты. Размер исходной матрицы игры для примера составил 23 × 16, в результате для защитника и нападающего получены по 4 решения, вероятности выбора для которых не равны 0. Эти решения по вероятностям близки с оценками, представленными в (табл.5).

Выводы

Исследована игровая задача выбора объектов (или активов) для защиты защитником и выбора объектов (активов) для атак нападающим. Математическая постановка задачи для каждого из игроков являлась задачей булевого программирования при фиксированном решении другого игрока, задачу можно свести к матричной игре большой размерности. Разработан модифицированный алгоритм поиска решения игры в смешанных стратегиях на основе идей алгоритма Брауна-Робинсона без построения матрицы игры в явном виде, так как при большой размерности потребуется много памяти.

Для снижения вычислительной сложности алгоритма предлагается решать задачи булевого программирования только на начальных шагах алгоритма, на последующих шагах используются результаты, полученные ранее. В качестве критерия завершения решения задач булевого программирования и перехода к поиску решений в списке уже найденных решений методом их перебора предложено использовать превышение некоторого заданного значения числа решений, найденных алгоритмом подряд, которые не являются новыми.

В ходе экспериментов выявлена зависимость между числом получаемых неновых решений подряд и числом полученных разных решений алгоритмом. Предложено максимальное число полученных подряд неновых решений задавать переменным значением, которое линейно зависит от числа полученных новых решений.

Представлен пример решения задачи. Достоверность полученных результатов подтверждается их проверкой решением задачи точным методом, основанным на сведение игры к решению задачи линейного программирования.

Рецензент: *Басараб Михаил Алексеевич, доктор физико-математических наук, профессор МГТУ им.Н.Э.Баумана, bmic@mail.ru*

Литература

1. Jianming Huang, Hengwei Zhang, Jindong Wang. Markov Evolutionary Games for Network Defense Strategy Selection. IEEE Access. 2017. Vol. 5. P. 19505-19516. DOI: 10.1109/ACCESS.2017.2753278
2. Zubair Md. Fadlullah, Chao Wei, Zhiguo Shi, Nei Kato. GT-QoSec: A Game-Theoretic Joint Optimization of QoS and Security for Differ-entiated Services in Next Generation Heterogeneous Networks. IEEE Transactions on Wireless Communications. 2017. Vol. 16. Iss. 2. P. 1037-1050. DOI: 10.1109/TWC.2016.2636186
3. Liang Xiao, Dongjin Xu, Narayan B. Mandayam, H. Vincent. Poor Attacker-Centric View of a Detection Game against Advanced Persistent Threats IEEE Transactions on Mobile Computing. 2018. Vol. 17. Iss. 11. P. 2512-2523. DOI: 10.1109/TMC.2018.2814052
4. Shirui Huang, Hengwei Zhang, Jindong Wang, Jianming Huang. Markov Differential Game for Network Defense Decision-Making Method. IEEE Access. 2018. Vol. 6. P. 39621-39634. DOI: 10.1109/ACCESS.2018.2848242
5. Mauro Barni, Benedetta Tondi. Adversarial Source Identification Game with Corrupted Training. IEEE Transactions on Information Theory. 2018. Vol. 64. Iss. 5. P. 3894-3915. DOI: 10.1109/TIT.2018.2806742
6. Jun Du, Chunxiao Jiang, Kwang-Cheng Chen, Yong Ren, H. Vincent Poor. Community-Structured Evolutionary Game for Privacy Protection in Social Networks. IEEE Transactions on Information Forensics and Security. 2018. Vol. 13. Iss. 3. P. 574-589. DOI: 10.1109/TIFS.2017.2758756
7. Ahmad Hammoud, Hadi Otrok, Azzam Mourad, Omar Abdel Wahab, Jamal Bentahar. On the Detection of Passive Malicious Providers in Cloud Federations. IEEE Communications Letters. 2019. Vol. 23. Iss. 1. P. 64-67. DOI: 10.1109/LCOMM.2018.2878714
8. Xiayang Chen, Xingtong Liu, Lei Zhang, Chaojing Tang. Optimal Defense Strategy Selection for Spear-Phishing Attack Based on a Multi-stage Signaling Game. IEEE Access. 2019. Vol. 7. P. 19907-19921. DOI: 10.1109/ACCESS.2019.2897724
9. José Moura, David Hutchison. Game Theory for Multi-Access Edge Computing: Survey, Use Cases, and Future Trends. IEEE Communications Surveys & Tutorials. 2019. Vol. 21. Iss. 1. P. 260 – 288. DOI: 10.1109/COMST.2018.2863030
10. Suguo Du, Xiaolong Li, Jinli Zhong, Lu Zhou, Minhui Xue, Haojin Zhu, Limin Sun. Modeling Privacy Leakage Risks in Large-Scale Social Networks. IEEE Access. 2018. Vol. 6. P. 17653-17665. DOI: 10.1109/ACCESS.2018.2818116
11. Савченко С. О., Капчук Н. В. Алгоритм построения модели нарушителя в системе информационной безопасности с применением теории игр. Динамика систем, механизмов и машин. 2017. Т. 5. № 4. С. 84-89. DOI: 10.25206/2310-9793-2017-5-4-84-89
12. Цирулева В.М., Кярт А.М. Применение теории игр в информационной безопасности. В сборнике: Математические методы управления Сборник научных трудов. Тверь. 2017. С. 76-90.

13. Кунаковская О.В., Меньших Т.В. Применение методов теории игр к задачам информационной безопасности. Некоторые вопросы анализа, алгебры, геометрии и математического образования. 2016. № 5-1. С. 173-174.
14. Кучер В.А., Тарасов Е.С. Математическое моделирование процессов управления информационной безопасностью автоматизированных систем на основе методов теории игр. Научные труды Кубанского государственного технологического университета. 2016. № 16. С. 244-255.
15. Артюшкин А.С., Ключарёв П.Г. Обзор теоретико-игровых подходов к моделированию обманных систем. В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А.Басараба. 2017. С. 27-29.
16. Быков А. Ю., Шматова Е.С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов. Наука и образование: научное издание. 2015. № 9. DOI: 10.7463/0915.0812283.
17. Быков А.Ю., Крыгин И.А., Муллин А.Р. Алгоритм распределения ресурсов системы защиты между активами мобильного устройства на основе игры с нулевой суммой и принципа равной защищенности. Вестник МГТУ им. Н.Э. Баумана. Приборостроение. 2018. № 2. С. 48- 68. DOI: 10.18698/0236-3933-2018-2-48-68
18. Быков А. Ю., Алтухов Н. О., Сосенко А. С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры. Инженерный вестник МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 4. Режим доступа: http://engbul.bmstu.ru/doc/708106.html
19. Быков А.Ю., Крыгин И.А., Гришунин М.В. Алгоритм поиска седловой точки в смешанных стратегиях на основе модификации метода Брауна-Робинсона для решения задачи выбора защищаемых объектов. В сборнике: Безопасные информационные технологии Сборник трудов Девятой всероссийской научно-технической конференции. 2018. С. 33-38.
20. Ключарев П.Г. Квантовые вычисления и атаки на криптоалгоритмы, основанные на обобщенных клеточных автоматах. В сборнике: Безопасные информационные технологии Сборник трудов Восьмой всероссийской научно-технической конференции. НУК «Информатика и системы управления». Под. ред. М.А. Басараба. 2017. С. 234-236.
21. Басараб М.А., Вельц С.В. Методы оптимизации и исследование операций в области информационной безопасности: Методические указания к выполнению лабораторных работ по дисциплине «Методы оптимизации и исследования операций». М.: МГТУ им. Н.Э. Баумана, 2015. 64 с. Режим доступа: http://ebooks.bmstu.press/catalog/117/book967.html

THE GAME PROBLEM OF SELECTION OF ASSETS TO PROTECT AND RESEARCH OF SADDLE POINT SEARCH ALGORITHM BASED ON BROWN-ROBINSON METHOD MODIFICATION

Bykov A.Yu., Grishunin M.V., Krygin I.A.

Abstract. In this paper it is presented a game statement of assets to protect and attack selection problem of two players with attacker and defender limited resources. The game statement is a zero-sum game with finite strategies, each player must solve his own boolean programming problem with resource limitation and fixed another player solution. The game can lead to large dimension matrix game. To find a saddle point in mixed strategies Brown-Robinson method can be applied, but it requires explicit game matrix construction. With a large dimension of a matrix its construction requires a lot of memory. It is suggested a method modification without explicit game matrix construction. At start steps of algorithm, the boolean programming problems is solved for each player. At the next steps the solution is searched from already searched solutions to reduce computational complexity. A limitation of algorithm steps, on which the same values were given in a row, is suggested to be a criterion of completion of boolean programming problem solving. Experiments revealed, that the max amount of such steps depends on amount of various solutions. Estimation of correlation coefficient between these parameters was given experimentally. The problem solution example is presented.

Keywords: *information security, game theory, matrix game, zero-sum game, mixed strategy, discrete optimization, boolean programming.*

References

1. Jianming Huang, Hengwei Zhang, Jindong Wang. Markov Evolutionary Games for Network Defense Strategy Selection. IEEE Access, 2017, vol. 5, pp. 19505-19516. DOI: 10.1109/ACCESS.2017.2753278

4 Aleksandr Bykov, Associated Professor, Ph.D., Associated Professor at Bauman Moscow State Technical University, Moscow,Russia. E-mail: abykov@bmstu.ru
5 Maxim Grishunin, Graduate student of Bauman Moscow State Technical University Moscow, Russia. E-mail: grishunin-mv@ya.ru
6 Ivan Krygin, Graduate student of Bauman Moscow State Technical University, Moscow, Russia. E-mail: krygin.ia@gmail.com

2. Zubair Md. Fadlullah, Chao Wei, Zhiguo Shi, Nei Kato. GT-QoSec: A Game-Theoretic Joint Optimization of QoS and Security for Differ-entiated Services in Next Generation Hetero-geneous Networks. IEEE Transactions on Wireless Communications, 2017, vol. 16, iss. 2, pp. 1037-1050. DOI: 10.1109/TWC.2016.2636186
3. Liang Xiao, Dongjin Xu, Narayan B. Mandayam, H. Vincent. Poor Attacker-Centric View of a Detection Game against Advanced Persistent Threats IEEE Transactions on Mobile Computing, 2018, vol. 17, iss. 11, pp. 2512-2523. DOI: 10.1109/TMC.2018.2814052
4. Shirui Huang, Hengwei Zhang, Jindong Wang, Jianming Huang. Markov Differential Game for Network Defense Decision-Making Method. IEEE Access, 2018, vol. 6, pp. 39621-39634. DOI: 10.1109/ACCESS.2018.2848242
5. Mauro Barni, Benedetta Tondi. Adversarial Source Identification Game with Corrupted Training. IEEE Transactions on Information Theory, 2018, vol. 64, iss. 5, pp. 3894-3915. DOI: 10.1109/TIT.2018.2806742
6. Jun Du, Chunxiao Jiang, Kwang-Cheng Chen, Yong Ren, H. Vincent Poor. Community-Structured Evolutionary Game for Privacy Protection in Social Networks. IEEE Transactions on Information Forensics and Security, 2018, vol. 13, iss. 3, pp. 574-589. DOI: 10.1109/TIFS.2017.2758756
7. Ahmad Hammoud, Hadi Otrok, Azzam Mourad, Omar Abdel Wahab, Jamal Bentahar. On the Detection of Passive Malicious Providers in Cloud Federations. IEEE Communications Letters, 2019, vol. 23, iss. 1, pp. 64-67. DOI: 10.1109/LCOMM.2018.2878714
8. Xiayang Chen, Xingtong Liu, Lei Zhang, Chaojing Tang. Optimal Defense Strategy Se-lection for Spear-Phishing Attack Based on a Multi-stage Signaling Game. IEEE Access, 2019, vol. 7, pp. 19907-19921. DOI: 10.1109/ACCESS.2019.2897724
9. José Moura, David Hutchison. Game Theory for Multi-Access Edge Computing: Survey, Use Cases, and Future Trends. IEEE Communications Surveys & Tutorials, 2019, vol. 21, iss. 1, pp. 260-288. DOI: 10.1109/COMST.2018.2863030
10. Suguo Du, Xiaolong Li, Jinli Zhong, Lu Zhou, Minhui Xue, Haojin Zhu, Limin Sun. Modeling Privacy Leakage Risks in Large-Scale Social Networks. IEEE Access, 2018, vol. 6, pp. 17653-17665. DOI: 10.1109/ACCESS.2018.2818116
11. Savchenko S. O., Kapchuk N. V. Algoritm postroenija modeli narushitelja v sisteme informacionnoj bezopasnosti s primeneniem teorii igr. Dinamika sistem, mehanizmov i mashin. 2017, vol. 5, no 4, pp. 84-89. DOI: 10.25206/2310-9793-2017-5-4-84-89
12. Ciruleva V.M., Kjart A.M. Primenenie teorii igr v informacionnoj bezopasnosti. V sbornike: Matematicheskie metody upravlenija Sbornik nauchnyh trudov. Tver', 2017, pp. 76-90.
13. Kunakovskaja O.V., Men'shih T.V. Primenenie metodov teorii igr k zadacham in-formacionnoj bezopasnosti. Nekotorye voprosy analiza, algebry, geometrii i matematicheskogo obrazovanija, 2016, no. 5-1, pp. 173-174.
14. Kucher V.A., Tarasov E.S. Matematicheskoe modelirovanie processov upravlenija informacionnoj bezopasnost'ju avtomatizirovannyh sistem na osnove metodov teorii igr. Nauchnye trudy Kubanskogo gosudarstvennogo tehnologicheskogo universiteta, 2016, no. 16, pp. 244-255.
15. Artjushkin A.S., Kljucharjov P.G. Obzor teoretiko-igrovyh podhodov k modeli-rovaniju obmannyh sistem. V sbornike: Bezopasnye informacionnye tehnologii Sbornik trudov Vos'moj vserossijskoj nauchno-tehnicheskoj konferencii. NUK «Informatika i sistemy upravlenija», pod. red. M.A.Basaraba, 2017, pp. 27-29.
16. Bykov A. Ju., Shmatova E.S. Algoritmy raspredelenija resursov dlja zashhity in-formacii mezhdu ob»ektami informacionnoj sistemy na osnove igrovoj modeli i principa ravnoj zashhishhennosti ob»ektov. Nauka i obrazovanie: nauchnoe izdanie, 2015, no. 9. DOI: 10.7463/0915.0812283.
17. Bykov A.Ju., Krygin I.A., Mullin A.R. Algoritm raspredelenija resursov sistemy zashhity mezhdu aktivami mobil'nogo ustrojstva na osnove igry s nulevoj summoj i principa ravnoj zashhishhennosti. Vestnik MGTU im. N.Je. Baumana. Priborostroenie, 2018, no. 2, pp. 48-68. DOI: 10.18698/0236-3933-2018-2-48-68
18. Bykov A. Ju., Altuhov N. O., Sosenko A. S. Zadacha vybora sredstv zashhity in-formacii v avtomatizirovannyh sistemah na osnove modeli antagonisticheskoj igry. Inzhenernyj vestnik MGTU im. N.Je. Baumana. Jelektron. zhurn, 2014, no. 4. Rezhim dostupa: http://engbul.bmstu.ru/doc/708106.html
19. Bykov A.Ju., Krygin I.A., Grishunin M.V. Algoritm poiska sedlovoj tochki v smeshannyh strategijah na osnove modifikacii metoda Brauna-Robinsona dlja reshenija zadachi vybora zashhishhaemyh ob»ektov. V sbornike: Bezopasnye informacionnye tehnologii Sbornik trudov Devjatoj vserossijskoj nauchno-tehnicheskoj konferencii, 2018, pp. 33-38.
20. Kljucharev P.G. Kvantovye vychislenija i ataki na kriptoalgoritmy, osnovan-nye na obobshhennyh kletochnyh avtomatah. V sbornike: Bezopasnye informacionnye tehnologii Sbornik trudov Vos'moj vserossijskoj nauchno-tehnicheskoj konferencii. NUK «Informatika i sistemy upravlenija», pod. red. M.A. Basaraba, 2017, pp. 234-236.
21. Basarab M.A., Vel'c S.V. Metody optimizacii i issledovanie operacij v oblasti informacionnoj bezopasnosti: Metodicheskie ukazanija k vypolneniju laboratornyh rabot po discipline «Metody optimizacii i issledovanija operacij». M.: MGTU im. N.Je. Baumana, 2015, 64 p. Rezhim dostupa: http://ebooks.bmstu.press/catalog/117/book967.html