УДК 004.056:519.832 EDN: QYMMDE

АЛГОРИТМЫ РЕШЕНИЯ ДИСКРЕТНО-НЕПРЕРЫВНОЙ ИГРЫ ПРИМЕНИТЕЛЬНО К ЗАДАЧАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ КОМБИНАЦИИ ПРИБЛИЖЕННОГО И ТОЧНОГО МЕТОДОВ

А.Ю. Быков abykov@bmstu.ru
В.В. Сысоев valsus88@mail.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Приведена модель дискретно-непрерывной игры с нулевой суммой двух игроков, защитника и нападающего, применительно к задаче выбора защитником средств защиты, а нападающим — вариантов проведения атак. Для выбора комбинаций средств защиты и проведения атак защитник решает задачу булевого программирования, а нападающий — задачу линейного программирования. Показано, как свести такую задачу к матричной игре. Для поиска седловой точки в смешанных стратегиях можно использовать точный алгоритм, основанный на решении прямой и двойственной задач линейного программирования, но в таком виде задача может иметь большую размерность и недопустимое время решения. Для уменьшения размерности задачи предложено на предварительном этапе использовать приближенный алгоритм на основе метода Брауна — Робинсона, но без явного построения матрицы игры, что позволило существенно уменьшить размерность задач, решаемых с помощью точного алгоритма. По сокращенной матрице игры, полученной приближенным алгоритмом, предложено искать седловую точку в чистых или смешанных стратегиях, а также MinMax и MaxMin, если использовать принцип гарантированного результата при принятии решений. Приведены пример решения задачи и результаты тестирования алгоритмов на исходных данных, полученных с помощью генератора псевдослучайных чисел

Ключевые слова

Средства защиты информации, игра с нулевой суммой, седловая точка, дискретное программирование, линейное программирование, двойственная задача

Поступила 06.10.2023
Принята 27.11.2023

Введение. В исследовательских задачах обеспечения информационной безопасности достаточно часто используется математическая теория игр, позволяющая исследовать различные конфликтные ситуации при принятии решений. Теория игр при принятии решений позволяет учесть возможные цели и действия стороны, выполняющей атаки на защищаемые информационные ресурсы. Рассмотрим задачи выбора средств или способов защиты от различных угроз, выбора защищаемых объектов и некоторые примеры.

Модель оценки рисков информационной безопасности на основе статической байесовской игры двух игроков, защитника и нападающего, построена в [1], где приведены чистые и смешанные стратегии стороны защиты.

Модель, основанная на комбинации теории игр и глубокой нейронной сети для классификации атак в системах обнаружения вторжений, предложена в [2]. Показано, что предлагаемая модель демонстрирует улучшенные характеристики по сравнению с существующими методами, в частности имеет меньшую частоту ложных срабатываний.

Эволюционная игровая модель в [3] использована для анализа проведения возможных атак и защиты сетей. Предложены механизм динамического обучения для описания процесса изменения вероятности выбора стратегий атаки и защиты, и стратегии для получения равновесного состояния.

Некоторые работы на стыке искусственного интеллекта и безопасности, основанные на теории игр, рассмотрены в [4]. Приведены приложения теории игр и обучающих алгоритмов для решения различных задач, связанных с безопасностью, таких как общественная безопасность и охрана дикой природы.

В [5] предложено использовать игру трех игроков для обеспечения защиты персональных данных в различных приложениях. Создана эволюционная игровая модель трех игроков, контролирующих данный процесс: местные органы власти, платформы распространения приложений и пользователи. Проведен анализ устойчивости точек равновесия и условий их устойчивости на основе первого закона Ляпунова.

Механизм контроля доступа на основе теории игр в среде Интернета вещей рассмотрен в [6]. Игроками являются две стороны транзакции: 1) объект, получающий доступ; 2) механизм управления доступом. Принятие решений осуществляется на основе гибридной стратегии равновесия по Нэшу.

Игровая модель нападения и обороны для подводных беспроводных сенсорных сетей на основе подводных беспроводных датчиков предложена

в [7]. Рассмотрены наступательная и оборонительная игровые модели, использовано динамическое уравнение для анализа тенденций развития стратегий при различных обстоятельствах, а также разработан алгоритм выбора оптимальной стратегии, который проверяет эффективность модели посредством моделирования и дает рекомендации по технологиям активной защиты.

Обзор применения теории игр и искусственного интеллекта для анализа социальных сетей приведен в [8]. В исследовании проблемы теории игр, применяемые к социальным сетям, разделены на четыре категории: распространение информации, анализ поведения, обнаружение сообщества и информационная безопасность. Каждая категория исследуется на основе применения знаний.

В [9] предложено выбирать оптимальную стратегию для игр с графом атаки, используя глубокое обучение с подкреплением. Рассмотрена игровая модель Штакельберга для имитации взаимодействия между злоумышленниками и защитниками. Для поиска оптимальной стратегии защиты разработан подход, основанный на обучении с подкреплением.

В [10] показано, как обеспечить безопасность киберфизических систем на основе стохастической игры с асимметричной информацией и игроками с ограниченными ресурсами. Игроками являются датчики для оценки состояния системы. Сформулирована динамическая игра с ненулевой суммой, асимметричной информацией, в которой каждый датчик с ограниченным ресурсом должен решить, следует ли инвестировать в безопасность для отправки пакетов данных, принимая во внимание поведение других датчиков. Предложены алгоритмы для вычисления положений равновесия по Нэшу.

На примере беспилотных автомобилей в [11] предложен краткий обзор угроз безопасности. Приведен обзор литературы с примерами различных игровых моделей для обеспечения безопасности движения, включая проезд регулируемых и нерегулируемых перекрестков, кооперативные игры нескольких автомобилей и различные критерии принятия решений, например критерий Нэша и др.

В [12] предложен протокол для сети беспроводных датчиков (wireless sensor networks) — это самоорганизующиеся сети мониторинга с большим числом случайно развернутых датчиков для сбора различной информации при принятии решений. Датчики питаются от батарей, емкость их ограничена. Теория игр используется для получения компромисса между производительностью при передаче и сроком службы батарей датчиков.

Цель настоящей работы — рассмотреть модель игры двух игроков, защитника и нападающего, в сравнении с приведенными различными подходами [1–12]. Модель может быть применена в широком диапазоне проектирования систем защиты от различных атак на основе выбора средств или методов (подходов) защиты от этих атак. Преимуществом предлагаемой модели является учет неопределенности выбора нападающего с помощью непрерывных переменных, которые можно интерпретировать как вероятности выбора атак. Множество элементов выбора защитника является дискретным, так получена дискретно-непрерывная игра. Основное внимание уделено алгоритму, основанному на комбинации приближенного и точного методов, что позволило комбинировать преимущества этих методов — относительно небольшую вычислительную сложность и точность решения.

Другие математические модели, используемые при защите информации, рассмотрены в [13–16].

Математическая постановка задачи. В настоящей работе поставленная задача является дискретно-непрерывной игрой. Подобные математические постановки задач для дискретных множеств выбора игроков приведены в [17], для непрерывных множеств — в [18]. Похожая постановка задачи защиты серверов вычислительной сети без подробного описания алгоритма решения рассмотрена в [19].

Базисные множества. 1. $A = \{a_1, a_2, \ldots, a_m\}$ — множество типов атак (реализаций угроз безопасности) в защищаемой системе; $M = \{1, 2, \ldots, m\}$ — множество индексов этих атак.

2. $S = \{s_1, s_2, \ldots, s_n\}$ — множество средств или способов защиты от возможных атак (угроз безопасности); $N = \{1, 2, \ldots, n\}$ — множество индексов этих средств или способов защиты.

3. $R^{\text{з}} = \{r_1^{\text{з}}, r_2^{\text{з}}, \ldots, r_{l^{\text{з}}}^{\text{з}}\}$ — множество ограниченных ресурсов стороны защиты; $L^{\text{з}} = \{1, 2, \ldots, l^{\text{з}}\}$ — множество индексов этих ресурсов.

4. $R^{\text{н}} = \{r_1^{\text{н}}, r_2^{\text{н}}, \ldots, r_{l^{\text{н}}}^{\text{н}}\}$ — множество ограниченных ресурсов стороны нападения; $L^{\text{н}} = \{1, 2, \ldots, l^{\text{н}}\}$ — множество индексов этих ресурсов.

Параметры элементов множеств и отношений между ними.

1. $w_i \geq 0, \ \forall\, i \in M$ — оценка ущерба защитника при успешной для нападающего реализации i-го типа атаки.

2. $p_{ij} \in \left[0, 1\right]$, $\forall i \in M$, $j \in N$ — вероятность (или возможность) предотвращения i-й атаки (реализации угрозы) при использовании j-го средства защиты.

3. $v^{з}_{kj} \geq 0$, $\forall\ k \in L^{з}$, $j \in N$ — значение k-го ресурса, требуемого для работы j-го средства защиты.

4. $V^{з}_{k} \geq 0$, $\forall k \in L^{з}$ — максимальное доступное значение k-го ресурса защитника.

5. $v^{н}_{ki} \geq 0$, $\forall k \in L^{н}$, $i \in M$ — значение k-го ресурса нападающего, требуемого для организации i-й атаки.

6. $V^{н}_{k} \geq 0$, $\forall\ k \in L^{н}$ — максимальное доступное значение k-го ресурса нападающего.

Искомые переменные. Для стороны защиты введем булеву переменную $x_j \in \left\{0, 1\right\}$, $\forall\ \ j \in N$, $\ x_j = 1$, если защитник будет использовать j-е средство защиты, то $x_j = 0$. В противном случае, переменные образуют вектор X.

Для стороны нападения введем переменную $y_i \in \left[0, 1\right]$, $\forall\ i \in M$. Значение y_i можно интерпретировать как вероятность или возможность (в терминах нечетких множеств) проведения i-го типа атаки, переменные образуют вектор Y .

Показатель игроков. Оценка полного ущерба стороны защиты — это разность оценок максимального ущерба (если не использовать защиту) и предотвращенного:

$$U\left(X, Y\right) = \sum_{i \in M} w_i\ y_i\ - \sum_{i \in M} w_i\, y_i\ \max_{j \in N} \left\{p_{ij} x_j\right\} =$$

$$= \sum_{i \in M} w_i\, y_i \left(1 - \max_{j \in N} \left\{p_{ij} x_j\right\}\right), \tag{1}$$

$\max\limits_{j \in N} \left\{p_{ij}\ \ x_j\right\}$ задает условие того, что если несколько средств защищают от одной угрозы, то в модели учитывается лучшее из средств защиты (с максимальной вероятностью предотвращения).

Ограничения

$$\sum_{j \in N} v^{з}_{kj}\, x_j\ \leq V^{з}_{k},\ \forall\ k\ \in L^{з} \tag{2}$$

на использование ресурсов защитником;

$$\sum_{i \in M} v_{ki}^{\text{н}} y_i \le V_k^{\text{н}}, \ \forall \ k \in L^{\text{н}} \tag{3}$$

на использование ресурсов нападающего, требуемых на проведение атак.

Таким образом, при фиксированном решении нападающего защитник должен решить задачу булевого программирования минимизации показателя качества (1) с ограничениями (2):

$$U(X, Y) \to \min_X$$

— задача является нелинейной по показателю качества. Нападающий при фиксированном решении защитника должен решать задачу линейного программирования (ЗЛП) максимизации показателя (1) с ограничениями (3):

$$U(X, Y) \to \max_Y$$

— задача является дискретно-непрерывной игрой с нулевой суммой. Допустимое множество решений защитника является конечным и дискретным, а множество допустимых решений нападающего непрерывно.

Алгоритмы решения задачи. Приведем данную задачу к матричной игре с нулевой суммой. Число решений каждого игрока должно быть конечным. Для защитника, решающего задачу булевого программирования при заданном Y с показателем (1) и ограничениями (2), это так, поскольку число различных булевых векторов X заданной размерности всегда конечно. Для нападающего, который решает ЗЛП с показателем (1) при заданном X и ограничениями (3), решение находится в одной вершине многогранника допустимых решений. Исходя из ограничений (3), многогранник допустимых решений выпуклый и ограниченный. Вершин у этого многогранника конечное число. Если существует множество решений, которые лежат на некоторой грани многогранника (в каждой точке грани целевая функция принимает одно и то же значение), то решением можно считать вершину, принадлежащую грани. Поэтому в качестве возможных решений нападающего можно считать только те решения, которые находятся в вершинах многогранника допустимых решений, заданного ограничениями (3). Так задачу можно свести к матричной игре, но размер матрицы может быть относительно большим.

Для матричной игры можно определить MinMax для защитника, если использовать принцип гарантированного результата: $U(X, Y) \to \min_X, \min_Y$ а также седловую точку игры в чистых стратегиях, если она существует, когда MinMax равен MaxMin, или в смешанных страте-

гиях в противном случае. Для поиска седловой точки в смешанных стратегиях существуют как точные, так и приближенные методы. Наиболее распространенный точный метод сводится к решению прямой и двойственной ЗЛП [20], а также один из часто используемых приближенных методов — метод Брауна — Робинсона [20], основной недостаток которого — медленная сходимость. Рассмотрим особенности точного метода и его основные недостатки применительно к указанной задаче, а также случай, когда седловой точки в чистых стратегиях не существует, а существует она в смешанных стратегиях.

Особенности применения точного метода поиска седловой точки. Точный метод основан на том, что по матрице игры формулируются две ЗЛП: прямая и двойственная [20]. При решении этих задач получаем решения защитника и нападающего в смешанных стратегиях. Рассмотрим, как построить матрицу игры для этой задачи. Для защитника, который решает задачу минимизации показателя (1) с ограничениями (2), необходимо рассматривать только допустимые решения с максимальным числом 1, так как особенность показателя (1) заключается в том, что при исключении из допустимого решения защитником любого средства защиты (в векторе X единица заменяется нулем), значение показателя для защитника не улучшится. Алгоритмы решения подобных задач рассмотрены в [13]. Таким образом, для построения матрицы игры необходимо найти все допустимые векторы X по ограничениям (2) с максимальным числом 1, число таких решений составляет одну из размерностей матрицы игры, например число столбцов. Для каждого такого решения X решаем ЗЛП максимизации показателя (1) для нападающего с ограничениями (3). Число полученных различных решений для нападающего (некоторые решения могут быть одинаковыми по вектору Y) составляет вторую размерность матрицы игры, например, число строк. Для полученных векторов X и Y вычисляем значения показателя (1), которые и являются элементами матрицы игры, полученной в явном виде.

Как показали эксперименты, размерность матрицы игры в явном виде может быть достаточно большой, что затрудняет поиск решения с точки зрения вычислительной сложности.

Комбинированное применение точного и приближенного методов поиска седловой точки. Для сокращения размерности матрицы игры воспользуемся комбинированным использованием приближенного метода Брауна — Робинсона и точного метода, сводящегося к решению прямой и двойственной ЗЛП. На первом этапе применяем приближенный метод Брауна — Робинсона. Для уменьшения вычислительной сложности задаем

относительно небольшую точность, что позволяет получить относительно небольшое число решений, входящих в седловую точку в смешанных стратегиях, среди которых некоторые будут активными (вероятности выбора стратегий не равны нулю), другие будут неактивными. Для полученных решений составляем матрицу игры в явном виде. Для нее используем точный метод, основанный на решении прямой и двойственной ЗЛП. Опишем модификацию метода Брауна — Робинсона, используемую на первом этапе. Причем модификация не требует построения матрицы игры в явном виде по аналогии с [18].

Алгоритм на основе метода Брауна — Робинсона без построения матрицы игры. Алгоритм основан на том, что последовательно многократно разыгрывается игра между двумя игроками и на каждом шаге k (k =1, 2, 3, 4,…) решение принимается с учетом суммарного выигрыша (проигрыша) на всех предыдущих партиях игры. Процесс итераций алгоритма можно начать с любого решения, например, предварительно задать для нападающего решение $Y = \left[1,\ 1, \ldots, 1\right]^{\mathrm{T}}$, состоящее из единиц (нападающий проводит все возможные атаки), скорее всего, это решение будет недопустимым по ограничениям (3), на первом шаге находим оптимальное решение $X^{(1)}$, решив каким-либо методом булева программирования задачу минимизации показателя качества (1) с ограничениями (2). При $X^{(1)}$ решаем ЗЛП максимизации показателя (1) с ограничениями (3), находим оптимальное решение $Y^{(1)}$. Значения показателя при $X^{(1)}$ и $Y^{(1)}$ будут оценками нижней и верхней ценами игры.

Задачу булева программирования для защитника решаем путем минимизации показателя качества

$$U^k\left(\vec{X}\right) = \sum_{l=1}^{k-1} \sum_{i \in M} w_i y_i^l \left(1 - \max_{j \in N}\left\{p_{ij} x_j\right\}\right) =$$

$$= \sum_{i \in M} \left(1 - \max_{j \in N}\left\{p_{ij} x_j\right\}\right) \sum_{l=1}^{k-1} w_i y_i^l,$$

где y_i^l, $i \in M$ — компоненты вектора оптимального решения Y^l, полученного на l-м шаге. Оптимальное решение, найденное при решении этой задачи, будет X^k. Оценка нижней цены игры при этом будет $\underline{v} = U^k\left(X^k\right)/k$.

Задачу линейного программирования для нападающего решаем путем максимизации показателя качества

$$U^k\left(\vec{Y}\right)=\sum_{l=1}^{k-1}\sum_{i\in M} w_i y_i\left(1-\max_{j\in N}\left\{p_{ij}x_j^l\right\}\right)=$$

$$=\sum_{i\in M} w_i y_i \sum_{l=1}^{k-1}\left(1-\max_{j\in N}\left\{p_{ij}x_j^l\right\}\right),$$

где x_j^l, $j\in N$ — компоненты вектора решения X^l, полученного на l-м шаге. Оптимальное решение, найденное при решении этой задачи, будет Y^k, при этом оценка верхней цены игры $\overline{v}=U^k\left(Y^k\right)/k$.

На каждом шаге алгоритма полученные решения отдельно для защитника и нападающего помещаем в «карты» (словари, в языке C++ шаблоны *map* или *unordered_map*), ключом являются решения (векторы X^k и Y^k), а значением — число повторений этого решения. Если полученного решения (ключа) нет в «карте», то оно помещается в «карту» со значением единица. Если решение (ключ) есть в «карте», то его значение увеличивается на единицу.

Критерий остановки алгоритма $\overline{v}-\underline{v}\le\varepsilon$, где ε — заданная погрешность алгоритма.

После остановки алгоритма по «картам» для защитника и нападающего вычисляем оценки вероятностей решений, это будут приближенные оценки смешанных стратегий игроков. По полученным различным решениям защитника и нападающего также можно составить матрицу игры в явном виде и далее использовать точный алгоритм. Как показали эксперименты, размерность матрицы игры будет существенно ниже, по сравнению со случаем, если не использовать на предварительном шаге приближенный алгоритм.

Результаты. Рассмотрим пример решения задачи с условно-реальными исходными данными.

Некоторые возможные атаки (реализации угроз) для условной автоматизированной системы обработки информации и управления, оценка возможного ущерба от этих атак и стоимость их проведения для нападающего приведены в табл. 1. Предположим, что у нападающего один ограниченный ресурс, заданный деньгами, которые идут на проведение атак. В табл. 1 для каждого типа атаки указана соответствующая компонента вектора Y. Данные о возможном ущербе зависят от специфики деятельности компании, в которой используется система, данные в табл. 1 являются условными.

Некоторые средства защиты от угроз безопасности без названия производителей приведены в табл. 2. Вероятности (возможности) предотвращения атак заданы условно и могут быть получены на основе экспертных оценок, что выходит за рамки настоящей работы, атаки в табл. 2 заданы номерами в соответствии с табл. 1. Для использования средств защиты будем учитывать один ограниченный ресурс — денежные средства, которые можно потратить на защиту. В табл. 2 также приведены компоненты вектора X, соответствующие средствам защиты. Примерные цены задают конфигурацию средств защиты для информационной системы на основе локальной вычислительной сети с одним сервером и 20 рабочими местами.

Таблица 1

Ущерб от возможных атак и стоимость их реализации для нападающего

№	Атака (реализация) ($A = \{a_1, a_2, \ldots, a_m\}$)	Ущерб от возможных атак (w_i, $\forall i \in M$), руб.	Стоимость реализации угроз для нападающего ($v_{1i}^{\text{н}}$, $\forall i \in M$), руб.
1	Утечка конфиденциальной информации из сети по каналам связи (e-mail, web, chat/IM и др.) y_1	10 000 000	100 000
2	Прослушивание внешних каналов связи злоумышленниками y_2	1 000 000	100 000
3	Нарушение конфиденциальности данных, передаваемых по линиям связи, проходящим вне контролируемой зоны, внешними нарушителями путем пассивного прослушивания каналов связи y_3	10 000 000	50 000
4	Перехват информации на линиях связи с помощью различных видов анализаторов сетевого трафика y_4	1 000 000	50 000
5	Замена, вставка, удаление или изменение данных пользователей в информационном потоке y_5	5 000 000	90 000

Окончание табл. 1

№	Атака (реализация) ($A = \{a_1, a_2, \ldots, a_m\}$)	Ущерб от возможных атак (w_i, $\forall i \in M$), руб.	Стоимость реализации угроз для нападающего ($v_{1i}^{н}$, $\forall i \in M$), руб.
6	Перехват информации, например пользовательских паролей, передаваемой по каналам связи, в целях ее последующего использования для обхода средств сетевой аутентификации y_6	5 000 000	100 000
7	Статистический анализ сетевого трафика (например, наличие или отсутствие определенной информации, частота передачи, направление, типы данных и т. п.) y_7	1 000 000	50 000
8	Внедрение несанкционированного, непроверенного или вредоносного программного кода (вирусов, троянских программ и др.) y_8	1 000 000	40 000
9	Анализ и модификация ПО y_9	5 000 000	200 000
10	Пересылаемые по e-mail логические бомбы y_{10}	1 000 000	50 000
11	Атаки на отказ в обслуживании против внешних хостов компании y_{11}	1 000 000	20 000
Примечание. Всего на реализацию угроз выделено $V_1^{н}$ = 500 000 руб.			

При исходных данных, приведенных в табл. 1 и 2, если строить полную матрицу игры с помощью определения всех допустимых решений защитника с максимальным числом 1, то таких решений будет 48, решая для этого ЗЛП для нападающего, получаем 15 различных решений. Матрица игры имеет размер 15 × 48. Если использовать приближенный алгоритм на основе метода Брауна — Робинсона и задать относительную погрешность вычисления 0,1 %, то получим:

– число итераций алгоритма Брауна — Робинсона, равное 247;

– число решений X для защитника в «карте» (словаре), равное трем (p — приближенные вероятности решений):

1) $X = [1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1]^{\mathrm{T}}$, $p = 0{,}713$;

2) $X = [1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1]^{\mathrm{T}}$, $p = 0{,}15$;

3) $X = [1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0]^{\mathrm{T}}$, $p = 0{,}138$;

– число решений Y для нападающего в «карте» (словаре), равное четырем (q — приближенные вероятности):

1) $Y = [1.00\ 0.00\ 0.00\ 1.00\ 1.00\ 1.00\ 0.00\ 0.00\ 0.70\ 0.00\ 1.00]^{\mathrm{T}}$,

$q = 0{,}559$;

2) $Y = [1.00\ 0.00\ 1.00\ 1.00\ 1.00\ 1.00\ 0.00\ 0.00\ 0.45\ 0.00\ 1.00]^{\mathrm{T}}$,

$q = 0{,}433$;

3) $Y = [1.00\ 0.00\ 1.00\ 1.00\ 1.00\ 1.00\ 1.00\ 0.00\ 0.20\ 0.00\ 1.00]^{\mathrm{T}}$,

$q = 0{,}004$;

4) $Y = [1.00\ 0.40\ 1.00\ 1.00\ 1.00\ 1.00\ 1.00\ 0.00\ 0.00\ 0.00\ 1.00]^{\mathrm{T}}$,

$q = 0{,}004$.

Таблица 2

Средства защиты, стоимость их реализации и возможности (вероятности) предотвращения угроз

Средство защиты ($S = \{s_1, s_2, \ldots, s_n\}$)	Стоимость реализации ($v^3_{1j}, \forall\ j \in N$), руб.	Возможности (вероятности) предотвращения угрозы ($p_{ij}, \forall i \in N, \forall j \in M$), атака (см. табл. 1)										
		1	2	3	4	5	6	7	8	9	10	11
Простой антивирус x_1	30 000	0	0	0	0	0	0	0	0,9	0,8	0,9	0
Программа криптографической защиты x_2	60 000	0,6	0,7	0,9	0	0,8	0,6	0	0	0	0	0
Средство для защиты от сетевых вторжений x_3	40 000	0	0	0	0	0	0	0	0,7	0,6	0,8	0
Средство обнаружения вторжений x_4	20 000	0	0	0	0,6	0,5	0,4	0,8	0,1	0	0	0,4

Окончание табл. 2

Средство защиты ($S = \{s_1, s_2, \ldots, s_n\}$)	Стоимость реализации ($v^{з}_{1j}$, $\forall\ j \in N$), руб.	Возможности (вероятности) предотвращения угрозы (p_{ij}, $\forall i \in N$, $\forall j \in M$), атака (см. табл. 1)										
		1	2	3	4	5	6	7	8	9	10	11
Средство, включающее в себя межсетевой экран, антивирус и средства обнаружения вторжений x_5	50 000	0	0	0	0,7	0,5	0,4	0,7	0,1	0,6	0,7	0,6
Комплекс шифрования x_6	300 000	0,7	0,8	0,99	0	0,7	0,1	0	0	0	0	0
Средство защиты информации от НСД x_7	35 000	0	0	0	0	0,5	0,6	0	0,8	0,8	0	0
Электронный замок x_8	200 000	0	0	0	0	0,6	0,5	0	0,9	0,9	0	0
Средство защиты данных при взломе или краже дисков x_9	28 000	0,9	0	0	0	0	0,8	0	0	0	0	0
Средство защиты от DDoS x_{10}	60 000	0	0	0	0	0	0	0	0	0	0	0,7

Примечание. Всего выделено средств $V^{з}_{1} = 500\,000$ руб.

На основе полученных решений приближенным алгоритмом можно составить матрицу игры размером 4 × 3:

$$A = \begin{Vmatrix} 44\ 000\ 00.00 & 3\ 950\ 000.00 & 4\ 400\ 000.00 \\ 4\ 250\ 000.00 & 4\ 825\ 000.00 & 4\ 250\ 000.00 \\ 4\ 200\ 000.00 & 4\ 900\ 000.00 & 4\ 200\ 000.00 \\ 4\ 080\ 000.00 & 4\ 920\ 000.00 & 4\ 080\ 000.00 \end{Vmatrix}.$$

Для полученной матрицы игры MaxMin = 4 250 000.00, MinMax = = 4 400 000.00. Таким образом, седловой точки в чистых стратегиях не существует. При поиске седловой точки в смешанных стратегиях точным методом, основанным на решении прямой и двойственной ЗЛП, получаем следующие решения:

1) $X = [1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1]^{\mathrm{T}}$, $p = 0{,}854$;

2) $X = [1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1]^{\mathrm{T}}$, $p = 0{,}146$;

3) $X = [1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0]^{\mathrm{T}}$, $p = 0$

— для защитника;

1) $Y = [1.00\ 0.00\ 0.00\ 1.00\ 1.00\ 1.00\ 0.00\ 0.00\ 0.70\ 0.00\ 1.00]^{\mathrm{T}}$, $q = 0{,}561$;

2) $Y = [1.00\ 0.00\ 1.00\ 1.00\ 1.00\ 1.00\ 0.00\ 0.00\ 0.45\ 0.00\ 1.00]^{\mathrm{T}}$, $q = 0{,}439$;

3) $Y = [1.00\ 0.00\ 1.00\ 1.00\ 1.00\ 1.00\ 1.00\ 0.00\ 0.20\ 0.00\ 1.00]^{\mathrm{T}}$, $q = 0$;

4) $Y = [1.00\ 0.40\ 1.00\ 1.00\ 1.00\ 1.00\ 1.00\ 0.00\ 0.00\ 0.00\ 1.00]^{\mathrm{T}}$, $q = 0$

— для нападающего.

Цена игры при этом составляет 4 334 146,34 руб.

Если решить задачу напрямую, без предварительного использования приближенного алгоритма для матрицы размером 15 × 48, то получены те же по две активные стратегии (вероятности не равны нулю) в седловой точке.

Пример решения задачи с данными, полученными с помощью генераторов псевдослучайных чисел. При генерации псевдослучайных исходных данных использовались следующие параметры: возможный ущерб w_i, $\forall\, i \in M$ — равномерное распределение от 100 до 1000; вероятность или возможность предотвращения атаки p_{ij}, $\forall\, i \in M$, $j \in N$ — равномерное распределение от 0,5 до 0,99; число ресурсов защитника равно трем; значение каждого ресурса для средства защиты $v_{kj}^{\mathrm{з}}$, $\forall\, k \in L^{\mathrm{з}}$, $j \in N$ — равномерное распределение от 10 до 100; максимальное значение каждого ресурса $V_k^{\mathrm{з}}$, $\forall\, k \in L^{\mathrm{з}}$ — половина от требуемого для использования всех средств защиты; число ресурсов нападающего равно трем; значение каждого ресурса для типа атаки $v_{ki}^{\mathrm{н}}$, $\forall\, k \in L^{\mathrm{н}}$, $i \in M$ — равномерное распределение от 10 до 100; максимальное значение каждого ресурса $V_k^{\mathrm{н}}$, $\forall\ k \in L^{\mathrm{н}}$ — половина от требуемого для реализации всех типов атак.

Зависимости чисел решений защитника без использования приближенного метода (т. е. число допустимых решений защитника с максимальным числом 1), решений защитника после использования прибли-

женного метода (число решений, полученных методом Брауна — Робинсона) и активных стратегий защитника в седловой точке (в смешанном варианте) от числа средств защиты приведены в табл. 3. Эти зависимости приведены для 15 типов атак нападающего. Тестирование при числе типов атак 10 и 20 показало такой же качественный характер. Число активных стратегий в седловой точке — это стратегии, вероятности выбора которых не равны нулю. Если в седловой точке указана одна активная стратегия, то это означает, что в данном примере получена седловая точка в чистых стратегиях.

Таблица 3

Зависимости числа решений защитника от числа средств защиты для 15 типов атак нападающего

Число средств защиты (размерность X)	Число решений защитника		Число активных стратегий в седловой точке
	Без использования приближенного метода	После использования приближенного метода	
10	129	4	3
11	207	3	2
12	452	7	5
13	695	3	2
14	1329	1	1
15	2903	3	2
16	6245	4	3
17	9707	6	7
18	18 885	8	4
19	31 870	3	1
20	68 212	1	1

Зависимости числа решений защитника от числа средств защиты для 15 типов атак нападающего приведены на рис. 1. Зависимости числа решений нападающего от числа типов атак при 15 средствах защиты приведены в табл. 4.

Обсуждение полученных результатов. Из приведенных в табл. 3, 4 данных и рис. 2 следует, что сложность использования только точного метода для поиска седловой точки, основанного на решении прямой и двойственной ЗЛП при определенных числах средств защиты и типов атак, заключается в размерности задачи, особенно для защитника, число решений которого растет экспоненциально, поскольку он решает задачу

булевого программирования. Использование же на предварительном этапе приближенного алгоритма, основанного на методе Брауна — Робинсона без явного построения матрицы игры, позволяет существенно сократить размерность задачи для точного алгоритма и сделать его приемлемым для применения с точки зрения размерности задачи.

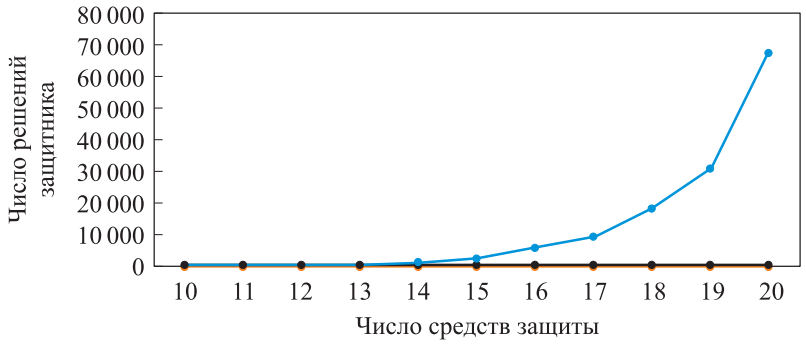

Рис. 1. Зависимости числа решений защитника от числа средств защиты для 15 типов атак нападающего:

и — число решений защитника без использования приближенного метода и после его применения; — число активных стратегий защитника

Таблица 4

Зависимости числа решений нападающего от числа типов атак при 15 средствах защиты

Число атак (размерность Y)	Число решений нападающего		Число активных стратегий нападающего
	Без использования приближенного метода	После использования приближенного метода	
10	78	5	2
11	80	3	1
12	221	7	2
13	234	1	1
14	427	11	4
15	372	4	2
16	666	33	5
17	508	17	4
18	549	142	7
19	568	6	2
20	916	18	4
21	1487	35	6

Зависимости числа решений нападающего от числа типов атак при различном числе средств защиты приведены на рис. 2.

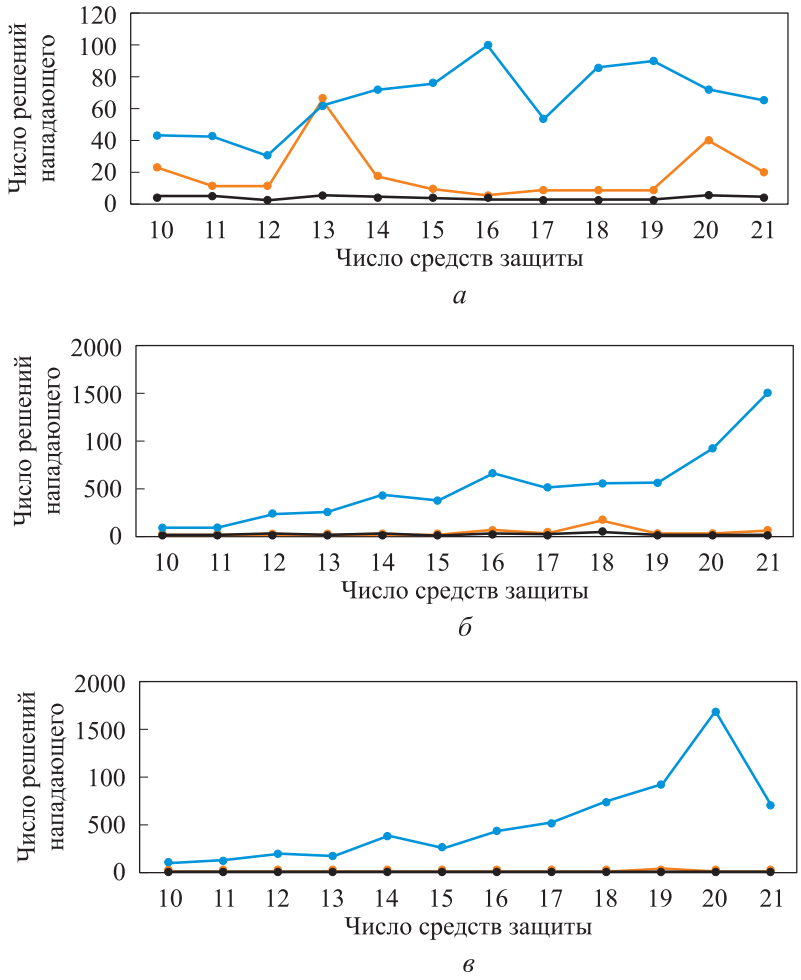

Рис. 2. Зависимости числа решений нападающего от числа типов атак при 10 (*а*), 15 (*б*), 20 (*в*) средствах защиты:

и — число решений нападающего без использования приближенного метода и после его применения; — число активных стратегий нападающего

С точки зрения размерности задачи, для защитника получен следующий парадоксальный результат: при увеличении числа средств защиты имеется тенденция к уменьшению числа возможных решений защитника после применения приближенного метода и тенденция к уменьшению активных стратегий внутри седловой точки.

Проверка точности полученного решения на предварительном этапе с помощью приближенного алгоритма по сравнению со случаем исполь-

зования изначально точного алгоритма для размера матрицы игры, позволяющего за разумное время решить задачу, выявила, что во всех примерах решения совпадали, т. е. приближенный метод позволил определять все активные стратегии седловой точки за приемлемое время с заданной относительно небольшой точностью.

Заключение. Рассмотрена игра с нулевой суммой двух игроков при ограничениях на ресурсы для выбора средств или способов защиты защитником и выбора типов атак нападающим. Множество элементов выбора защитника дискретное, а множество элементов выбора нападающего непрерывное. Защитник решает задачу булевого программирования при фиксированном решении нападающего, а нападающий ЗЛП — при фиксированном решении защитника.

Для определения седловой точки в чистых или смешанных стратегиях можно построить матрицу игры в явном виде, найдя все допустимые решения защитника с максимальными наборами средств защиты (допустимые векторы X с максимальным числом 1) и решая ЗЛП для нападающего. В этом случае размер матрицы игры будет достаточно большим, что создает проблемы с точки зрения вычислительной сложности. Для уменьшения исходной матрицы игры на предварительном этапе предложено использовать приближенный алгоритм с небольшой точностью, основанный на методе Брауна — Робинсона, но без явного построения матрицы игры. Решения, полученные приближенным алгоритмом, задают стратегии для матрицы игры, размер которой будет существенно меньше, чем матрицы, полученной без использования приближенного алгоритма. Для полученной матрицы далее использован точный алгоритм, основанный на решении прямой и двойственной ЗЛП.

Приведен пример решения задачи и результаты тестирования алгоритмов на исходных данных, полученных с помощью генераторов псевдослучайных чисел. Эксперименты показали существенное сокращение размера матрицы игры при использовании приближенного алгоритма на предварительном этапе. Для защитника выявлены тенденции к снижению числа возможных решений после применения приближенного метода при увеличении числа средств защиты и к уменьшению активных стратегий внутри седловой точки.

ЛИТЕРАТУРА

[1] Min H., Li C.Y. Construction of information security risk assessment model based on static game. *ISCIPT*, 2021, pp. 647–650.
DOI: https://doi.ieeecomputersociety.org/10.1109/ISCIPT53667.2021.00137

[2] Jain A., Tripathi K., Jatain A., et al. A game theory based attacker defender model for IDS in cloud security. *INDIACom*, 2022, pp. 190–194.
DOI: https://doi.org/10.23919/INDIACom54597.2022.9763191

[3] Zhang H., Zhang X., Sun P., et al. Traceability method of network attack based on evolutionary game. *NaNA*, 2022, pp. 232–236.
DOI: https://doi.ieeecomputersociety.org/10.1109/NaNA56854.2022.00046

[4] Sinha A. AI and security: a game perspective. *COMSNETS*, 2022.
DOI: http://doi.org/10.1109/COMSNETS53615.2022.9668430

[5] Guo Y., Zou K., Yang M., et al. Tripartite evolutionary game of multiparty collaborative supervision of personal information security in app: empirical evidence from China. *IEEE Access*, 2022, vol. 10, pp. 85429–85441.
DOI: https://doi.org/10.1109/ACCESS.2022.3198705

[6] Zhang X. Access control mechanism based on game theory in the internet of things environment. *IEEE ICCC*, 2022.
DOI: https://doi.org/10.1109/ICCC56324.2022.10065968

[7] Bian Y., Lin H., Song Y. Game model of attack and defense for underwater wireless sensor networks. *IEEE ITAIC*, 2022.
DOI: http://doi.org/10.1109/ITAIC54216.2022.9836681

[8] Miaji M., Miaji Y. exploiting game theory strategy and artificial intelligent to analyze social networks: a comprehensive survey. *SMAP*, 2022.
DOI: http://doi.org/10.1109/SMAP56125.2022.9941773

[9] Zhang Y., Liu F., Chen H. Optimal strategy selection for attack graph games using deep reinforcement learning. *2022 IEEE HPCC/DSS/SmartCity/DependSys*, 2022.
DOI: https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00135

[10] Xing W., Zhao X., Başar T., et al. Security investment in cyber-physical systems: stochastic games with asymmetric information and resource-constrained players. *IEEE Trans. Automat. Contr.*, 2022, vol. 67, no. 10, pp. 5384–5391.
DOI: http://doi.org/10.1109/TAC.2021.3116093

[11] Qurashi J.M., Ikram M.J., Jambi K., et al. Autonomous vehicles: security challenges and game theory-based countermeasures. *ICAISC*, 2023.
DOI: http://doi.org/10.1109/ICAISC56366.2023.10085301

[12] Yao Y.D., Li X., Cui Y.P., et al. Game theory and coverage optimization based multihop routing protocol for network lifetime in wireless sensor networks. *IEEE Sens. J.*, 2022, vol. 22, no. 13, pp. 13739–13752. DOI: http://doi.org/10.1109/JSEN.2022.3178441

[13] Басараб М.А., Троицкий И.И., Онуфриева Е.В. Исследование функционирования SIEM-систем с помощью различных корреляторов для бинарных последовательностей вида (1, –1) при условии, что случайные величины принимают свои значения с одинаковыми вероятностями. *Сб. тр. XI Междунар. науч.-техн. конф. «Безопасные информационные технологии»*. М., Изд-во МГТУ им. Н.Э. Баумана, 2021, с. 32–36.

[14] Ключарёв П.Г. Клеточные автоматы и их обобщения в задачах криптографии. Часть 1. *Вопросы кибербезопасности*, 2021, № 6, с. 90–101.

[15] Ключарёв П.Г. Клеточные автоматы и их обобщения в задачах криптографии. Часть 2. *Вопросы кибербезопасности*, 2022, № 1, с. 37–48.

[16] Зеленецкий А.С., Ключарев П.Г. Алгоритм поиска аффинных аннигиляторов булевой функции. *Математика и математическое моделирование*, 2021, № 1, с. 13–26. DOI: http://doi.org/10.24108/mathm.0121.0000255

[17] Быков А.Ю., Гришунин М.В., Крыгин И.А. Игровая задача выбора защищаемых объектов и исследование алгоритма поиска седловой точки на основе модификации метода Брауна — Робинсона. *Вопросы кибербезопасности*, 2019, № 2, с. 2–12.

[18] Быков А.Ю., Крыгин И.А., Гришунин М.В. и др. Об одном алгоритме поиска седловой точки для непрерывных линейных игр применительно к задачам защиты информации. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2020, № 4 (133), с. 58–74. DOI: http://doi.org/10.18698/0236-3933-2020-4-58-74

[19] Bykov A.Yu., Grishunin M.V., Fedorov E.G., et al. Algorithm for determining saddle point in game theory problem of choosing software for information security on computer network servers. *CEUR Workshop Proceedings*. Moscow, 2021, с. 22–32.

[20] Стрекаловский А.С., Орлов А.В. Биматричные игры и билинейное программирование. М., ФИЗМАТЛИТ, 2007.

Быков Александр Юрьевич — канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Сысоев Валентин Валерьевич — аспирант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Просьба ссылаться на эту статью следующим образом:

Быков А.Ю., Сысоев В.В. Алгоритмы решения дискретно-непрерывной игры применительно к задачам информационной безопасности на основе комбинации приближенного и точного методов. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2024, № 2 (147), с. 102–124. EDN: QYMMDE

ALGORITHMS FOR SOLVING A DISCRETE-CONTINUOUS GAME BASED ON COMBINATION OF THE APPROXIMATE AND EXACT METHODS IN THE CONTEXT OF INFORMATION PROTECTION TASKS

A.Yu. Bykov abykov@bmstu.ru
V.V. Sysoev valsus88@mail.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The paper presents a model of a discrete-continuous zero-sum game between two players, i.e. defender and attacker, in relation to the problem of selecting protection means by the defender, and attack options by the attacker. The defender solves a Boolean programming problem to select the defense combinations, and the attacker solves a linear programming problem to find the attack combinations. It is shown how to reduce such problems to a matrix game. To find a saddle point in the mixed strategies, the exact algorithm could be introduced on the basis of solutions to the direct and dual linear programming problems. However, the problem in this form could have large dimension and unacceptable solution time. To reduce the problem dimension, the paper proposes to use at the preliminary stage an approximate algorithm based on the Brown — Robinson method, but without explicitly constructing the game matrix making it possible to significantly reduce dimension of the problems solved by the exact algorithm. Based on the game reduced matrix obtained by the approximate algorithm, it is proposed to search for a saddle point in the pure or mixed strategies, as well as the minimax and maximin, if the principle of guaranteed results in decision-making is used. An example of solving the problem is provided, as well as results of testing the algorithms on initial data obtained using a pseudorandom number generator

Keywords

Information protection tools, zero-sum game, saddle point, discrete programming, linear programming, dual problem

Received 06.10.2023
Accepted 27.11.2023

REFERENCES

[1] Min H., Li C.Y. Construction of information security risk assessment model based on static game. *ISCIPT*, 2021, pp. 647–650.
DOI: https://doi.ieeecomputersociety.org/10.1109/ISCIPT53667.2021.00137

[2] Jain A., Tripathi K., Jatain A., et al. A game theory based attacker defender model for IDS in cloud security. *INDIACom*, 2022, pp. 190–194.
DOI: https://doi.org/10.23919/INDIACom54597.2022.9763191

[3] Zhang H., Zhang X., Sun P., et al. Traceability method of network attack based on evolutionary game. *NaNA*, 2022, pp. 232–236.
DOI: https://doi.ieeecomputersociety.org/10.1109/NaNA56854.2022.00046

[4] Sinha A. AI and security: a game perspective. *COMSNETS*, 2022.
DOI: http://doi.org/10.1109/COMSNETS53615.2022.9668430

[5] Guo Y., Zou K., Yang M., et al. Tripartite evolutionary game of multiparty collaborative supervision of personal information security in app: empirical evidence from China. *IEEE Access*, 2022, vol. 10, pp. 85429–85441.
DOI: https://doi.org/10.1109/ACCESS.2022.3198705

[6] Zhang X. Access control mechanism based on game theory in the internet of things environment. *IEEE ICCC*, 2022.
DOI: https://doi.org/10.1109/ICCC56324.2022.10065968

[7] Bian Y., Lin H., Song Y. Game model of attack and defense for underwater wireless sensor networks. *IEEE ITAIC*, 2022.
DOI: http://doi.org/10.1109/ITAIC54216.2022.9836681

[8] Miaji M., Miaji Y. exploiting game theory strategy and artificial intelligent to analyze social networks: a comprehensive survey. *SMAP*, 2022.
DOI: http://doi.org/10.1109/SMAP56125.2022.9941773

[9] Zhang Y., Liu F., Chen H. Optimal strategy selection for attack graph games using deep reinforcement learning. *IEEE HPCC/DSS/SmartCity/DependSys*, 2022.
DOI: https://doi.org/10.1109/HPCC-DSS-SmartCity-DependSys57074.2022.00135

[10] Xing W., Zhao X., Başar T., et al. Security investment in cyber-physical systems: stochastic games with asymmetric information and resource-constrained players. *IEEE Trans. Automat. Contr.*, 2022, vol. 67, no. 10, pp. 5384–5391.
DOI: http://doi.org/10.1109/TAC.2021.3116093

[11] Qurashi J.M., Ikram M.J., Jambi K., et al. Autonomous vehicles: security challenges and game theory-based countermeasures. *ICAISC*, 2023.
DOI: http://doi.org/10.1109/ICAISC56366.2023.10085301

[12] Yao Y.D., Li X., Cui Y.P., et al. Game theory and coverage optimization based multihop routing protocol for network lifetime in wireless sensor networks. *IEEE Sens. J.*, 2022, vol. 22, no. 13, pp. 13739–13752.
DOI: http://doi.org/10.1109/JSEN.2022.3178441

[13] Basarab M.A., Troitskii I.I., Onufrieva E.V. [The investigation of the operation of SIEM-systems using various correlators for binary sequences (1, –1) under condition, that random values take values with same probability]. *Sb. tr. XI Mezhdunar. nauch.-tekh. konf. "Bezopasnye informatsionnye tekhnologii"* [Secure Information Technologies. Proc. 11th Int. Sc.-Tech. Conf.]. Moscow, BMSTU Publ., 2021, pp. 32–36 (in Russ.).

[14] Klyucharev P.G. Cellular automata and their generalizations in cryptography. Part 1. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2021, no. 6, pp. 90–101 (in Russ.).

[15] Klyucharev P.G. Cellular automata and their generalizations in cryptography. Part 2. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2022, no. 1, pp. 37–48 (in Russ.).

[16] Zelenetskiy A.S., Klyucharev P.G. Affine annihilator finding algorithm for Boolean function. *Matematika i matematicheskoe modelirovanie* [Mathematics and Mathematical Modeling], 2021, no. 1, pp. 13–26 (in Russ.).
DOI: http://doi.org/10.24108/mathm.0121.0000255

[17] Bykov A.Yu., Grishunin M.V., Krygin I.A. The game problem of selection of assets to protect and research of saddle point search algorithm based on Brown — Robinson method modification. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2019, no. 2, pp. 2–12 (in Russ.).

[18] Bykov A.Yu., Krygin I.A., Grishunin M.V., et al. On one saddle point search algorithm for continuous linear games as applied to information security problems. *Herald of the Bauman Moscow State Technical University, Series Natural Sciences*, 2020, no. 4 (133), pp. 58–74 (in Russ.). DOI: http://doi.org/10.18698/0236-3933-2020-4-58-74

[19] Bykov A.Yu., Grishunin M.V., Fedorov E.G., et al. Algorithm for determining saddle point in game theory problem of choosing software for information security on computer network servers. *CEUR Workshop Proceedings*. Moscow, 2021, pp. 22–32.

[20] Strekalovskiy A.S., Orlov A.V. Bimatrichnye igry i bilineynoe programmirovanie [Bimatrix games and bilinear programming]. Moscow, FIZMATLIT Publ., 2007.

Bykov A.Yu. — Cand. Sc. (Eng.), Assoc. Professor, Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Sysoev V.V. — Post-Graduate Student, Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Please cite this article in English as:

Bykov A.Yu., Sysoev V.V. Algorithms for solving a discrete-continuous game based on combination of the approximate and exact methods in the context of information protection tasks. *Herald of the Bauman Moscow State Technical University, Series Instrument Engineering*, 2024, no. 2 (147), pp. 102–124 (in Russ.). EDN: QYMMDE