УДК 004.056+519.832.2 DOI: 10.18698/0236-3933-2018-2-48-68

АЛГОРИТМЫ РАСПРЕДЕЛЕНИЯ РЕСУРСОВ СИСТЕМЫ ЗАЩИТЫ МЕЖДУ АКТИВАМИ МОБИЛЬНОГО УСТРОЙСТВА НА ОСНОВЕ ИГРЫ С НУЛЕВОЙ СУММОЙ И ПРИНЦИПА РАВНОЙ ЗАЩИЩЕННОСТИ

А.Ю. Быков abykov@bmstu.ru
И.А. Крыгин krygin.ia@gmail.com
А.Р. Муллин alexandermullin@mail.com

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

Аннотация

Для определения важности защищаемых активов или ресурсов мобильного устройства предложено использовать модель игры с нулевой суммой. В игре участвуют стороны нападения и защиты. Для оптимизации своего показателя каждый игрок должен решать задачу линейного программирования при фиксированном решении другого игрока. В целях предсказуемости решения стороны нападения для стороны защиты предложено использовать принцип равной защищенности для классов активов. Активы разбиваются на классы с равной защищенностью. Для выравнивания защищенности внутри одного класса стороне защиты необходимо решить специально сформулированную задачу линейного программирования. Подход, основанный на выравнивании защищенности активов, позволяет обеспечить предсказуемый результат для стороны защиты, может применяться, когда нет полной информации о ресурсах нападающего. Приведен пример решения задачи

Ключевые слова

Информационная безопасность, игра с нулевой суммой, линейное программирование, равная защищенность

Поступила в редакцию 13.09.2017

Введение. В задачах, связанных с защитой информации, достаточно часто используются математические модели теории игр. В [1] представлен обзор работ, посвященных использованию моделей теории игр в области защиты информации. Дополнительно к этому обзору рассмотрим работы, опубликованные после выхода [1].

В [2] разработан алгоритм поиска оптимальных решений в выпуклых распределенных онлайн-задачах. Обучение осуществляется онлайн. Поскольку функция стоимости вычисляется последовательно — информация доступна только от соседних узлов и распространяется последовательно от узла к узлу. Предложена модификация алгоритма метода Эрроу — Гурвича для поиска седловой точки в целях выполнения глобального сетевого критерия Сэвиджа, при этом использован метод множителей Лагранжа. Представлено применение алгоритма к решению задачи обеспечения безопасности компьютерной сети, в которой сотрудничают провайдеры для обнаружения сигнатур вредоносных пользователей.

В [3] описан алгоритм маршрутизации в мобильных сенсорных сетях на основе моделей теории игр. В основе этого алгоритма лежат динамическая байесовская сигнальная игра и достижение полного байесовского равновесия (Perfect Bayesian Equilibrium — PBE). Алгоритм позволяет обеспечить защиту узлов от анонимных действий пользователей.

В [4] показано, как эволюционная теория игр может помочь в экономике организации для оптимизации затрат на системы информационной безопасности. В работе нарушения информационной безопасности описаны возможными экономическими потерями. Рассмотрены два вида нарушений безопасности: целенаправленные атаки и проявление стихийных (случайных) угроз. Также приведено соотношение инвестиций в информационную безопасность и возможных потерь.

В [5] представлены динамические игры с игроками, имеющими неполную информацию о ресурсах других игроков, применительно к киберфизическим системам. Также рассмотрена атака «Отказ в обслуживании» и разработан алгоритм для вычисления седловой точки.

В [6] рассмотрено применение теории игр в стеганографии. Авторы отмечают, что эта тема практически не освещена, так как до недавнего времени адаптивные атаки в области стеганографии не проводились. Рассмотрены игроки внедрения и обнаружения. Предложен алгоритм поиска седловой точки в смешанных стратегиях.

В [7] приведена стратегия для защиты сети с использованием концепции движущихся целей (Moving Target Defense — MTD), основанная на игре Маркова. Суть MTD — определенные элементы сети меняются во времени, затрудняя «поражение» цели. Марковский процесс принятия решения используется для описания переходов между мультисостояниями сети. Динамическая игра используется для описания многофазных шагов защиты и атаки в условиях MTD.

В [8] исследована аутентификация на физическом уровне, при этом использована информация о радиоканале для обнаружения атак спуфинга в MIMO-системах (Multiple-Input Multiple-Output). Приведено взаимодействие между приемником и узлом спуфинга в качестве игры с нулевой суммой.

В [9] рассмотрено применение обучения, основанного на теории игр, для анализа больших объемов данных. Такой подход может быть полезен для анализа данных социальных сетей. Рассмотрена линейная игровая модель многих игроков (агентов), данные которых хранятся в большом хранилище, с каждым агентом связана конфиденциальная информация. Модель является непрерывной. Выполнен поиск решений, удовлетворяющих критерию Нэша.

В [10] показано распределение ресурсов в каналах прослушивания с множественным доступом. В модели представлено несколько пользователей, которые хотят конфиденциально передать данные законному получателю. На принимающей стороне есть противник, который пассивно прослушивает канал и пытается декодировать сообщения. Рассмотрена стохастическая игра, решения ищутся оптимальные по Парето и по Нэшу.

В [11] приведено эффективное решение стохастической игры с нулевой суммой и недостаточной информацией игроков друг о друге. Также рассмотрена проблема раскрытия игроком собственной секретной информации для получения секретной информации противника и предложены стратегии для ее решения.

В [12, 13] для назначения классов защищенности объектам информационной системы и распределения данных по этим объектам в целях снижения размерности задачи дискретной оптимизации использован искусственный прием сведения оптимизационной задачи к игре двух игроков с непротивоположными интересами. Один игрок отвечает за назначения классов защищенности объектам, а второй — за распределение данных по объектам. Решение ищется оптимальное по Нэшу.

Игровые модели могут применяться и комбинироваться с другими математическими моделями в различных задачах [14–17], связанных с защитой информации.

Рассмотрим особенности защиты мобильных устройств, таких как ноутбуки, смартфоны, планшеты и даже «умные» часы, которые стали частью повседневной жизни. Они хранят информацию об активности пользователей в Интернете, следят за состоянием здоровья, помогают совершать покупки. Это приводит к тому, что устройства превращаются в хранилища конфиденциальной информации, которую следует защищать, кроме конфиденциальности необходимо также обеспечить сохранение целостности и доступности данных.

Особенности обеспечения информационной безопасности мобильных устройств связаны с существованием дополнительных угроз, не характерных для стационарных компьютеров, а также с повышением вероятности реализации некоторых общих угроз, таких как потеря и кража, угроз, связанных с подключением к беспроводным сетям. Кроме того, мобильные устройства имеют существенно меньшие вычислительные ресурсы. Таким образом, программные средства защиты мобильных устройств должны проектироваться с учетом этих ограничений, т. е. обеспечить информационную безопасность и минимально использовать вычислительные ресурсы устройства.

Особенно актуальной становится задача защиты данных мобильных устройств в связи с началом их активного использования в силовых структурах. В этом случае устройства могут обрабатывать и хранить данные определенного уровня секретности, поэтому необходимо обеспечить ряд требований, определенных руководящими документами различных ведомств.

Эти особенности делают актуальной задачу распределения ресурсов системы защиты информации между важными активами мобильного устройства (можно использовать термин защищаемый ресурс, но для устранения терминологической неоднозначности защищаемые ресурсы будем называть активами, а используемые для защиты вычислительные и другие ресурсы устройства — просто ресурсами).

Защищаемыми активами могут быть:

– целостность, доступность и конфиденциальность данных, хранимых на мобильных устройствах и передаваемых с устройства на устройство по различным каналам;

– целостность приложений, установленных на мобильном устройстве;

– неизменность множества установленных приложений;

– защита от несанкционированного использования в целях получения данных различных датчиков или систем мобильного устройства, таких как видеокамера, микрофон, навигационная система и др.

Для защиты устройства, как правило, используются программные средства. Под ресурсами системы защиты могут рассматриваться: процессорное время, оперативная память, дисковое хранилище, сетевое соединение, другие ресурсы.

Далее рассмотрим задачу распределения ресурсов мобильного устройства между активами, при этом будем использовать модель двух игроков с нулевой суммой. Игроками являются сторона защиты и сторона нападения. Часто при поиске решений в игровых задачах ищут седловую точку в чистых или смешанных стратегиях. Если рассматривать поиск решения с точки зрения стороны защиты, то подход, основанный на поиске седловой точки, возможен, когда существует полная информация о стороне нападения, что часто бывает не так. Будем использовать подход, который можно применять в случае неполной информации о ресурсах стороны нападения. Этот подход, по сути, близок к максиминному критерию, который гарантирует определенный выигрыш при наихудших условиях, но в данном случае обеспечивается предсказуемость поведения стороны нападения для защитника.

Постановка задачи, представленная далее, похожа на задачу, рассмотренную в [1], но в отличие от нее для стороны защиты существует не одно ограничение (ограничение на стоимость), а несколько ограничений на ресурсы мобильного устройства. Также в [1] рассмотренные алгоритмы были в основном ориентированы на получение седловой точки, если ее можно найти разработанными алгоритмами.

1. Математическая постановка задачи.

Исходные данные.

Базисные множества:

$Z = \{z_1, z_2, \ldots, z_m\}$ — множество защищаемых активов мобильного устройства; $M = \{1, 2, \ldots, m\}$ — множество индексов этих активов;

$R = \{r_1, r_2, \ldots, r_l\}$ — множество ограниченных ресурсов мобильного устройства (вычислительные ресурсы процессора, ресурсы памяти и дискового хранилища, ресурсы аккумуляторной батареи); $L = \{1, 2, \ldots, l\}$ — множество индексов этих ресурсов.

Параметры элементов множеств и отношений между ними:

$w_i > 0, \ \forall\, i \in M$ — возможный ущерб при нарушении безопасности i-го защищаемого актива (стоимость актива), рассматриваем активы, стоимости которых не равны нулю;

$c_{зi} \geq 0, \forall i \in M$ — предполагаемая стоимость защиты i-го актива;

$c_{нi} \geq 0, \forall i \in M$ — стоимость проведения атаки на защищаемый актив мобильного устройства со стороны нападения;

$p_{пр\,i} \in [0,1], \forall i \in M$ — вероятность (или возможность при нечетком описании) предотвращения атаки на i-й актив при использовании средств защиты, как правило, значение меньше единицы (значение 1 является идеальным случаем);

$a_{ji} \in [0, 1), \forall j \in L, i \in M$ — нормированное значение j-го ограниченного ресурса мобильного устройства, используемого для обеспечения защиты i-го актива, весь ресурс считается равным единице.

Искомые параметры.

Для стороны защиты введем переменные $x_i \in [0, 1], \forall i \in M$, имеющие содержательный смысл вероятности защиты i-го актива или возможность его защиты при описании в терминах нечетких множеств. Переменные образуют вектор $\vec{X}$. Для стороны нападения введем переменные $y_i \in [0, 1], \forall i \in M$, имеющие содержательный смысл вероятности атаки на актив или возможности атаки при описании в терминах нечетких множеств. Переменные образуют вектор $\vec{Y}$.

Показатели игроков.

Для игры с нулевой суммой показатели качества игроков определяются ущербом стороны защиты. Ущерб можно определить так:

$$U\left(\vec{X}, \vec{Y}\right) = U_{\max}\left(\vec{Y}\right) - U_{пр}\left(\vec{X}, \vec{Y}\right),$$

где $U_{\max}\left(\vec{Y}\right) = \sum\limits_{i \in M} w_i y_i$ — максимальный ущерб, который может быть нанесен стороной нападения при отсутствии защиты; $U_{пр}\left(\vec{X}, \vec{Y}\right) = \sum\limits_{i \in M} p_{pr\,i} w_i x_i y_i$ — ущерб, предотвращенный стороной защиты.

Тогда показатель качества стороны защиты, который она желает максимизировать, имеет вид

$$F_з\left(\vec{X}, \vec{Y}\right) = -U\left(\vec{X}, \vec{Y}\right) = \sum_{i \in M} p_{pr\,i} w_i x_i y_i - \sum_{i \in M} w_i y_i . \quad (1)$$

Показатель качества стороны нападения, который она желает максимизировать, имеет вид

$$F_н\left(\vec{X}, \vec{Y}\right) = U\left(\vec{X}, \vec{Y}\right) = \sum_{i \in M} w_i y_i - \sum_{i \in M} p_{pr\,i} w_i x_i y_i . \quad (2)$$

Ограничения.

Могут быть введены ограничения на стоимость ресурсов, выделенных на защиту и (или) нападение, они могут не вводиться, если считать, что для защитника и (или) нападающего все доступно по стоимости. Если ограничения вводятся, то для защитника ограничение имеет вид

$$\sum_{i \in M} c_{зi} x_i \le C_з^{(\max)}, \tag{3}$$

где $C_з^{(\max)}$ — максимальная стоимость ресурсов, выделенных на защиту.

Для стороны нападения ограничение на стоимость ресурсов, выделяемых на проведение атак, можно представить так:

$$\sum_{i \in M} c_{нi} y_i \le C_н^{(\max)}, \tag{4}$$

где $C_н^{(\max)}$ — максимальная стоимость ресурсов, выделенных на проведение атак.

Ограничения на использование ресурсов мобильного устройства имеют вид

$$\sum_{i \in M} a_{ji} x_i \le b_j, \forall j \in L, \tag{5}$$

где $b_j \in [0, 1)$ — максимальное нормированное значение j-го ограниченного ресурса, выделенного на защиту.

Не ограничивая общность постановки задачи, ограничение (3) на стоимость для стороны защиты можно включить в систему ограничений на ресурсы (5) как дополнительное ограничение (максимальную стоимость можно рассматривать как ограниченный ресурс).

Получаем игру с нулевой суммой, в отличие от матричной игры с нулевой суммой [18] множества допустимых альтернатив игроков являются непрерывными. При принятии решения каждым игроком (поиск неизвестного вектора $\vec{X}$ или $\vec{Y}$) при фиксированном решении другого игрока ему приходится решать задачу линейного программирования (ЗЛП). Для стороны защиты при фиксированном решении стороны нападения $\vec{Y}$ необходимо решать задачу максимизации показателя (1) и системой ограничений (5) с учетом $x_i \in [0, 1], \forall i \in M$. Для стороны нападения при фиксированном решении стороны защиты $\vec{X}$ необходимо решать задачу максимизации показателя (2) с одним ограничением на стоимость (4) с учетом $y_i \in [0, 1], \forall i \in M$.

2. Алгоритмы поиска решения стороной защиты на основе равной защищенности активов. Существуют тривиальные случаи, когда защитник и (или) нападающий не ограничены в ресурсах, т. е. допустимо решение, состоящее из всех единиц. В этих случаях решение, состоящее из всех единиц, будет оптимальным, а второму игроку необходимо решить свою ЗЛП. Далее рассмотрим случай, когда решения, все состоящие из единиц, являются недопустимыми для игроков по ограничениям. Остановимся на подходе к решению со стороны защитника, при этом будем учитывать стратегию принятия решений со стороны нападения. Сторона нападения решает задачу линейного программирования с показателем (2) и одним ограничением (4). В этом случае, как доказано в [1], для получения точного решения можно использовать модификацию «жадного» алгоритма. Рассмотрим основы этого алгоритма.

2.1. Алгоритм решения задачи линейного программирования с одним ограничением стороной нападения на основе «жадного» алгоритма. Алгоритм работает для заданного решения стороны защиты — $\vec{X}$. Перед работой алгоритма полагаем $\vec{Y} = \|0,0,0,\ldots,0\|^{\mathrm{T}}$ (все компоненты равны нулю), $C_{\text{н}}^{(\text{ост})} = C_{\text{н}}^{(\max)}$ — значение оставшегося ресурса стоимости, $M' = M$ — множество индексов активов, еще не выбранных алгоритмом.

Сторона нападения на каждом шаге алгоритма для фиксированного вектора $\vec{X}$ ищет $\max\limits_{i \in M'} \dfrac{w_i - p_{pr\,i} w_i x_i}{c_{\text{н}i}}$. Выражение $v_i(x_i) = \dfrac{w_i - p_{pr\,i} w_i x_i}{c_{\text{н}i}}$ задает выигрыш игрока нападения, приходящийся на единицу ресурса стоимости, затраченного на атаку актива. Пусть $i^* = \arg\max\limits_{i \in M'} v_i(x_i)$ (в случае существования нескольких максимумов выбирается любой из них), тогда, если ограничение (4) позволяет, т. е. $C_{\text{н}}^{(\text{ост})} \geq c_{\text{н}i^*}$, компоненте y_{i^*} присваиваем значение 1, i^* исключаем из множества M', полагаем $C_{\text{н}}^{(\text{ост})} = C_{\text{н}}^{(\text{ост})} - c_{\text{н}i^*}$, переходим к следующему шагу. Если ограничение (4) не позволяет присвоить y_{i^*} значение 1, т. е. $C_{\text{н}}^{(\text{ост})} < c_{\text{н}i^*}$, то $y_{i^*} = \dfrac{C_{\text{н}}^{(\text{ост})}}{c_{\text{н}i^*}}$, работа алгоритма завершена.

2.2. Понятие класса активов с равной защищенностью. Когда сторона защиты выбирает значение компонент вектора $\vec{X}$, то она задает значения $v_i(x_i)$, $\forall i \in M$, которые определяют степень или уровень угрозы для i-го актива со стороны нападения, для стороны защиты эти значения можно интерпретировать как степени защищенности. Чем меньше $v_i(x_i)$, тем меньше уровень угрозы и тем выше степень защищенности. Желательно определить такой вектор $\vec{X}$, чтобы значения $v_i(x_i)$ сделать меньше. Если сделать все значения $v_i(x_i)$ или некоторые из них равными, то для равных значений $v_i(x_i)$ стороне нападения безразлично, как распределять свои ресурсы, можно считать, что для этих активов стороной защиты обеспечивается равная защищенность.

Введем для любого актива следующие понятия:

– максимальная степень угрозы (или минимальная защищенность), при атаке на актив она равна $v_i^{(\max)} = \dfrac{w_i}{c_{\text{н}i}}, \forall i \in M,$ в этом случае компонента вектора $x_i = 0,$ т. е. сторона защиты не защищает этот актив;

– минимальная степень угрозы (максимальная защищенность) $v_i^{(\min)} = \dfrac{w_i - p_{pr\,i} w_i x_i}{c_{\text{н}i}}, \forall i \in M,$ где $x_i = 1$, если $a_{ji} \leq b_j, \forall j \in L$ (ресурсов хватает для полной защиты актива), $x_i = \min\limits_{j \in L} \dfrac{b_j}{a_{ji}}$ в противном случае (существует ограниченный ресурс, которого не хватает для полной защиты актива).

Для некоторого вектора $\vec{X}$ все множество активов можно разбить на *непересекающиеся* множества (классы), для множества индексов активов можно записать $M = M^{(1)} \cup M^{(2)} \cup \ldots \cup M^{(n)}$ (возможно существование одного класса $M = M^{(1)}$, $n = 1$, также число классов может быть равно числу активов $n = m$). Для активов каждого класса обеспечивается равная степень защищенности $V^{(k)}$, т. е. $v_i(x_i) = V^{(k)}, \forall i \in M^{(k)}$. Нумерация классов упорядочена так, что $V^{(k)} > V^{(k+1)}, \forall k \in \{1, 2, \ldots, n-1\}$, если $n > 1$. Назовем эти классы активов классами с равной защищенностью. На рис. 1, *а* приведен пример двух активов с индексами *i* и *j*, которые не могут принадлежать одному классу с равной защищенностью. На координатной оси показаны для активов значения $v_j^{(\min)}$, $v_j^{(\max)}$, $v_i^{(\min)}$, $v_i^{(\max)}$, дуга на рисунке соединяет минимальное и максимальное значения степени угрозы для актива. Поскольку отрезки, заданные дугами на координатной оси, не пересекаются, то невозможно обеспечить одинаковую степень угрозы или степень защищенности для этих активов.

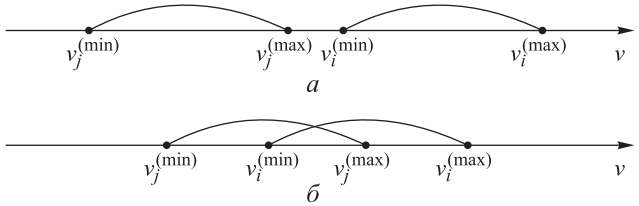

Рис. 1. Пример активов, для которых невозможно (*а*) и возможно (*б*) обеспечить равную защищенность

На рис. 1, *б* представлен пример двух активов с индексами *i* и *j*, которые могут принадлежать одному классу с равной защищенностью, выравнивание в этом случае возможно, так как отрезки, заданные дугами, пересекаются. При выравнивании значения степеней угрозы для двух активов (или значения уровней защищенности) будут находиться в интервале $\left[v_i^{(\min)}, v_j^{(\max)} \right]$.

Получение защитником решения, обеспечивающего классы активов равной защищенностью, гарантирует предсказуемость стороны нападения при использовании алгоритма, описанного в пункте 2.1, сторона нападения в первую очередь будет выбирать для нападения активы класса $M^{(1)}$, затем $M^{(2)}$ и т. д.

Рассмотрим алгоритм построения классов с равной защищенностью и его обоснование.

2.3. Алгоритм построения классов с равной защищенностью.

Шаг 0. Полагаем $k = 1$ (номер рассматриваемого класса с равной защищенностью), $M^{(\text{ост})} = M$ — множество оставшихся индексов активов (активы, не включенные в классы), $b_j^{(\text{ост})} = b_j, \forall j \in L$ — значения оставшихся ресурсов. Все элементы вектора $\vec{X}$ равны нулю.

Шаг k (k = 1, 2, …, максимальное число шагов m, возможно меньше). Полагаем $V^{(k)} = \max\limits_{i \in M^{(\text{ост})}} v_i^{(\min)}$, пусть $h \in M^{(\text{ост})}$ — индекс актива, являющийся решением этой задачи (если задача имеет несколько решений, ты выбираем любое). Актив с индексом h определяет минимальную степень угрозы для активов формируемого k-го класса. Находим индексы активов, которые потенциально могут входить в k-й класс, эти индексы задаются множеством $M^{(k)} = \left\{ j \mid v_j^{(\max)} \geq V^{(k)},\ j \in M^{(\text{ост})} \right\}$ и определяют активы, для которых интервалы изменения степени угрозы пересекаются по аналогии с рис. 1, *б*, для них потенциально возможно обеспечить равную защищенность.

Для демонстрации работы алгоритма будем использовать рис. 2. Видно, что дуга соединяет минимальное и максимальное значения степени угрозы для актива на координатной оси. Не уменьшая общности, на рис. 2 активы пронумерованы в порядке убывания минимальных степеней угрозы, номер актива стоит у точки на координатной оси, соответствующей минимальной степени угрозы. Для примера (см. рис. 2), на первом шаге значение $V^{(1)}$ соответствует точке 1 (h = 1), а индексы активов, потенциально входящие в первый класс, $M^{(1)} = \{1, 2, 10\}$. Минимальная степень угрозы для этого потенциального класса с активами 1, 2, 10 может быть равна значению $V^{(1)}$, если позволят ресурсы. Проверяем, позволяют ли это ресурсы, т. е. допустимо ли по ограничениям (5) решение, в котором x_1 = 1, $x_2 = \dfrac{w_2 - V^{(1)} c_{\text{н}2}}{p_{pr\,2} w_2}$, $x_{10} = \dfrac{w_{10} - V^{(1)} c_{\text{н}10}}{p_{pr\,10} w_{10}}$, значения x_2 и x_{10} получены из условия $\dfrac{w_i - p_{pr\,i} w_i x_i}{c_{\text{н}i}} = V^{(k)} \Rightarrow x_i = \dfrac{w_i - V^{(k)} c_{\text{н}i}}{p_{pr\,i} w_i}$.

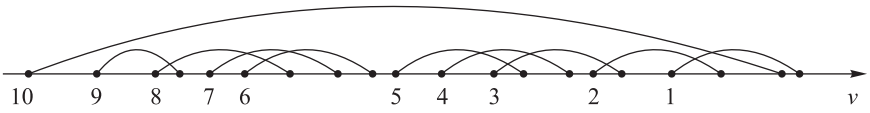

Рис. 2. Демонстрация построения классов с одинаковой степенью угрозы (равной защищенностью)

Возможны два случая.

1. *Решение допустимое*. В этом случае считаем, что класс $M^{(k)}$ содержит один индекс h, полагаем x_h = 1 (для рис. 2 при k = 1, x_1 = 1). Для актива с индексом 1 (см. рис. 2) степень угрозы нельзя уменьшить, а для активов 2 и 10 степени угрозы можно уменьшить (ресурсы позволяют), поэтому $M^{(1)} = \{1\}$. Индекс h исключаем из множества $M^{(\text{ост})}$, полагаем $b_j^{(\text{ост})} = b_j^{(\text{ост})} - a_{jh}, \forall\, j \in L$, $k = k + 1$, переходим к следующему шагу.

После первого шага (см. рис. 2), если решение допустимое, то x_1 = 1. На втором шаге (см. рис. 2) $V^{(2)} = \max\limits_{i \in M^{(\text{ост})}} v_i^{(\min)}$ будет в точке 2, а индексы активов, потенциально входящих во второй класс, $M^{(2)} = \{2, 3, 10\}$.

2. *Решение недопустимое*. В этом случае для выбранных активов, потенциально входящих в k-й класс, невозможно обеспечить степень угрозы со значением $V^{(k)}$, так как ресурсы не позволяют. Далее постараемся выравнить степени угрозы для активов, потенциально входящих в класс $M^{(k)}$, распределив между этими активами ресурсы защиты, при этом степень угрозы будет больше, чем $V^{(k)}$. Для этого рассмотрим отдельный алгоритм, основанный на решении задачи линейного программирования.

2.4. Алгоритм выравнивания защищенности активов внутри класса на основе решения задачи линейного программирования. Рассмотрим, как распределить ресурсы защиты между активами, индексы которых потенциально входят в некоторый класс $M^{(k)}$, если ресурсы не позволяют обеспечить степень угрозы $V^{(k)} = \max\limits_{i \in M^{(\text{ост})}} v_i^{(\min)}$. При этом для активов, индексы которых принадлежат классам $M^{(j)}$, $j < k$, если они существуют, т. е. $k > 1$, обеспечена полная защита $x_i = 1$, $\forall i \in M^{(j)}$. При распределении ресурсов между активами, индексы которых потенциально входят в класс $M^{(k)}$, в правых частях ограничений (5) будут оставшиеся ресурсы $b_j^{(\text{ост})}$, $\forall j \in L$ после выделения ресурсов на защиту активов, индексы которых принадлежат классам $M^{(j)}$, $j < k$, если эти классы существуют.

Шаг i (i = 1, 2, …, максимальное число шагов $card(M^{(k)})$, возможно меньше). Если число элементов множества $card(M^{(k)}) = 1$, то решение тривиальное $x_i = \min\limits_{j \in L} \dfrac{b_j^{(\text{ост})}}{a_{ji}}$, $i \in M^{(k)}$. Если $card(M^{(k)}) > 1$, то для выравнивания степени угрозы необходимо решить следующую задачу линейного программирования:

$$F\left(\vec{X}^{(k)}\right) = v_g\left(x_g\right) = \frac{w_g - p_{pr\,g}\, w_g\, x_g}{c_{\text{нg}}} \to \min_{\vec{X}^{(k)} \in \Delta_{\text{доп}}^{(k)}}, \quad g \in M^{(k)}, \tag{6}$$

$$\Delta_{\text{доп}}^{(k)}: \begin{cases} \dfrac{w_i - p_{pr\,i}\, w_i\, x_i}{c_{\text{н}i}} \le \dfrac{w_g - p_{pr\,g}\, w_g\, x_g}{c_{\text{нg}}}, \ \forall i \in M^{(k)}, \ i \ne g, \\ \sum\limits_{i \in M^{(k)}} a_{ji}\, x_i \le b_j^{(\text{ост})}, \ \forall j \in L, \\ x_i \le 1, \forall\ i \in M^{(k)}, \\ x_i \ge 0, \forall\ i \in M^{(k)}, \end{cases} \tag{7}$$

где $\vec{X}^{(k)}$ — вектор искомых переменных, состоящий из элементов исходного вектора $\vec{X}$, соответствующих активам, индексы которых предварительно входят в множество $M^{(k)}$; $g \in M^{(k)}$ — индекс актива, который является решением задачи $\min\limits_{i \in M^{(k)},\, v_i^{(\max)} > V^{(k)}} v_i^{(\max)}$ (выбираем актив, который имеет минимальную

степень угрозы среди максимальных степеней угрозы, это значение максимально близко к $V^{(k)}$, которое недостижимо, и больше, чем $V^{(k)}$); $\Delta_{\text{доп}}^{(k)}$ — множество допустимых альтернатив, соответствующее вектору $\vec{X}^{(k)}$, заданное системой неравенств. Показатель качества определяется одним активом с индексом $g \in M^{(k)}$, степень угрозы $v_g\left(x_g\right)$ для g-го актива минимизируем, при этом степени угрозы для всех остальных активов, индексы которых входят в $M^{(k)}$, должны быть не больше, чем $v_g\left(x_g\right)$, что задается в ограничениях. Значение $v_g^{(\max)}$ на координатной оси показано на рис. 3.

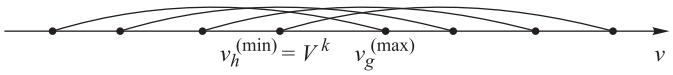

Рис. 3. Значение $v_g^{(\max)}$ на координатной оси

Докажем, что в случае, если решение задачи с показателем (6) и системой ограничений (7) существует, то оно обеспечивает равную защищенность. Предположим, что для оптимального решения задачи существует актив $\exists i \in M^{(k)}$, $i \neq g$, $v_i\left(x_i\right) = \dfrac{w_i - p_{pr\,i}\, w_i\, x_i}{c_{\text{н}i}} < v_g\left(x_g\right) = \dfrac{w_g - p_{pr\,g}\, w_g\, x_g}{c_{\text{н}g}}$, в этом случае всегда $x_i > 0$, так как при $x_i = 0$ $v_i\left(x_i\right) = v_i^{(\max)}$, а $v_i^{(\max)} \geq v_g^{(\max)} \geq v_g\left(x_g\right)$ всегда, что противоречит условию $v_i\left(x_i\right) < v_g\left(x_g\right)$. Но если $x_i > 0$, тогда x_i можно уменьшить на некоторую, возможно бесконечно малую величину Δx_i так, чтобы увеличившееся значение $v_i\left(x_i\right)$ не нарушило условие $v_i\left(x_i\right) < v_g\left(x_g\right)$, при этом освободится часть ресурсов, и можно увеличить на некоторое (возможно бесконечно малое) значение Δx_g переменную x_g, что приведет к уменьшению $v_g\left(x_g\right)$, но тогда полученное ранее решение не является оптимальным, следовательно, предположение $\exists i \in M^{(k)}$, $i \neq g$, $v_i\left(x_i\right) < v_g\left(x_g\right)$ неверное.

При решении задачи (6) с ограничениями (7) возможны следующие случаи.

1. Задача имеет решение, в этом случае работа алгоритма завершена. Для активов, индексы которых входят в множество $M^{(k)}$, обеспечена равная защищенность. Индексы этих активов исключаются из множества $M^{(\text{ост})}$. Для оставшихся активов, индексы которых входят в $M^{(\text{ост})}$, полагаем $x_j = 0$, $\forall\, j \in M^{(\text{ост})}$ (ресурсы для защиты закончились). Их сортируем в порядке невозрастания $v_j^{(\max)}$ и назначаем им номера классов с равной защищенностью, начиная с номера $k+1$ (каждый класс состоит, как правило, из одного индекса, за исключением случаев, когда $v_j^{(\max)} = v_i^{(\max)}$, $\exists\, i, j \in M^{(\text{ост})}$, $i \neq j$).

2. Задача не имеет решения из-за недостатка ресурсов. Пример для класса из двух активов представлен на рис. 4.

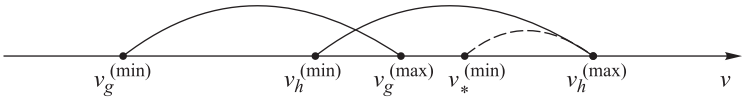

Рис. 4. Пример, когда для потенциального класса из двух активов решения не существует

На рис. 4 показано, что ресурсы позволяют снизить степень угрозы для h-го объекта только до уровня $v_*^{(\min)} > v_g^{(\max)}$. Значение $v_g^{(\max)}$ недостижимо, поэтому ограничения (7) не могут быть выполнены.

На рис. 5 приведен пример с большим числом активов, при этом для активов с индексами i и h ресурсы позволили уменьшить степень угрозы до значения $v_*^{(\min)}$, что больше, чем $v_g^{(\max)}$, в этом случае решения задачи также не существует.

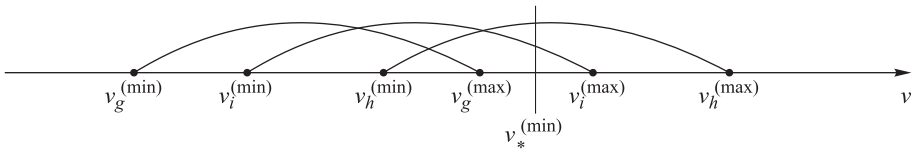

Рис. 5. Пример, когда решения ЗЛП не существует, $v_g^{(\max)} < v_*^{(\min)}$

В подобных случаях, когда решения задачи (6) с ограничениями (7) не существует, поступаем следующим образом: из множества $M^{(k)}$ исключаем элемент с индексом g, полаем, что $x_g = 0$, и переходим к шагу $i + 1$. В этом случае можно считать, что число множеств (классов) с одинаковой защищенностью увеличивается на единицу, актив с индексом g может потенциально входить в класс с индексом $k + 1$ (класс с меньшей степенью угрозы). Переходим к шагу $i + 1$.

3. Пример решения задачи. Рассмотрим пример решения задачи со следующими параметрами: число активов 10, число ресурсов мобильного устройства 3. Основные параметры защищаемых активов (оценка возможного ущерба при нарушении защиты актива, оценка стоимости программного обеспечения для защиты актива, оценка стоимости проведения атаки на актив, вероятность или возможность предотвращения атаки при использовании средств защиты) представлены в табл. 1. Значения стоимостей зависят от целей использования мобильного устройства, особенностей пользователя, которому принадлежит устройство, они заданы примерно в условных единицах (у. е.).

Будем учитывать следующие ресурсы мобильного устройства, расходуемые на работу дополнительных приложений для защиты активов: загрузку процессора, загрузку оперативной памяти, загрузку дискового хранилища. Параметры этих ресурсов и значения правых частей ограничений на использование этих ресурсов приведены в табл. 2.

Результаты решения задачи с исходными данными описанными ранее алгоритмами сведены в табл. 3.

Таблица 1

Параметры защищаемых активов

Номер п/п	Название защищаемого актива	Размер возможного ущерба при нарушении защиты (w_i, $\forall\, i \in M$), у. е.	Стоимость защиты ($c_{зi}, \forall i \in M$), у. е.	Стоимость атаки ($c_{нi}, \forall i \in M$), у. е.	Вероятность предотвращения атаки ($p_{пр\,i}, \forall i \in M$)
1	Целостность и доступность данных на устройстве	4000	100	50	0,80
2	Конфиденциальность данных на устройстве	10000	1000	600	0,99
3	Целостность и доступность передаваемых данных	3000	200	60	0,70
4	Конфиденциальность передаваемых данных	8000	900	500	0,90
5	Целостность приложений на устройстве	5000	400	100	0,80
6	Неизменность множества установленных приложений (запрет на несанкционированную установку приложений)	8000	500	120	0,90
7	Конфиденциальность данных на устройстве в случае потери или кражи	10000	1200	1000	0,50
8	Защита видеокамеры от несанкционированного использования приложениями	8000	1000	500	0,90
9	Защита микрофона от несанкционированного использования приложениями	15000	1000	500	0,90
10	Защита навигационной системы от несанкционированного использования приложениями	7000	1000	500	0,90
Всего выделено на защиту ($C_з^{(max)}$) и нападение ($C_н^{(max)}$), у. е.		–	3000	1500	–

Таблица 2

Ресурсы мобильного устройства, расходуемые на защиту активов

Номер п/п	Название защищаемого актива	Нормированное значение ограниченного ресурса мобильного устройства, используемого для обеспечения защиты актива $(a_{ji}, \forall j \in L, i \in M)$		
		Загрузка процессора	Загрузка оперативной памяти	Загрузка дискового хранилища
1	Целостность и доступность данных на устройстве	0,03	0,05	0,01
2	Конфиденциальность данных на устройстве	0,10	0,10	0,05
3	Целостность и доступность передаваемых данных	0,05	0,10	0,02
4	Конфиденциальность передаваемых данных	0,15	0,10	0,05
5	Целостность приложений на устройстве	0,10	0,10	0,02
6	Неизменность множества установленных приложений (запрет на несанкционированную установку приложений)	0,10	0,10	0,01
7	Конфиденциальность данных на устройстве в случае потери или кражи	0,10	0,10	0,01
8	Защита видеокамеры от несанкционированного использования приложениями	0,10	0,10	0,01
9	Защита микрофона от несанкционированного использования приложениями	0,10	0,10	0,01
10	Защита навигационной системы от несанкционированного использования приложениями	0,10	0,10	0,01
Всего выделено нормированного значения на защиту $(b_j, \forall j \in L)$		0,40	0,40	0,20

Таблица 3

Результаты решения задачи

Параметры	Значения параметров									
$\vec{X}^{(1)}$	1,000	0,095	0,997	0,062	0,872	0,859	0,000	0,062	0,552	0,000
Значения $v_i(x_i)$	16,000	15,103	15,103	15,103	15,103	15,103	10,000	15,103	15,103	14,000
Номер класса	1	2	2	2	2	2	4	2	2	3
$\vec{Y}^{(1)}$ ущерб 22699.20 у. е.	1,000	0,650	1,000	1,000	0,000	0,000	0,000	1,000	0,000	0,000
$\vec{X}^{(2)}$, ущерб 4956.88 у. е.	1,000	0,875	0,625	1,000	0,000	0,000	0,000	1,000	0,000	0,000
$\vec{Y}^{(2)}$, ущерб 39187.50 у. е.	1,000	0,000	1,000	0,000	1,000	1,000	0,170	0,000	1,000	1,000
$\vec{Y}^{(11)}$, ущерб 22699.2 у. е.	1,000	0,515	1,000	0,708	1,000	0,708	0,000	0,708	0,377	0,000
$\vec{X}^{(11)}$, ущерб 18867.50 у. е.	1,000	1,000	0,000	0,400	0,100	1,000	0,000	0,000	1,000	0,000
$\vec{Y}^{(12)}$, ущерб 26369.60 у. е.	1,000	0,000	1,000	0,580	1,000	0,000	0,000	1,000	0,000	1,000

В первой строке табл. 3 заданы значения компонент вектора $\vec{X}^{(1)}$, найденные описанными ранее алгоритмами для получения классов с равными защищенностями. В следующей строке заданы значения степеней угроз для активов, соответствующие полученному вектору $\vec{X}^{(1)}$. В третьей строке для каждого актива задан номер класса с равной защищенностью, которому актив принадлежит.

Всего получено 4 класса:

– *класс 1* состоит из одного актива со степенью угрозы 16,000, значение компоненты вектора $\vec{X}$ для этого актива равно единице;

– *класс 2* состоит из семи активов, для них обеспечена равная степень угрозы — 15,103, это означает, что стороне нападения безразлично с точки зрения введенного показателя, на какие активы этого класса осуществлять атаки, между этими активами были распределены оставшиеся ресурсы стороны защиты с помощью решения ЗЛП алгоритмом, описанным в пункте 2.4;

– *классы 3 и 4* включают по одному активу, значения степеней угроз для этих классов — 14,000 и 10,000, для защиты этих активов стороне защиты ресурсов не хватило, поэтому значения компонент вектора $\vec{X}^{(1)}$, соответствующие этим активам, равны нулю.

Следующая строка задает значения вектора $\vec{Y}^{(1)}$, данное решение получено алгоритмом, описанным в пункте 2.1, значение показателя ущерба при этом было 22699.2 у. е. Следующая строка задает решение $\vec{X}^{(2)}$, полученное путем решения

ЗЛП с показателем (1) и ограничениями (5) при заданном $\vec{Y}^{(1)}$, полученный ущерб при этом 4956.88 у. е., что меньше, чем 22699.20 у. е., и для защитника более предпочтительно. Но если сторона нападения при заданном $\vec{X}^{(2)}$ будет решать свою ЗЛП с показателем (2) и ограничением (4), то будет получено решение $\vec{Y}^{(2)}$, представленное в следующей строке таблицы, с ущербом 39187.50 у. е., что существенно хуже, чем значение 22699.20, которое было гарантировано изначально.

Строка ниже задает альтернативное решение стороны нападения — $\vec{Y}^{(11)}$: также осуществляется полная атака на актив класса 1, а распределение ресурсов для атак на объекты класса 2 было получено с помощью генератора псевдослучайных чисел. Для атак на активы классов 3 и 4 ресурсов стороны нападения не хватило, при этом было получено такое же значение показателя качества — значение ущерба 22699.2 у. е., как для решения $\vec{Y}^{(1)}$. Строки ниже задают решения игроков, полученные при решении своих ЗЛП по аналогии со строками выше. Решение $\vec{X}^{(11)}$ получено при заданном $\vec{Y}^{(11)}$, ущерб составил 18867.50 у. е., что меньше, чем исходное значение 22699.2 у. е. В последней строке решение $\vec{Y}^{(12)}$ получено при заданном $\vec{X}^{(11)}$, ущерб составил 26369.60 у. е., что больше исходного решения.

Заключение. В статье рассмотрена постановка задачи распределения ресурсов мобильного устройства между защищаемыми активами. Постановка задачи являлась игрой с нулевой суммой, при этом каждый игрок (сторона нападения и сторона защиты) для получения своего решения должен решать задачу линейного программирования при фиксированном решении другого игрока. Для получения решения стороной защиты предложен подход, основанный на разбиении всех защищаемых активов на классы с равными защищенностями или равными степенями угрозы. Этот подход позволяет предсказать защитнику выбор стороны нападения, в том числе и в случае, когда защитнику не известна информация о ресурсах нападающего. Для обеспечения равной защищенности активов (выравнивание защищенности), входящих в один класс, предложено решать специально сформулированную задачу линейного программирования.

Результаты решения тестового примера показали, что выбор нападающего в рамках предложенной модели игры становится предсказуемым, в первую очередь нападающий атакует классы объектов с наименьшей защищенностью. При атаке на активы класса с равной защищенностью для стороны нападения все равно с точки зрения своего показателя качества, как распределять ресурсы между этими активами. Проведенный анализ и решение тестовой задачи показали, что стороне защиты не имеет смысла отклоняться от решения, полученного на основе равной защищенности классов активов, если сторона нападения решает свою оптимизационную задачу. При заданном решении стороны нападения сторона защиты может улучшить для себя значение показателя, отклонившись от решения, полученного на основе принципа равной защищенности, решив свою оптимизационную задачу. Но в этом случае, как правило, сторона нападения может существенно ухудшить значение показателя для стороны за-

щиты, решив свою оптимизационную задачу для нового решения защитника. Таким образом, решение стороны защиты, полученное на основе принципа равной защищенности активов, можно рассматривать как решение, позволяющее предсказать результат при известном значении ресурсов стороны нападения, при неизвестном значении ресурсов стороны нападения можно предсказать приоритеты нападающего при выборе активов для атаки.

ЛИТЕРАТУРА

1. *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 URL: http://technomag.bmstu.ru/doc/812283.html

2. *Koppel A., Jakubiec F.Y., Ribeiro A.* A saddle point algorithm for networked online convex optimization // IEEE Transactions on Signal Processing. 2015. Vol. 63. No. 19. P. 5149–5164. DOI: 10.1109/TSP.2015.2449255 URL: http://ieeexplore.ieee.org/document/7131577

3. *Paramasivan B., Prakash M., Kaliappan M.* Development of a secure routing protocol using game theory model in mobile ad hoc networks // Journal of Communications and Networks. 2015. Vol. 17. No. 1. P. 75–83. DOI: 10.1109/JCN.2015.000012
URL: http://ieeexplore.ieee.org/document/7059537

4. *Wang Q., Zhu J.* Optimal information security investment analyses with the consideration of the benefits of investment and using evolutionary game theory // 2016 2nd Int. Conf. on Information Management (ICIM). 2016. P. 105–109. DOI: 10.1109/INFOMAN.2016.7477542
URL: http://ieeexplore.ieee.org/document/7477542

5. *Gupta A., Langbort C., Başar T.* Dynamic games with asymmetric information and resource constrained players with applications to security of cyberphysical systems // IEEE Transactions on Control of Network Systems. 2017. Vol. 4. No. 1. P. 71–81. DOI: 10.1109/TCNS.2016.2584183
URL: http://ieeexplore.ieee.org/document/7498672

6. *Schöttle P., Böhme R.* Game theory and adaptive steganography // IEEE Transactions on Information Forensics and Security. 2016. Vol. 11. No. 4. P. 760–773. DOI: 10.1109/TIFS.2015.2509941
URL: http://ieeexplore.ieee.org/document/7360156

7. *Lei C., Ma D., Zhang H.* Optimal strategy selection for moving target defense based on Markov game // IEEE Access. 2017. Vol. 5. P. 156–169. DOI: 10.1109/ACCESS.2016.2633983
URL: http://ieeexplore.ieee.org/document/7805250

8. *Channel-based* authentication game in MIMO systems / L. Xiao, T. Chen, G. Han, W. Zhuang, L. Sun // 2016 IEEE Global Communications Conf. (GLOBECOM). 2016. P. 1–6.
DOI: 10.1109/GLOCOM.2016.7841657 URL: http://ieeexplore.ieee.org/document/7841657

9. *Chessa M., Grossklags J., Loiseau P.* A game-theoretic study on non-monetary incentives in data analytics projects with privacy implications // 2015 IEEE 28th Computer Security Foundations Symposium. 2015. P. 90–104. DOI: 10.1109/CSF.2015.14
URL: http://ieeexplore.ieee.org/document/7243727

10. *Shah S.V., Chaitanya A.K., Sharma V.* Resource allocation in fading multiple access wiretap channel via game theoretic learning // 2016 Information Theory and Applications Workshop (ITA). 2016. P. 1–7. DOI: 10.1109/ITA.2016.7888137
URL: http://ieeexplore.ieee.org/document/7888137

11. *Li L., Shamma J.* Efficient computation of discounted asymmetric information zero-sum stochastic games // 54th IEEE Conf. on Decision and Control (CDC). 2015. P. 4531–4536. DOI: 10.1109/CDC.2015.7402927 URL: http://ieeexplore.ieee.org/document/7402927

12. *Быков А.Ю., Панфилов Ф.А., Ховрина А.В.* Алгоритм выбора классов защищенности для объектов распределенной информационной системы и размещения данных по объектам на основе приведения оптимизационной задачи к задаче теории игр с непротивоположными интересами // Наука и образование: научное издание. 2016. № 1. DOI: 10.7463/0116.0830972 URL: http://technomag.bmstu.ru/doc/830972.html

13. *Быков А.Ю., Панфилов Ф.А., Зенькович С.А.* Модель и методы многокритериального выбора классов защищенности для объектов распределенной информационной системы и размещения баз данных по объектам // Вопросы кибербезопасности. 2016. № 2 (15). С. 9–20.

14. *Ключарёв П.Г.* Реализация криптографических хэш-функций, основанных на обобщенных клеточных автоматах, на базе ПЛИС: производительность и эффективность // Наука и образование: научное издание. 2014. № 1. DOI: 10.7463/0114.0675812 URL: http://technomag.bmstu.ru/doc/675812.html

15. *Балк Е.А., Ключарёв П.Г.* Исследование характеристик лавинного эффекта обобщенных клеточных автоматов на основе графов малого диаметра // Наука и образование: научное издание. 2016. № 4. DOI: 10.7463/0416.0837506 URL: http://technomag.bmstu.ru/doc/837506.html

16. *Ключарёв П.Г.* Производительность поточных шифров, основанных на клеточных автоматах, при реализации на графических процессорах // Наука и образование: научное издание. 2016. № 6. DOI: 10.7463/0616.0842091 URL: http://old.technomag.edu.ru/doc/842091.html

17. *Ключарёв П.Г.* Метод построения криптографических хэш-функций на основе итераций обобщенного клеточного автомата // Вопросы кибербезопасности. 2017. № 1 (19). С. 45–50. DOI: 10.21581/2311-3456-2017-1-45-50

18. *Стрекаловский А.С., Орлов А.В.* Биматричные игры и билинейное программирование. М.: Физматлит, 2007. 224 с.

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).

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

Муллин Александр Ренатович — магистрант 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., Крыгин И.А., Муллин А.Р. Алгоритмы распределения ресурсов системы защиты между активами мобильного устройства на основе игры с нулевой суммой и принципа равной защищенности // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2018. № 2. С. 48–68. DOI: 10.18698/0236-3933-2018-2-48-68

SCHEDULING ALGORITHMS OF THE PROTECTION SYSTEM BETWEEN ASSETS OF A MOBILE DEVICE ON THE BASIS OF ZERO-SUM GAME AND EQUAL SECURITY PRINCIPLE

A.Yu. Bykov abykov@bmstu.ru
I.A. Krygin krygin.ia@gmail.com
A.R. Mullin alexandermullin@mail.com

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

To determine the importance of the protected assets or resources of a mobile device, we suggest using the zero-sum game model. The game involves the parties to attack and defense. To optimize their indicator, each player must solve the linear programming problem with a fixed decision of the other player. In order to predict the decision of the attack, it is suggested for the defense using the equal security principle for asset classes. The assets are divided into classes with equal security. To equalize the security within one class, the defense should solve the specially formulated linear programming problem. The approach based on equalizing the assets security provides a predictable result for the defense and can be used when there is no complete information about the resources of the attack. An example of the solution of the problem is given

Keywords

Information security, zero-sum game, linear programming, equal security

Received 13.09.2017

REFERENCES

[1] Bykov A.Yu., Shmatova E.S. The algorithms of resource distribution for information security between objects of an information system based on the game model and principle of equal security of objects. *Nauka i obrazovanie: nauchnoe izdanie* [Science and Education: Scientific Publication], 2015, no. 9 (in Russ.). DOI: 10.7463/0915.0812283
Available at: http://technomag.bmstu.ru/doc/812283.html

[2] Koppel A., Jakubiec F.Y., Ribeiro A. A saddle point algorithm for networked online convex optimization. *IEEE Transactions on Signal Processing*, 2015, vol. 63, no. 19, pp. 5149–5164. DOI: 10.1109/TSP.2015.2449255 Available at: http://ieeexplore.ieee.org/document/7131577

[3] Paramasivan B., Prakash M., Kaliappan M. Development of a secure routing protocol using game theory model in mobile ad hoc networks. *Journal of Communications and Networks*, 2015, vol. 17, no. 1, pp. 75–83. DOI: 10.1109/JCN.2015.000012
Available at: http://ieeexplore.ieee.org/document/7059537

[4] Wang Q., Zhu J. Optimal information security investment analyses with the consideration of the benefits of investment and using evolutionary game theory. *2016 2nd Int. Conf. on Information Management* (ICIM), 2016, pp. 105–109. DOI: 10.1109/INFOMAN.2016.7477542
Available at: http://ieeexplore.ieee.org/document/7477542

[5] Gupta A., Langbort C., Başar T. Dynamic games with asymmetric information and resource constrained players with applications to security of cyberphysical systems. *IEEE Transactions on Control of Network Systems*, 2017, vol. 4, no. 1, pp. 71–81. DOI: 10.1109/TCNS.2016.2584183
Available at: http://ieeexplore.ieee.org/document/7498672

[6] Schöttle P., Böhme R. Game theory and adaptive steganography. *IEEE Transactions on Information Forensics and Security*, 2016, vol. 11, no. 4, pp. 760–773. DOI: 10.1109/TIFS.2015.2509941
Available at: http://ieeexplore.ieee.org/document/7360156

[7] Lei C., Ma D., Zhang H. Optimal strategy selection for moving target defense based on Markov game. *IEEE Access*, 2017, vol. 5, pp. 156–169. DOI: 10.1109/ACCESS.2016.2633983
Available at: http://ieeexplore.ieee.org/document/7805250

[8] Xiao L., Chen T., Han G., Zhuang W., Sun L. Channel-based authentication game in MIMO systems. *2016 IEEE Global Communications Conf. (GLOBECOM)*, 2016, pp. 1–6.
DOI: 10.1109/GLOCOM.2016.7841657 Available at: http://ieeexplore.ieee.org/document/7841657

[9] Chessa M., Grossklags J., Loiseau P. A game-theoretic study on non-monetary incentives in data analytics projects with privacy implications. *2015 IEEE 28th Computer Security Foundations Symposium*, 2015, pp. 90–104. DOI: 10.1109/CSF.2015.14
Available at: http://ieeexplore.ieee.org/document/7243727

[10] Shah S.V., Chaitanya A.K., Sharma V. Resource allocation in fading multiple access wiretap channel via game theoretic learning. *2016 Information Theory and Applications Workshop (ITA)*, 2016, pp. 1–7. DOI: 10.1109/ITA.2016.7888137
Available at: http://ieeexplore.ieee.org/document/7888137

[11] Li L., Shamma J. Efficient computation of discounted asymmetric information zero-sum stochastic games. *54th IEEE Conf. on Decision and Control (CDC)*, 2015, pp. 4531–4536. DOI: 10.1109/CDC.2015.7402927 Available at: http://ieeexplore.ieee.org/document/7402927

[12] Bykov A.Yu., Panfilov F.A., Khovrina A.V. The algorithm to select security classes for objects in distributed information systems and place data in the objects through reducing the optimization problem to the theory of games with non-conflicting interests. *Nauka i obrazovanie: nauchnoe izdanie* [Science and Education: Scientific Publication], 2016, no. 1 (in Russ.).
DOI: 10.7463/0116.0830972 Available at: http://technomag.bmstu.ru/doc/830972.html

[13] Bykov A.Yu., Panfilov F.A., Zen'kovich S.A. Model and methods of multi-criteria selection of the security classes for objects in distributed information system and databases placement on objects. *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2016, no. 2 (15), pp. 9–20 (in Russ.).

[14] Klyucharev P.G. FPGA implementation of general cellular automata based cryptographic hash functions: performance and effectiveness. *Nauka i obrazovanie: nauchnoe izdanie* [Science and Education: Scientific Publication], 2014, no. 1 (in Russ.).
DOI: 10.7463/0114.0675812 Available at: http://technomag.bmstu.ru/doc/675812.html

[15] Balk E. A., Klyucharev P.G. Small diameter graph-based investigation of avalanche effect characteristics of generalized cellular automata. *Nauka i obrazovanie: nauchnoe izdanie* [Science and Education: Scientific Publication], 2016, no. 4 (in Russ.).
DOI: 10.7463/0416.0837506 Available at: http://technomag.bmstu.ru/doc/837506.html

[16] Klyucharev P.G. Performance of cellular automata-based stream ciphers in GPU implementation. *Nauka i obrazovanie: nauchnoe izdanie* [Science and Education: Scientific Publication], 2016, no. 6 (in Russ.). DOI: 10.7463/0616.0842091
Available at: http://old.technomag.edu.ru/doc/842091.html

[17] Klyucharev P.G. Methods of designing cryptographic hash-functions based on iteration of the uniform cellular automata. *Voprosy kiberbezopasnosti* [Cybersecurity issues], 2017, no. 1 (19), pp. 45–50 (in Russ.).

[18] Strekalovskiy A.S., Orlov A.V. Bimatrichnye igry i bilineynoe programmirovanie [Bimatrix games and bilinear programming]. Moscow, Fizmatlit Publ., 2007. 224 p.

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).

Krygin I.A. — post-graduate student, Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Mullin A.R. — Master's Degree 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., Krygin I.A., Mullin A.R. Scheduling Algorithms of the Protection System between Assets of a Mobile Device on the Basis of Zero-Sum Game and Equal Security Principle. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr*. [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2018, no. 2, pp. 48–68 (in Russ.).
DOI: 10.18698/0236-3933-2018-2-48-68