Наука и Образование
МГТУ им. Н.Э. Баумана
Сетевое научное издание
ISSN 1994-0408

Наука и Образование. МГТУ им. Н.Э. Баумана.
Электрон. журн. 2016. № 01. С. 90–107.

DOI: **10.7463/0116.0830972**

Представлена в редакцию: 30.12.2015
Исправлена: 14.01.2016

© МГТУ им. Н.Э. Баумана

УДК 004.056+519.834

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

Быков А. Ю.[1,*], Панфилов Ф. А.[1], Ховрина А. В.[1]

*abykov@bmstu.ru

[1]МГТУ им. Н.Э. Баумана, Москва, Россия

В статье рассмотрена постановка задачи назначения классов защищенностей для объектов распределенной информационной системы и распределения баз данных по объектам. Задача сформулирована как задача билинейного булевого программирования. Для снижения размерности задачи предложено задачу интерпретировать как задачу двух игроков с непротивоположными интересами. Предложен алгоритм поиска положения равновесия по Нэшу, доказана сходимость представленного алгоритма. Представлены результаты решения задачи и тестирования алгоритмов с точки зрения временной сложности при использовании двух подходов к решению задачи: подхода, основанного на решении одной задачи булева программирования большой размерности, и подхода, основанного на сведении задачи к игре с непротивоположными интересами, при этом для поиска состояния равновесия по Нэшу на каждом шаге алгоритма решается задача булевого программирования меньшей размерности.

Ключевые слова: информационная безопасность, распределенная информационная система, дискретное программирование, игра с непротивоположными интересами, положение равновесия по Нэшу

Введение

При проектировании распределенных информационных систем (РИС), в том числе, основанных на «облачных» технологиях, возникает задача определения классов защищенности для объектов РИС и распределения баз данных (БД) по этим объектам с целью повышения защищенности хранимых данных. Рассмотрим оптимизационную математическую постановку подобной задачи и возможную интерпретацию этой задачи как игры с непротивоположными интересами [1].

Такие направления в исследовании операций как теория игр и теория оптимизации, включая оптимизацию по нескольким показателям качества, достаточно сильно связаны друг с другом, используются в различных областях, в том числе, в задачах, связанных с защитой информации. Рассмотрим некоторые примеры.

В [2] проводится оценка состояния дел в современных коммерческих мобильных программных продуктах защиты от вредоносных программ для операционной системы (ОС) Android. Проводится сравнение программных продуктов по различным показателям, в частности, способность выявлять известный вредоносный код после его модификации различными методами. Строится таблица значений этих показателей для различных средств защиты от вредоносных программ.

В [3] разработан полиномиальный алгоритм для назначения идентификаторов узлам сети для анонимного обмена данными между любыми двумя абонентами сети, т.е. закрытого для других узлов сети, для этого используется ряд Штурма.

В [4] рассматривается подход к проектированию корпоративных сетей. Рассматривается проблемы размещения виртуальных локальных сетей (VLAN) и обеспечения достижимости узлов сети. Задачи проектирования сформулированы в виде задач дискретного (булевого) программирования. Рассмотрены эвристические алгоритмы с полиномиальной трудоемкостью для размещения различных элементов сети с целью обеспечения достижимости узлов, алгоритмы ориентированы на специфику задачи. Алгоритмы верифицированы на крупномасштабной сети кампуса с сотнями маршрутизаторов и сетей VLAN.

В [5] рассматривается алгоритм размещения специальных устройств в узлах сети – карт ускорения протокола Secure Socket Layer (SSL) (SSL acceleration cards). SSL-протокол используется в сети Интернет для обеспечения требуемого уровня конфиденциальности. Алгоритм минимизирует совокупную стоимость размещения карт ускорения, при этом в ограничениях учитывается производительность, которая определяется задержками при передаче данных и решении распределенных прикладных задач. Таким образом, рассматриваются различные компромиссы цены и качества. Алгоритм выполняет совместную оптимизацию вычислительных и коммуникационных ресурсов, хотя обычно эти задачи решаются отдельно, алгоритм комбинаторный и учитывает специфику задачи.

В [6] рассматриваются проблемы обеспечения безопасности в мобильных одноранговых сетях MANET (Mobile Ad hoc Network – беспроводные децентрализованные самоорганизующиеся сети, состоящие из мобильных устройств). В статье совместно рассматриваются вопросы аутентификации и управления топологией. Обычно вопросы аутентификации и управления топологией изучаются отдельно, но данные вопросы тесно связаны в сети MANET. Алгоритмы аутентификации и управления топологией оказывают существенное воздействие на пропускную способность сети. Анализируются зависимости пропускной способности от алгоритма аутентификации, который используется на верхних уровнях стека протокола и алгоритма физического уровня, связанного с условиями канала передачи данных. Для решения задачи используются алгоритмы дискрет-

ной стохастической оптимизации с целью повышения пропускной способности сети. Исследуются скорости сходимости предложенных алгоритмов.

В [7] представлен метод обнаружения вредоносных программ, основанный на признаках их проявления, метод назвали «растущий виноград». При этом используются методы кластеризации и методы распознавания (обнаружения). Методы кластеризации группируют объекты, например, процессы и файлы, в кластеры (классы). Механизм распознавания распознает кластер как вредоносный, если поведение кластера соответствует некоторым предопределенным шаблонам, сформированным на основе многократного предыдущего опыта. Предложенный подход не требует больших вычислительных ресурсов, так как используются информационные потоки уровня ОС вместо потоков данных, как в традиционных антивирусах, которые обычно требуют больших вычислительных ресурсов. Также для повышения быстродействия и уменьшения требуемой памяти предложен новый методы организации шаблона поведения и хранения базы данных шаблонов. При этом проводится компромиссная оптимизация двух показателей: точности обнаружения и производительность, предложен комбинаторный алгоритм оптимизации.

Некоторый обзор зарубежных работ по вопросам применения моделей теории игр в задачах защиты информации представлен в [8, 9].

В [10] рассматривается связи биматричных игр с задачами билинейного программирования, в частности, поиск ситуации равновесия по Нэшу в биматричной игре сводится к решению задачи билинейного программирования. В [11] рассматриваются задачи равновесного программирования и связи задач равновесного программирования с антагонистическими играми и выпуклым программированием, а также связь равновесного программирования с некооперативными играми n игроков и поиском состояния равновесия по Нэшу.

1. Постановка задачи

Рассмотрим следующую содержательную постановку задачи. В РИС существует множество объектов территориально распределенной информационной системы, объектами могут быть отдельные сервера, центры обработки данных, внутри объекта может быть своя локальная сеть, также могут быть использованы различные облачные технологи. В этой системе могут храниться конфиденциальные данные различной степени конфиденциальности. Для обеспечения необходимого уровня защищенности данных на объектах могут применяться различные технологии и средства защиты. Для хранения определенных типов данных могут предъявляться некоторые требования, это могут быть требования ФСТЭК [12], требования к хранению персональных данных и др. Таким образом, для хранения некоторых типов данных объект РИС должен удовлетворять требованиям заданного класса защищенности (в терминологии ФСТЭК). Обеспечение требований классов защищенности требует применения определенных технологий или средств защиты, т.е. требует материальных затрат. Множество классов защищенности задано. Необходимо решить одновременно две задачи: определить для каждого объекта РИС класс за-

щищенности, требованиям которого должен удовлетворять объект РИС; распределить данные (БД) по объектам РИС. При решении этой задачи будем стараться повысить уровень защищенности данных при ограничениях на стоимость реализации требований классов защищенностей. Рассмотрим возможную математическую постановку задачи.

Исходные данные

Введем в рассмотрение следующие базисные множества:

- $S = \{S_i, i \in M\}$ – множество объектов РИС (серверов, центров обработки данных и т.п.), на которых могут храниться БД; $M = \{1, 2, \dots, m\}$ – множество индексов объектов РИС.
- $D = \{D_j, j \in N\}$ – множество БД (массивов данных), которые должны храниться в РИС; $N = \{1, 2, \dots, n\}$ – множество индексов БД.
- $K = \{K_k, k \in L\}$ – множество классов защищенностей, требованиям которых должны удовлетворять объекты РИС; $L = \{1, 2, \dots, l\}$ – множество индексов классов защищенностей.

Элементы множеств и отношения между ними характеризуются следующими параметрами:

- $c_k, \forall k \in L$ – стоимость создания объекта, удовлетворяющего требованиям k-го класса защищенности, при этом, чем более жесткие требования защищенности определены в классе, тем выше стоимость объекта.
- $z_k \in [0, 1], \forall k \in L$ – коэффициент защищенности, отражающий уровень защиты класса защищенности, определяется экспертами.
- $f_j \in [0, 1], \forall j \in N$ – коэффициент, отражающий важность j-й БД с точки зрения необходимости обеспечения защиты этих данных, определяется экспертами или владельцем данных.
- $v_j, \forall j \in N$ – верхняя оценка объема j-й БД.
- $V_i, \forall i \in M$ – суммарный объем баз данных, который экономически целесообразно хранить на i-м объекте.

Показатель качества

Для формализации задачи введены два вида булевых переменных. Первая группа булевых переменных: переменная $x_{ik}, i \in M, k \in L,$ принимает значение, равное 1, если i-й объект удовлетворяет требованиям k-го класса защищенности, и равное 0 – в противном случае. Обозначим через $\vec{X} = \|x_{11}, \dots, x_{1l}, x_{21}, \dots, x_{2l}, \dots, x_{m1}, \dots, x_{ml}\|^T$ вектор булевых переменных. Вторая группа булевых переменных: переменная $y_{ij}, i \in M, j \in N,$ принимает значение, равное 1, если j-я БД, хранится на i-м объекте, и равное 0 – в противном случае. Обозначим через $\vec{Y} = \|y_{11}, \dots, y_{1n}, y_{21}, \dots, y_{2n}, \dots, y_{m1}, \dots, y_{mn}\|^T$ вектор булевых переменных.

Тогда общий нормированный показатель защищенности данных имеет вид:

$$F(\vec{X},\vec{Y}) = \frac{\sum_{i \in M}\sum_{j \in N}\sum_{k \in L} f_j z_k x_{ik} y_{ij}}{\sum_{j \in N} f_j}. \quad (1)$$

Значение показателя может принадлежать интервалу [0, 1] (максимальное значение показателя не может превышать максимальный коэффициент защищенности для классов защищенностей), в знаменателе дроби представлено суммарное значение важностей БД, если бы они хранились на объектах с максимальной защищенностью (коэффициент защищенности равен 1). Значение показателя необходимо максимизировать.

Ограничения

На значения компонент вектора $\vec{X}$ наложены ограничения:

$$\sum_{k \in L} x_{ik} = 1, \forall\, i \in M, \quad (2)$$

выражающее условие того, что i-й объект обязательно удовлетворяет требованиям одного класса защищенности.

Ограничение на стоимость защиты объектов РИС:

$$\sum_{i \in M}\sum_{k \in L} c_k x_{ik} \le C^{(max)}, \quad (3)$$

где $C^{(max)}$ - максимальная стоимость, которую можно потратить на реализацию требований классов защищенностей на объектах РИС.

На значения компонент вектора $\vec{Y}$ наложены ограничения:

$$\sum_{i \in M} y_{ij} = 1, \forall\, j \in N, \quad (4)$$

выражающее условие того, что j-я БД должна обязательно храниться на объектах РИС в одном экземпляре.

Замечание. В ограничении (4) вместо знака равенства может присутствовать знак «≥», т.е. j-я БД должна обязательно храниться на объектах РИС, как минимум, в одном экземпляре, что повышает доступность и другие характеристики данных с точки зрения их безопасности, но усложняет процесс администрирования, поэтому на данном этапе это обстоятельство учитывать не будем.

Ограничения на объем данных, который экономически целесообразно хранить на i-м объекте:

$$\sum_{j \in N} v_j y_{ij} \le V_i, \forall\, i \in M. \quad (5)$$

Поставленная задача выбора классов защищенностей для объектов РИС и распределения БД между объектами является задачей булева программирования с показателем качества (1) и ограничениями (2)-(5). Задача, как правило, является большой размерности (в зависимости от размерности исходных данных), точные алгоритмы с полиномиальной трудоемкостью в общем случае для таких задач не найдены. Также задача является задачей билинейного программирования, алгоритмы решения подобных задач в случае, когда множество решений непрерывно, а функции выпуклые рассмотрены в [10], но эти алгоритмы здесь неприменимы, так как задача является задачей дискретного программирования.

2. Алгоритм решения задачи

Данную задачу можно решать напрямую с помощью любого метода дискретной оптимизации, который может быть применен для случая, когда целевая функция является билинейной. Но можно применить другой подход к решению задачи, будем интерпретировать задачу как задачу 2-х игроков с непротивоположными интересами [1]: один игрок отвечает за выбор вектора $\vec{X}$, а второй за выбор вектора $\vec{Y}$. Связь задач билинейного программирования и биматричных игр для непрерывного случая рассмотрена в [10]. При таком игровом подходе к поставленной задаче, чаще всего, ищут решение, которое удовлетворяет критерию равновесия по Нэшу [1, 10].

Если обозначить Δ_X – множество допустимых векторов $\vec{X}$, т.е. векторов, удовлетворяющих ограничениям (2), (3), а Δ_Y – множество допустимых векторов $\vec{Y}$, т.е. векторов, удовлетворяющих ограничениям (4), (5), то решением, которое удовлетворяет критерию равновесия Нэша, является пара векторов $\langle\vec{X}^*,\vec{Y}^*\rangle$, $\vec{X}^* \in \Delta_X$, $\vec{Y}^* \in \Delta_Y$, таких, что выполняются условия (в случае максимизации показателя качества):

$$F(\vec{X}^*,\vec{Y}^*) \geq F(\vec{X}^*,\vec{Y}), \forall \vec{Y} \in \Delta_Y;$$

$$F(\vec{X}^*,\vec{Y}^*) \geq F(\vec{X},\vec{Y}^*), \forall \vec{X} \in \Delta_X.$$

Для нахождения решения удовлетворяющего критерию равновесия по Нэшу рассмотрим следующий алгоритм. Похожий алгоритм применялся [10] для поиска локального оптимума в задаче билинейного программирования для непрерывного случая.

Шаг 0. Положим i=0, $\vec{X}_i = \vec{X}_0$, где $\vec{X}_0 \in \Delta_X$ – некоторый начальный допустимый вектор $\vec{X}$, удовлетворяющий ограничениям (2) и (3). Для нахождения $\vec{X}_0$ будем полагать, что все объекты удовлетворяют требованиям самого низшего класса защищенности (стоимость реализации требований этого класса самая низкая), если это решение по ограничению (3) недопустимо, значит, допустимого решения не существует, работа алгоритма прекращается.

Шаг 1. При заданном векторе $\vec{X}_i$ находим вектор $\vec{Y}_{i+1}$, решая задачу булевого программирования некоторым методом дискретного программирования с показателем качества (1) и ограничениями (4) и (5). Проверяем критерий остановки, если он выполняется, то завершение работы алгоритма, вектора $\vec{X}_i$, и $\vec{Y}_i$ (вектор $\vec{Y}$, полученный ранее) являются решением задачи.

Шаг 2. При заданном векторе $\vec{Y}_{i+1}$ находим вектор $\vec{X}_{i+1}$, решая задачу булевого программирования некоторым методом дискретного программирования с показателем качества (1) и ограничениями (2) и (3). Проверяем критерий остановки, если он выполняется, то завершение работы алгоритма, вектора $\vec{X}_i$ (вектор $\vec{X}$, полученный ранее), и $\vec{Y}_{i+1}$ являются решением задачи.

Шаг 3. Положим i= i+1 и переходим к шагу 1.

Критерием остановки является условие того, что значения показателя (1), полученное на шагах 1 или 2, равно значению показателя, полученному на предшествующем шаге при решении задачи оптимизации (т.е. показатель не улучшился).

Достоинство такого подхода по сравнению с подходом, основанном на решении одной задачи дискретного программирования, заключается в том, на каждом шаге приходится решать задачу дискретной оптимизации, размерность которой меньше, чем исходная задача. Учитывая то, что в общем случае точные алгоритмы дискретной оптимизации имеют экспоненциальную трудоемкость, снижение размерности задачи может дать существенный выигрыш.

Справедлива следующая теорема о сходимости предложенного варианта алгоритма и о том, что полученное решение удовлетворяет критерию Нэша.

Теорема. Предложенный алгоритм имеет конечное число шагов, при этом если на некотором шаге алгоритма 1 или 2 при решении задачи оптимизации получено решение со значением показателя качества, таким же, как на предшествующем шаге, на котором решалась задача оптимизации (для шага 2, предшествующим является шаг 1, а для шага 1 – шаг 2), то решение, полученное на предшествующем шаге, является положением равновесия по Нэшу.

Доказательство. Конечность алгоритма следует из того, что множество допустимых решений является конечным, на каждом шаге, получаемое решение будет не хуже, чем было на предыдущем шаге, следовательно, наступит момент, когда получаемые значения показателя перестанут улучшаться. Докажем, что решение полученное на предшествующем шаге удовлетворяет критерию Нэша. Пусть на шаге 1 при заданном векторе $\vec{X}_i$ (i>0) найден вектор $\vec{Y}_{i+1} = \mathrm{argmax}_{\vec{Y} \in \Delta_Y} F(\vec{X}_i, \vec{Y})$ (решение, полученное на предшествующем шаге $\langle \vec{X}_i, \vec{Y}_i \rangle$), при этом значение показателя не улучшилось, т.е. $F(\vec{X}_i, \vec{Y}_{i+1}) = F(\vec{X}_i, \vec{Y}_i)$, очевидно, что $F(\vec{X}_i, \vec{Y}_i) = F(\vec{X}_i, \vec{Y}_{i+1}) \geq F(\vec{X}_i, \vec{Y}), \forall \vec{Y} \in \Delta_Y$. Решение $\vec{X}_i$ было найдено на предшествующем шаге 2 (на этом шаге значение i было на 1 меньше) как решение задачи $\vec{X}_i = \mathrm{argmax}_{\vec{X} \in \Delta_X} F(\vec{X}, \vec{Y}_i)$, тогда $F(\vec{X}_i, \vec{Y}_i) \geq F(\vec{X}, \vec{Y}_i), \forall \vec{X} \in \Delta_X$. Таким образом, решение $\langle \vec{X}_i, \vec{Y}_i \rangle$ является точкой равновесия по Нэшу.

Аналогично, если на шаге 2 при заданном векторе $\vec{Y}_{i+1}$ (i>0) найден вектор $\vec{X}_{i+1} = \mathrm{argmax}_{\vec{X} \in \Delta_X} F(\vec{X}, \vec{Y}_{i+1})$ (решение, полученное на предшествующем шаге $\langle \vec{X}_i, \vec{Y}_{i+1} \rangle$), при этом значение показателя не улучшилось, т.е. $F(\vec{X}_{i+1}, \vec{Y}_{i+1}) = F(\vec{X}_i, \vec{Y}_{i+1})$, очевидно, что $F(\vec{X}_{i+1}, \vec{Y}_{i+1}) = F(\vec{X}_i, \vec{Y}_{i+1}) \geq F(\vec{X}, \vec{Y}_{i+1}), \forall \vec{X} \in \Delta_X$. Решение $\vec{Y}_{i+1}$ было найдено на предшествующем шаге 1 как решение задачи $\vec{Y}_{i+1} = \mathrm{argmax}_{\vec{Y} \in \Delta_Y} F(\vec{X}_i, \vec{Y})$, тогда $F(\vec{X}_i, \vec{Y}_{i+1}) \geq F(\vec{X}_i, \vec{Y}), \forall \vec{Y} \in \Delta_Y$. Таким образом, решение $\langle \vec{X}_i, \vec{Y}_{i+1} \rangle$ является точкой равновесия по Нэшу.

3. Эксперименты

Рассмотрим пример решения задачи с заданными исходными данными, а также эксперименты, связанные с исследованиями временной сложности алгоритмов.

3.1. Пример решения задачи

Рассмотрим практический пример решения задачи для информационной системы со следующими исходными данными: число объектов – 6, число классов защищенностей – 3, число распределяемых БД – 12. Параметры классов защищенностей и максимальная стоимость для реализации требований классов защищенностей представлены в табл. 1, параметры объектов представлены в табл. 2, параметры баз данных представлены в табл. 3.

Таблица 1. Параметры классов защищенностей и максимальная стоимость для реализации требований классов

Номер класса	Стоимость создания объекта	Коэффициент защищенности класса
1	1 000 000	0,99
2	800 000	0,90
3	500 000	0,60
Максимальная стоимость:	5 000 000	

Таблица 2. Параметры объектов

Номер объекта	Экономически целесообразный объем БД для хранения на объекте
1	25
2	25
3	30
4	50
5	50
6	50

Таблица 3. Параметры баз данных

Номер БД	Коэффициент важность БД	Оценка верхнего объема БД
1	1,0	10
2	1,0	10
3	1,0	15
4	1,0	15
5	0,9	20
6	0,9	20
7	0,8	20
8	0,7	20
9	0,7	25
10	0,6	25
11	0,5	25
12	0,7	25

Для решения задачи дискретного программирования на каждом шаге алгоритма поиска равновесия по Нэшу был использован алгоритм метода полного перебора решений среди решений, допустимых по ограничениям (2) и (4). Можно использовать и другие методы дискретной оптимизации [13-22]. В результате работы алгоритма решение с повторяющимся значением показателя качества было получено на четвертом шаге (было решено 4 задачи дискретной оптимизации). В табл. 4 представлены выбранные классы защищенностей для объектов и размещенные на них БД.

Таблица 4. Выбранные классы защищенностей для объектов и номера БД, размещенных на объектах

Номер объекта	Номер класса для объекта	Номера БД, размещенные на объекте
1	3	11
2	3	10
3	1	2, 8
4	1	9, 12
5	1	3, 4, 7
6	1	1, 5, 6

Полученное значение показателя качества: 0,946

Для решения этого примера был также использован подход, основанный на решении одной задачи дискретной оптимизации (был использован метод полного перебора среди решений допустимых по ограничениям (2) и (4)), при этом было получено совпадающее решение, но время решения представленного примера на три порядка превышало время решения при использовании подхода, основанного на сведении задачи к игре.

3.2. Эксперименты, связанные с исследованиями временной сложности алгоритмов

Эксперименты выполнялись на ноутбуке с процессором Intel ® Core ™ i5-2410, тактовая частота 2,3 ГГц, для разработки использовался язык Си++, средство разработки Microsoft Visual Studio 2013. При этом сравнивались два подхода: подход, основанный на решении одной задачи дискретной оптимизации (ДО), и подход, основанный на сведении задачи к игре. Исходные данные для решаемого примера была получены с помощью генераторов псевдослучайных чисел. В табл. 5 представлены результаты экспериментов: полученные значения показателей качества и времена решения задач в зависимости от их размерности. Размерность задач определялась тремя параметрами: n – числом БД, m – числом объектов, l – числом классов защищенностей. В табл. 5 выделены красным цветом случаи, когда значения показателей не совпали при использовании разных подходов к решению задачи.

Таблица 5. Времена решения задач в зависимости от размерности и полученные значения показателя качества при использовании разных подходов

№ п/п	Исходные данные, определяющие размерность задачи (n, m, l)	Прямое решение задачи методом полного перебора		Сведение задачи к игре двух игроков, на каждом шаге алгоритма задача дискретного программирования решается методом полного перебора		
		Время решения, с.	Значение показателя	Время решения, с.	Значение показателя	Число решенные задач ДО
Изменяется число БД (*n*)						
1.	8, 4, 3	0,356	0,901	0,010	0,895	3
2.	9, 4, 3	1,622	0,479	0,047	0,479	2
3.	10, 4, 3	3,583	0,687	0,105	0,687	4
4.	11, 4, 3	12,299	0,622	0,322	0,622	4
5.	12, 4, 3	51,132	0,654	1,582	0,565	4
6.	13, 4, 3	323,298	0,637	8,299	0,637	4
7.	14, 4, 3	1104,624	0,574	27,159	0,574	4
Изменяется число объектов (*m*)						
8.	10, 3, 3	0,218	0,669	0,016	0,669	2
9.	10, 4, 3	3,583	0,687	0,105	0,687	4
10.	10, 5, 3	140,581	0,761	1,350	0,761	4
11.	10, 6, 3	2882,713	0,732	11,729	0,677	4
Изменяется число классов защищенностей (*l*)						
12.	10, 4, 3	3,583	0,687	0,105	0,687	4
13.	10, 4, 4	11,152	0,876	0,132	0,876	4
14.	10, 4, 5	25,758	0,797	0,125	0,770	4
15.	10, 4, 6	47,409	0,559	0,125	0,559	5

Графики зависимости времен решения задач в зависимости от параметров размерности задачи n, m или l представлены на рис 1, 2 и 3, соответственно.

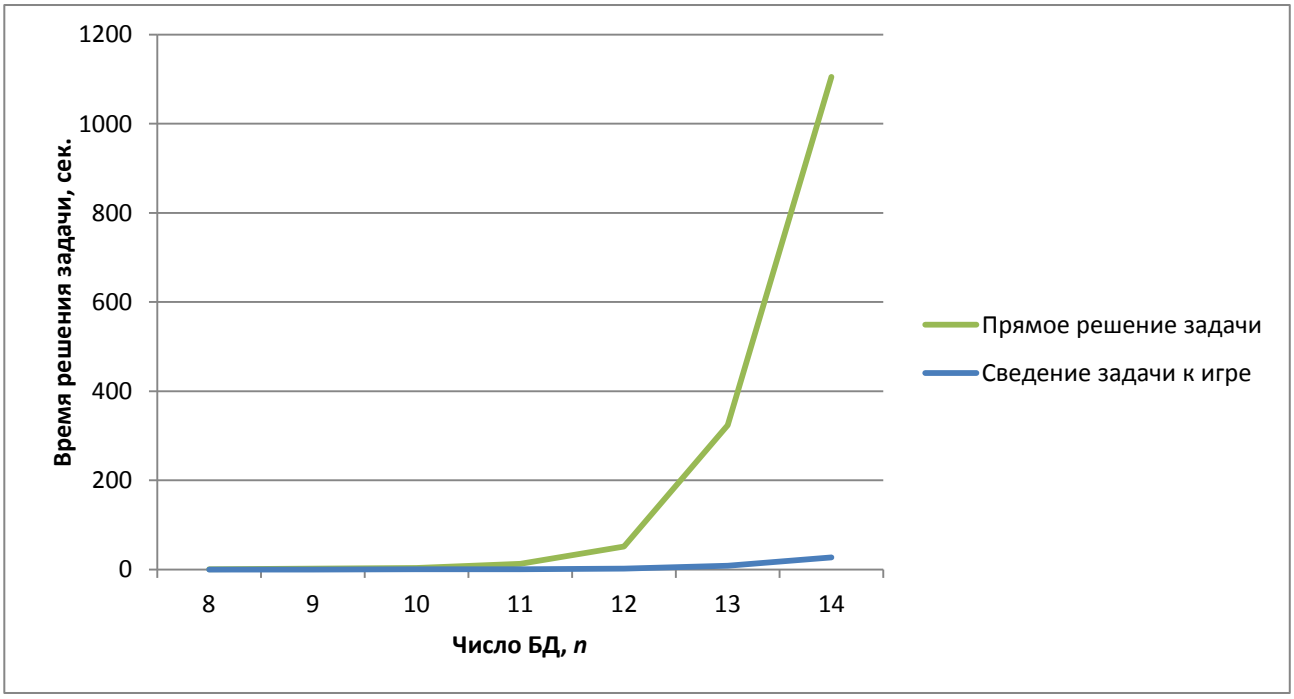

Рис. 1. График зависимости времени решения задач различными алгоритмами в зависимости от числа БД – n (m=4, l=3)

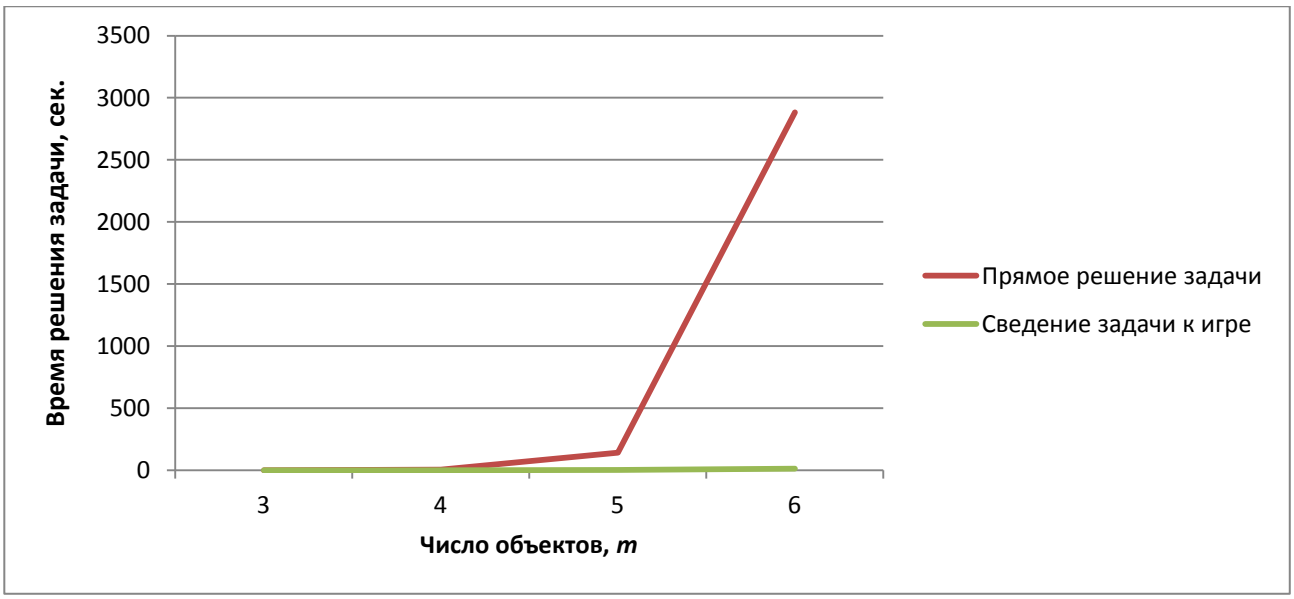

Рис. 2. График зависимости времени решения задач различными алгоритмами в зависимости от числа объектов – m (n=10, l=3)

Рис. 3. График зависимости времени решения задач различными алгоритмами в зависимости от числа классов защищенностей – l (n=10, m=4)

Заключение

В статье рассмотрена постановка задачи выбора классов защищенностей для объектов РИС и распределения БД по объектам РИС в виде задачи булевого билинейного программирования. Предложена интерпретация этой задачи в виде задачи двух игроков с непротивоположными интересами. Предложен алгоритм поиска равновесной ситуации по Нэшу в задаче игры двух игроков с непротивоположными интересами. Подобное представление задачи позволяет на каждом шаге алгоритма решать задачу дискретной оптимизации меньшей размерности, чем в случае решения одной задачи булевого билинейного

программирования. Практическое тестирование алгоритмов на исходных данных, полученных с помощью генераторов псевдослучайных чисел, показало следующее:

- в 73 % случаях решение, полученное при использовании подхода, основанного на сведении задачи к игре двух игроков с непротивоположными интересами, имело такое же значение показателя качества, как при решении одной общей задачи булевого программирования;
- при использовании подхода, основанного на сведении задачи к игре двух игроков с непротивоположными интересами, приходилось решать до 4-х задач дискретной оптимизации для проверенных исходных данных;
- эксперименты с исследованием временной сложности алгоритмов показали, что время решения задачи при использовании подхода, основанного на сведении задачи к игре двух игроков с непротивоположными интересами, существенно (на 2-3 порядка) меньше, чем время решения при использовании подхода, основанного на решении одной задачи булевого программирования;
- эксперименты с исследованием временной сложности алгоритмов показали, что зависимости времени решения задачи от числа объектов и числа баз данных, имеют экспоненциальный характер, а зависимость времени решения от числа классов защищенностей имеют форму графика, близкую к линейной.

Список литературы

1. Гермейер Ю.Б. Игры с непротивоположными интересами. М.: Наука, 1976. 327 с.
2. Rastogi V., Yan Chen, Xuxian Jiang. Catch Me If You Can: Evaluating Android Anti-Malware Against Transformation Attacks // IEEE Transactions on Information Forensics and Security. 2014. Vol. 9, iss. 1. P. 99-108. DOI: 10.1109/TIFS.2013.2290431
3. Dunning L.A., Kresman R. Privacy Preserving Data Sharing With Anonymous ID Assignment // IEEE Transactions on Information Forensics and Security. 2013. Vol. 8, iss. 2. P. 402-413. DOI: 10.1109/TIFS.2012.2235831
4. Sung, Y.E., Xin Sun, Rao S.G., Xie G.G., Maltz D.A. Towards Systematic Design of Enterprise Networks // IEEE/ACM Transactions on Networking. 2011. Vol. 19, iss. 3. P. 695-708. DOI: 10.1109/TNET.2010.2089640
5. Bregni S., Giacomazzi P., Poli A. Cost-Performance Optimization of SSL-Based Secure Distributed Infrastructures // IEEE Latin America Transactions. 2011. Vol. 9, iss. 4. P. 550-556. DOI: 10.1109/TLA.2011.5993742
6. Quansheng Guan, Yu F.R., Shengming Jiang, Leung V.C.M. Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications // IEEE Transactions on Vehicular Technology. 2012. Vol. 61, iss. 6. P. 2674-2685. DOI: 10.1109/TVT.2012.2196061

7. Zhiyong Shan, Xin Wang. Growing Grapes in Your Computer to Defend Against Malware // IEEE Transactions on Information Forensics and Security. 2014. Vol. 9, iss. 2. P. 196-207. DOI: 10.1109/TIFS.2013.2291066
8. Быков А.Ю., Алтухов Н.О., Сосенко А.С. Задача выбора средств защиты информации в автоматизированных системах на основе модели антагонистической игры // Инженерный вестник МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 4. С. 525-542. Режим доступа: http://engbul.bmstu.ru/doc/708106.html (дата обращения 12.01.2016).
9. 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. МГТУ им. Н.Э. Баумана. Электрон. журн. 2015. № 9. С. 160-187. DOI: 10.7463/0915.0812283
10. Стрекаловский А.С., Орлов А.В. Биматричные игры и билинейное программирование. М.: Физматлит, 2007. 224 с.
11. Алеева С.Р., Якубович Е.О. Равновесное программирование и его применение для нахождения равновесия по Нэшу // Вестник Челябинского государственного университета. 2013. № 28 (319). С. 6-20.
12. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации // Сборник руководящих документов по защите информации от НСД. М.: Гостехкомиссия России, 1998. С. 23-52.
13. Овчинников А.И., Журавлев А.М., Медведев Н.В., Быков А.Ю. Математическая модель оптимального выбора средств защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2007. № 3. С. 115-121.
14. Овчинников А.И., Медведев Н.В., Быков А.Ю. Применение метода вектора спада для решения задачи поиска вариантов защиты от угроз безопасности вычислительной сети предприятия // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2008. № 2. С. 73-82.
15. Быков А.Ю., Панфилов Ф.А., Шмырев Д.В. Задача выбора средств защиты в автоматизированных системах с учетом классов защищенности от несанкционированного доступа к информации // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 1. DOI: 10.18698/2308-6033-2012-1-85
16. Быков А.Ю., Гуров А.В. Задача выбора средств защиты информации от атак в автоматизированных системах при нечетких параметрах функции цели // Инженерный журнал: наука и инновации. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 1. DOI: 10.18698/2308-6033-2012-1-86
17. Ключарев П.Г. О вычислительной сложности некоторых задач на обобщенных клеточных автоматах // Безопасность информационных технологий. 2012. № 1. С. 30-32.

18. Ключарев П.Г. NP-трудность задачи о восстановлении предыдущего состояния обобщенного клеточного автомата // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 1. Режим доступа: http://technomag.bmstu.ru/doc/312834.html (дата обращения 12.01.2016).
19. Ключарев П.Г. О периоде обобщенных клеточных автоматов // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2012. № 2. Режим доступа: http://technomag.bmstu.ru/doc/340943.html (дата обращения 12.01.2016).
20. Ключарёв П.Г. Производительность и эффективность аппаратной реализации поточных шифров, основанных на обобщенных клеточных автоматах // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2013. № 10. С. 299-314. DOI: 1013.0624722
21. Ключарёв П.Г. Реализация криптографических хэш-функций, основанных на обобщенных клеточных автоматах, на базе ПЛИС: производительность и эффективность // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 1. С. 214-223. DOI: 10.7463/0114.0675812
22. Ключарёв П.Г. Об устойчивости обобщенных клеточных автоматов к некоторым типам коллизий // Наука и образование. МГТУ им. Н.Э. Баумана. Электрон. журн. 2014. № 9. С. 2314-223. DOI: 10.7463/0914.0727086

Science & Education of the Bauman MSTU
Electronic journal
ISSN 1994-0408

Science and Education of the Bauman MSTU, 2016, no. 01, pp. 90–107.

DOI: **10.7463/0116.0830972**

Received: 30.12.2015
Revised: 14.01.2016

© Bauman Moscow State Technical Unversity

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

A.Yu. Bykov[1,*], F.A. Panfilov[1], A.V. Hovrina[1]

[*]abykov@bmstu.ru

[1]Bauman Moscow State Technical University, Moscow, Russia

Keywords: information security, distributed information system, discrete optimization, game with nonconflicting interests, Nash equilibrium

Modern methods to solve the practical problems related to the information security system design in multipurpose distributed systems often use optimization models. The paper formulates a problem statement of bilinear Boolean programming with the quality score that determines the level of the system security to select classes of protected objects in distributed systems and allocate databases in these objects. Restrictions specify the maximum cost of protection and the recommended amount of data stored in the object. To solve this problem, using the algorithms of discrete programming is possible, but the accurate algorithms, generally, are exponentially time-consuming.

To find a solution the paper proposes to interpret this problem as a problem of two players with non-conflicting interests. The first player is responsible for the assignment of security classes for the system objects, and the second player is responsible for the distribution of databases between the objects. To find solutions the use of a Nash equilibrium criterion is offered. To find the equilibrium solution is developed an algorithm and are proved its convergence, and the fact that it really allows us to obtain the Nash equilibrium position. Using the problem-solving approach related to reducing the original optimization problem to a two-player game with non-conflicting interests allowed a decreasing dimension of the original problem, because at each step of the algorithm is solved the problem of discrete optimization of a smaller dimension than the original problem of Boolean programming.

The paper presents results of solving the problem, as well as research results on the time complexity of represented algorithms. It conducts a comparative analysis of the two approaches: an approach based on solving a discrete optimization problem and an approach based on reducing the problem to a two-player game with non-conflicting interests. An approach based on reducing the initial problem to a game, allowed us to decrease solution time significantly, by 2-3

orders, while, in general, the reached value was the same as in the original problem of Boolean programming.

References

1. Germeier Yu.B. *Igry s neprotivopolozhnymi interesami* [Games with nonconflicting interests]. Moscow, Nauka Publ., 1976. 327 p. (in Russian).
2. Rastogi V., Yan Chen, Xuxian Jiang. Catch Me If You Can: Evaluating Android Anti-Malware Against Transformation Attacks. *IEEE Transactions on Information Forensics and Security*, 2014, vol. 9, iss. 1, pp. 99-108. DOI: 10.1109/TIFS.2013.2290431
3. Dunning L.A., Kresman R. Privacy Preserving Data Sharing With Anonymous ID Assignment. *IEEE Transactions on Information Forensics and Security*, 2013, vol. 8, iss. 2, pp. 402-413. DOI: 10.1109/TIFS.2012.2235831
4. Sung, Y.E., Xin Sun, Rao S.G., Xie G.G., Maltz D.A. Towards Systematic Design of Enterprise Networks. *IEEE/ACM Transactions on Networking*, 2011, vol. 19, iss. 3, pp. 695-708. DOI: 10.1109/TNET.2010.2089640
5. Bregni S., Giacomazzi P., Poli A. Cost-Performance Optimization of SSL-Based Secure Distributed Infrastructures. *IEEE Latin America Transactions*, 2011, vol. 9, iss. 4, pp. 550-556. DOI: 10.1109/TLA.2011.5993742
6. Quansheng Guan, Yu F.R., Shengming Jiang, Leung V.C.M. Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications. *IEEE Transactions on Vehicular Technology*, 2012, vol. 61, iss. 6, pp. 2674-2685. DOI: 10.1109/TVT.2012.2196061
7. Zhiyong Shan, Xin Wang. Growing Grapes in Your Computer to Defend Against Malware. *IEEE Transactions on Information Forensics and Security*, 2014, vol. 9, iss. 2, pp. 196-207. DOI: 10.1109/TIFS.2013.2291066
8. Bykov A.Yu., Altukhov N.O., Sosenko A.S. The problem of choosing software / hardware means in automated information systems based on the model of an antagonistic game. *Inzhenernyi vestnik MGTU im. N.E. Baumana = Engineering Herald of the Bauman MSTU,* 2014, no. 4, pp. 525-542. Available at: http://engbul.bmstu.ru/doc/708106.html , accessed 12.01.2016. (in Russian).
9. 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 MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2015, no. 9, pp. 160-187. DOI: 10.7463/0915.0812283 (in Russian).
10. Strekalovskii A.S., Orlov A.V. *Bimatrichnye igry i bilineinoe programmirovanie* [Bimatrix games and bilinear programming]. Moscow, Fizmatlit Publ., 2007. 224 p. (in Russian).

11. Aleeva S.R., Yakubovich Y.O. Equilibrium programming and its application for a search of Nash equilibrium. *Vestnik Chelyabinskogo gosudarstvennogo universiteta = Herald of Chelyabinsk State University*, 2013, no. 28 (319), pp. 6-20. (in Russian).
12. Guidance document. The automated control system. Protection against unauthorized access to information. Automated systems classification and requirements for protection of information. *Sbornik rukovodyashchikh dokumentov po zashchite informatsii ot NSD* [Collection of guidelines to protect information from unauthorized access]. Moscow, Publ. of FSTEC of Russia, 1998, pp. 23-52. (in Russian).
13. Ovchinnikov A.I., Zhuravlev A.M., Medvedev N.V., Bykov A.Yu. Mathematical Model of Optimal Selection of Aids of Protection Against Threats for Safety of Enterprise Computer Network. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie = Herald of the Bauman Moscow State Technical University. Ser. Instrument Engineering*, 2007, no. 3, pp. 115-121. (in Russian).
14. Ovchinnikov A.I., Medvedev N.V., Bykov A.Yu. Application of Recession Vector Method to Solving Problem on Search of Variants of Protection against Security Threats of Enterprise Computer Network. *Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie = Herald of the Bauman Moscow State Technical University. Ser. Instrument Engineering*, 2008, no. 2, pp. 73-82. (in Russian).
15. Bykov A.Yu., Panfilov F.A., Shmyrev D.V. A Problem on Choosing Protection in Automated Systems Taking into Account the Classes of Immunity against Unauthorized Data Access. *Inzhenernyy zhurnal: nauka i innovatsii = Engineering Journal: Science and Innovation*, 2012, no. 1. DOI: 10.18698/2308-6033-2012-1-85 (in Russian).
16. Bykov A.Yu., Gurov A.V. A Problem on Choosing Protection against Attacks in Automated Systems with Fuzzy Parameters of Goal Function. *Inzhenernyy zhurnal: nauka i innovatsii = Engineering Journal: Science and Innovation*, 2012, no. 1. DOI: 10.18698/2308-6033-2012-1-86 (in Russian).
17. Klyucharev P.G. Computational Complexity of Some Problems on Generalized Cellular Automations. *Bezopasnost Informatsionnykh Tekhnology*, 2012, no. 1, pp. 30-32. (in Russian).
18. Klyucharev P.G. NP-hard of step backward problem in generalized cellular automaton. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 1. Available at: http://technomag.bmstu.ru/doc/312834.html , accessed 12.01.2016. (in Russian).
19. Klyucharev P.G. On period of generalized cellular automation. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2012, no. 2. Available at: http://technomag.bmstu.ru/doc/340943.html , accessed 12.01.2016. (in Russian).
20. Klyucharev P.G. Performance and effectiveness of hardware realization of stream ciphers based on generalized cellular automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2013, no. 10, pp. 299-314. DOI: 1013.0624722 (in Russian).

21. Klyucharev P.G. The FPGA realization of the general cellular automata based cryptographic hash functions: Performance and effectiveness. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2014, no. 1, pp. 214-223. DOI: 10.7463/0114.0675812 (in Russian).
22. Klyucharev P.G. On Collision Resistance of Generalized Cellular Automata. *Nauka i obrazovanie MGTU im. N.E. Baumana = Science and Education of the Bauman MSTU*, 2014, no. 9, pp. 2314-223. DOI: 10.7463/0914.0727086 (in Russian).