УДК 004.056.53 DOI 10.18522/2311-3103-2025-4-80-91

А.С. Жук

ПРИМЕНЕНИЕ РЮКЗАЧНЫХ АЛГОРИТМОВ ДЛЯ ПРЕДОТВРАЩЕНИЯ НЕСАНКЦИОНИРОВАННОГО ОБМЕНА ИНФОРМАЦИЕЙ МЕЖДУ ПОЛЬЗОВАТЕЛЯМИ РАЗЛИЧНОГО УРОВНЯ ИЕРАРХИЧЕСКОЙ СИСТЕМЫ ЗАЩИТЫ ОТ НСД

Рассматривается задача проектирования безопасной системы защиты от НСД. В частности анализируются иерархические системы защиты данных с криптографическим распределением ключей, а именно задача организации доступа к файловым хранилищам. Несмотря на то, что криптографическое распределение ключей позволяет обеспечить безопасность информации от пользователей, не имеющих к ней доступ, иерархическая система управления доступом изначально не предназначена для решения задачи защиты информации от недобросовестных действий самого пользователя. Таким образом целью исследования является совершенствование иерархической системы защиты от НСД с криптографическим распределением ключей сверху-вниз для предотвращения несанкционированного обмена информацией между пользователями различного уровня доступа. Для достижения поставленной цели автором ранее было предложено использовать задачи Диофантового анализа, в частности задачи о рюкзаке. На основании требований, предъявляемых к иерархическим системам с криптографическим распределением ключей в своих работах автор сформулировал требования к рюкзачному вектору для возможности его применения, а также сформулировал и доказал условия, при которых эти требования будут выполнятся, в частности, условия инъективности мультипликативного рюкзачного вектора и условия сохранения сложности задачи о мультипликативном рюкзаке. В данной статье разработан рекурсивный алгоритм построения рюкзачного вектора, удовлетворяющего этим условиям. Показано, что мультипликативные рюкзачные векторы, удовлетворяющие общеизвестным достаточным критериям инъективности являются частным случаем рюкзачного вектора, построенного с помощью разработанного алгоритма. Проведен анализ известных алгоритмов построения инъективных рюкзачных векторов как для мультипликативного, так и для аддитивного случая, и показано, что существующие алгоритмы построения рюкзачных векторов можно применять, как составные части разработанного алгоритма. Далее автор показывает применение разработанного алгоритма для совершенствования иерархической системы защиты от НСД с криптографическим распределением ключей сверху-вниз.

Модель защиты от несанкционированного доступа; иерархическая система защиты; криптографическое распределение ключей; задача о рюкзаке; мультипликативный рюкзачный вектор; инъективность рюкзачного вектора.

A.S. Zhuck

APPLICATION OF BACKPACK ALGORITHMS TO PREVENT UNAUTHORIZED EXCHANGE OF INFORMATION BETWEEN DIFFERENT LEVELS USERS IN THE HIERARCHICAL SYSTEM OF PROTECTION AGAINST UNAUTHORIZED ACCESS

The problem of designing a secure system of protection against unauthorized access is considered. In particular, this article considers hierarchical data protection systems with cryptographic key distribution, namely, the problem of organizing access to file storages is considered. Although cryptographic key distribution can ensure the security of information from users who do not have access to it, the hierarchical access control system was not originally designed to solve the problem of protecting information from the dishonest actions of the user himself. Thus, the overall objective of the study is to prevent unauthorized exchange of information between users of different levels of a hierarchical system of protection against unauthorized access with cryptographic key distribution. To achieve the stated goal, the authors previously proposed to use the problems of Diophantine analysis, in particular the knapsack problem. Previously, the authors formulated the properties of the knapsack vector, applicable for improving the hierarchical system of protection against unauthorized access. In this article, the authors present the conditions for the injectivity of knapsack vectors. A comparative analysis of these conditions with the already established injectivity conditions is carried out. The analysis shows the need to formulate such conditions and the applicability of knapsack vectors that satisfy them for improving the hierarchical model of protection against unauthorized access. Based on the specified conditions, this article develops a recursive algo-

rithm for constructing an injective multiplicative knapsack vector. The authors then analyze the possibility of its application for modeling a hierarchical mandatory model of information protection from unauthorized access. The analysis shows how already known algorithms for constructing knapsack vectors can be used as part of the developed algorithm. The authors also show where exactly in the developed system it is necessary to apply this algorithm to implement the properties required for hierarchical systems of protection against unauthorized access.

Access control problem; hierarchical security system; cryptographic key distribution; knapsack problem; multiplicative knapsack vector; multiplicative knapsack injectivity.

Введение. В распределенных информационных системах с выделенным файловым хранилищем основной проблемой информационной безопасности является реализация защиты данных от несанкционированного доступа. В рамках решения этой проблемы рассматриваются модели защиты от несанкционированного доступа (НСД) к иерархическим данным с криптографическим распределением ключей. Примерами основных алгоритмов распределения ключей, применяемыми в данных системах, являются, например, алгоритм J.Yeh, алгоритм хэш-функций, Hwang алгоритм [1–3].

Основной подход для построения таких систем строится на том утверждении, что пользователь с более высоким уровнем иерархии имеет доступ к информации своих потомков [1], в то время как доступ в обратном направлении не возможен. Безопасность подобных систем строится на безопасности применяемых криптоалгоритмов. Но при этом такой подход абсолютно не предусматривает защиту от нерегламентированных действий самих пользователей с высоким уровнем полномочий. В частности, в системах с криптографическим распределением ключей технически возможен несанкционированный информационный поток от родителя к потомку [2, 4]. В [5] приведена модель такого информационного потока и формализована математическая постановка задачи совершенствования данной системы в целях предотвращения несанкционированного обмена информацией между пользователями различного уровня иерархии. Отметим, что подобная задача решена в большинстве современных мандатных моделей контроля доступа [6–8]. Тем не менее, в иерархических системах с криптографическим распределением ключей данная проблема остается актуальной.

Так как рассматриваемые модели предполагают использование числовых идентификаторов всех предков данного субъекта доступа для определения возможности доступа субъекта к объекту, автор предположил, что подобную схему возможно моделировать с использованием задачи о рюкзаке [9]. На основании требований к системам защиты от НСД с криптографическим распределением ключей в [9] сформулированы требования, которым должен удовлетворять рюкзачный вектор. Далее в [10] требования модифицированы следующим образом:

- рюкзачный вектор должен быть инъективным;
- задача о рюкзаке должна предполагать нахождение решение алгоритмом с вычислительной сложностью, не менее экспоненциальной;
- алгоритм построения инъективного рюкзака должен обладать вычислительной сложностью не более полиномиальной.

В [10] проведен анализ рюкзачных векторов на инъективность и получены результаты, позволяющие утверждать, что известные подходы не позволяют построить инъективный аддитивный рюкзак заданной сложности. Дальнейшее же исследование строится автором на предположении о возможности нахождения мультипликативных рюкзаков, удовлетворяющих введенным выше условиям.

Представление задачи об обобщенном мультипликативном рюкзаке. Рассмотрим обобщенный мультипликативный рюкзачный вектор $A_{MP} = (a_1, a_2, a_3, ..., a_n)$ с заданным пороговым значением p и множество целых значений степеней компонент рюкзака $Z_p = \{0,1,..., p-1\}$. Для заданного натурального числа V требуется установить, существует ли вектор $w = (\alpha_1, \alpha_2, ..., \alpha_n)$, $\alpha_1, \alpha_2, ..., \alpha_n \in Z_p$, такой, что $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot ... \cdot a_n^{\alpha_n} = V$, и найти его, если он существует. Таким образом формулируется задача о рюкзаке с входом (A_{MP}, V).

В классических зарубежных [11–13] и отечественных [14, 15] научных работах приведен способ представления мультипликативных рюкзачных векторов, используемый для исследования их свойств. Применим это способ для исследования обобщенных мультипликативных рюкзаков на инъективность и формирования алгоритма построения рюкзачных векторов.

Рассчитаем значение $V' = a_1 \cdot a_2 \cdot ... \cdot a_n$. Построим вектор $P = (p_1, p_2, ..., p_m)$, составленный из всех простых делителей числа V'. Далее каждый из компонент заданного рюкзачного вектора $A_{MP} = (a_1, a_2, a_3, ..., a_n)$ представим как произведение степеней компонент вектора *P*:

$$\begin{aligned} a_1 &= p_1^{\alpha_{11}} \cdot p_2^{\alpha_{12}} \cdot ... \cdot p_m^{\alpha_{1m}} \\ a_2 &= p_1^{\alpha_{21}} \cdot p_2^{\alpha_{22}} \cdot ... \cdot p_m^{\alpha_{2m}} \\ &... \\ a_n &= p_1^{\alpha_{n1}} \cdot p_2^{\alpha_{n2}} \cdot ... \cdot p_m^{\alpha_{nm}} \end{aligned};$$

где $\alpha_{ij} \in \{0\} \cup N$ – степень простого числа p_j в разложении компоненты a_i.

Построим систему *m* аддитивных рюкзачных векторов

$$\begin{aligned} P_\alpha^{\,1} &= (\alpha_{11}, \alpha_{21}, ..., \alpha_{n1}) \\ P_\alpha^{\,2} &= (\alpha_{12}, \alpha_{22}, ..., \alpha_{n2}) \\ &... \\ P_\alpha^{\,i} &= (\alpha_{1i}, \alpha_{2i}, ..., \alpha_{ni}) \\ &... \\ P_\alpha^{\,m} &= (\alpha_{1m}, \alpha_{2m}, ..., \alpha_{nm}) \end{aligned}. \quad (1)$$

Теперь рассмотрим число V, которое можно представить следующим образом $V = p_1^{v_1} \cdot p_2^{v_2} \cdot ... \cdot p_m^{v_m} \cdot v$, $(v, p_1^{v_1} \cdot p_2^{v_2} \cdot ... \cdot p_m^{v_m}) = 1$, где v может быть равным 1. Для применения задачи о рюкзаке в моделировании иерархической системы защиты интерес представляет случай, когда значение $v = 1$.

Рассмотрим векторы (1). Каждому из заданных векторов поставим в соответствие задачу о аддитивном рюкзаке с входом $(P_\alpha^{\,i}, v_i), i = \overline{1..n}$ для вектора $(v_1, v_2, v_3, ..., v_n)$. Существует вектор $w = (\alpha_1, \alpha_2, ..., \alpha_n)$, $\alpha_1, \alpha_2, ..., \alpha_n \in Z_p$, являющейся решением каждой из задач об аддитивном рюкзаке с входом $(P_\alpha^{\,i}, v_i), i = \overline{1..n}$, то будем говорить, что этот вектор является решением системы задач об аддитивном рюкзаке.

Справедливо следующее утверждение.

Утверждение 1. Решение задачи об обобщенном мультипликативном векторе с входом (A_{MP}, V) эквивалентно решению системы задач об обобщенных инъективных векторах с входом $(P_\alpha^{\,i}, v_i), i = \overline{1..n}$, где $P_\alpha^{\,i} = (\alpha_{1i}, \alpha_{2i}, ..., \alpha_{ni})$, $V = p_1^{v_1} \cdot p_2^{v_2} \cdot ... \cdot p_m^{v_m} \cdot v$.

Подобный способ представления задачи о мультипликативном рюкзаке в виде системы задач об инъективном, в целом, логичен и интуитивно понятен, тем не менее в современных исследованиях о возможности применения мультипликативных рюкзаков в криптографии не использовался для исследования свойств мультипликативного вектора. Например, в [16, 17] приведены уже известные условия инъективности мультипликативных рюкзаков, которые, как получено авторами [10], не позволяют находить алгоритмов

решения задачи или построения вектора требуемой сложности. В [18], например, не исследуется инъективность рюкзачных векторов, в [19] приведен частный случай диагонального супервозрастания для двоичного вектора решения, но не произведено полное исследование рюкзачного вектора на инъективность. В [9] авторами произведены попытки сформулировать гипотезы для условия инъективности обобщенного мультипликативного рюкзака, но доказательная база не приведена. На основании указанных результатов в следующим пункте обобщим условия инъективности мультипликативного рюкзака.

Условие инъективности мультипликативного рюкзака. Рассмотрим обобщенный мультипликативный рюкзачный вектор $A_{MP} = (a_1, a_2, a_3, ..., a_n)$ с заданным пороговым значением p и множество $Z_p = \{0,1,..., p-1\}$. Далее для вывода условий инъективности модифицируем векторы $P_\alpha^{\,i} = (\alpha_{1i}, \alpha_{2i}, ..., \alpha_{ni})$, $i = \overline{1..n}$.

Важно, что некоторые из компонент данных векторов в общем случае равны 0. Преобразуем данную систему, убрав нулевые значения компонент и упорядочив их по возрастанию. Получим систему рюкзачных векторов

$$\begin{aligned} Q_\chi^{\,1} &= (\chi_{11}, \chi_{21}, ..., \chi_{k_1 1}) \\ Q_\chi^{\,2} &= (\chi_{12}, \chi_{22}, ..., \chi_{k_2 2}) \\ &... \\ Q_\chi^{\,i} &= (\chi_{1i}, \chi_{2i}, ..., \chi_{k_i i}) \\ &... \\ Q_\chi^{\,m} &= (\chi_{1m}, \chi_{2m}, ..., \chi_{k_m m}) \end{aligned} \quad . \qquad (2)$$

Утверждение 2. Для того, чтобы мультипликативный рюкзачный вектор $A_{MP} = (a_1, a_2, a_3, ..., a_n)$ был инъективен достаточно, чтобы аддитивные ранцы (2) были инъективны.

Доказательство этого утверждения было разработано автором в [20]

Отметим важность данного утверждения, оно формирует достаточное условие инъективности, но не необходимое, тем не менее, оно охватывает гораздо большее множество векторов, чем все рассмотренные ранее условия, так, достаточные условия инъективности из работ [16–19, 21] являются частными случаями условия из утверждения 2, что легко показать.

Кроме того, подобное условие позволяет представить задачу построения мультипликативного вектора как совокупность задач построения аддитивных векторов, что является, по сути, уже достаточно исследованной задачей и позволит осуществить поиск алгоритма построения такого вектора, который будет удовлетворять условиям, сформулированным в [10].

Таким образом, приведено авторское достаточное условие инъективности мультипликативного обобщенного вектора, являющееся обобщением существующих достаточных условий инъективности.

Алгоритм построения инъективного рюкзака. Теперь разработаем алгоритм построения инъективного мультипликативного обобщенного рюкзачного вектора (МОРВ). Отметим, что в процессе построения должен использоваться любой известный алгоритм получения инъективного аддитивного обобщенного рюкзачного вектора (АОРВ). Отметим изначально, что сложность такого алгоритма в среднем будет $T_{IA}(n) = O(n)$.

Для построения искомого МОРВ можно воспользоваться любым достаточным условием его инъективности. Выбор условия зависит от необходимой в рамках исследования сложности решения задачи о рюкзаке с входом (A_{MP}, V). Отметим, что для алгоритма будет использовано представление задачи об мультипликативном обобщенном рюкзаке в форме системы задач об аддитивных ранцах (1) и (2).

При этом, в общем случае, при использовании данного алгоритма решение получившейся задачи может иметь произвольную вычислительную сложность. В дальнейшем предполагается формализовать данный алгоритм так, что по заданному значению некоторых параметров можно получать вектор так, что задача с входом $\left(A_{MP}, V\right)$ будет иметь требуемую заранее сложность, как показано в [22].

Будем строить итерационный алгоритм. Такой алгоритм удобно применять, если необходимо иметь возможность динамически увеличивать размер вектора в процессе работы информационной системы, в частности, системы защиты от несанкционированного доступа.

Для разработки применим жадный алгоритм, то есть на каждой итерации разработки будем строить вектор размерности i так, чтобы он был инъективен. Далее предположим, что полученный вектор размерности n так же будет инъективен. Важно, что в рамках исследования рассматривается задача существования и единственности решения для входа $\left(A_{MP}, V\right)$, но не задача оптимизации, в связи с чем примененный метод построения эффективных алгоритмов «жадный алгоритм» позволит получить не приближенное решение с некоторой погрешностью, а точное решение.

Введем некоторые дополнительные понятия. Обозначим через A_{MP}^{i} МОРВ размерности *i.* При построении будем пользоваться таблицей простых чисел, и осуществлять случайный выбор простого числа. В рамках данного исследования качеество случайности значений рассмотрено не будет, хотя представляет интерес для дальнейших исследований.

Построение вектора будем осуществлять итерационно. На шаге i будем строить вектор A_{MP}^{i} так, чтобы он был инъективен, при условии, что вектор A_{MP}^{i-1}, построенный на предыдущем шаге так же инъективен. Для этого будем пользоваться полученным для вектора A_{MP}^{i-1} представлением (1). Каждый аддитивный вектор данного представления размерности *i-1* будем использовать для формирования нового вектора размерности *i*. При этом для формирования инъективного АОРВ используем любой существующий итерационный жадный алгоритм.

Для уменьшения вычислительной сложности разрабатываемого алгоритма и, как следствие, повышения его эффективности воспользуемся вторым утверждением.

С использованием этого условия на каждом шаге алгоритма мы будем добиваться инъективности векторов (2).

Теперь перейдем к построению инъективного МОРВ.

Построим вектор A_{MP}^{1}: вектор размерности 1. Выберем m_1 простых чисел $p_1, p_2, ..., p_{m_1}$, выберем m_1 значений $\alpha_1, \alpha_2, ..., \alpha_{m_1}$. Построим вектор $A_{MP}^{1} = \left(a_1\right) = \left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_{m_1}^{\alpha_{m_1}}\right)$. Для данного вектора построим представления (1), (2).

$$V' = a_1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_{m_1}^{\alpha_{m_1}}.$$

$$P^1 = \left(p_1, p_2, ..., p_{m_1}\right);$$

$$P_\alpha\left(1\right) = \begin{pmatrix} \alpha_{11} \\ \alpha_{12} \\ ... \\ \alpha_{1m_1} \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ ... \\ \alpha_{m_1} \end{pmatrix};$$

$$P_\alpha^{\,1}\left(1\right) = \left(\alpha_{11}\right) = \left(\alpha_1\right);$$

$$P_\alpha^{\,2}\left(1\right) = \left(\alpha_{12}\right) = \left(\alpha_2\right);$$

...

$$P_\alpha^{\,m_1}\left(1\right) = \left(\alpha_{1m_1}\right) = \left(\alpha_{m_1}\right).$$

$$Q_\chi^{\,1}(1)=(\chi_{11})=(\alpha_{11})=(\alpha_1);$$
$$Q_\chi^{\,2}(1)=(\chi_{12})=(\alpha_{12})=(\alpha_2);$$
...
$$Q_\chi^{\,m_1}(1)=(\chi_{1m_1})=(\alpha_{1m_1})=(\alpha_{m_1}).$$

Полученные вектора $Q_\chi^{\,1}(1), Q_\chi^{\,2}(1), Q_\chi^{\,m_1}(1)$ примитивно инъективны, следовательно, по достаточному условию утверждения (2) построенный вектор $A_{MP}^1=(a_1)=\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_{m_1}^{\alpha_{m_1}}\right)$ примитивно инъективен.

Построим вектор A_{MP}^2. Первоначально рассмотрим представления (1) и (2) вектора $A_{MP}^1=(a_1)=\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_{m_1}^{\alpha_{m_1}}\right)$. Далее «отметим» произвольное число векторов из числа $P_\alpha^{\,1}(1), P_\alpha^{\,2}(1),\ldots, P_\alpha^{\,m_1}(1)$. Далее построим вектора

$$P_\alpha^{\,1}(2)=(\alpha_{11},\alpha_{21});$$
$$P_\alpha^{\,2}(2)=(\alpha_{12},\alpha_{22});$$
...
$$P_\alpha^{\,m_1}(2)=\left(\alpha_{1m_1},\alpha_{2m_1}\right)$$

так, чтобы соответствующие вектора $Q_\chi^{\,1}(2), Q_\chi^{\,2}(2), Q_\chi^{\,m_1}(2)$ остались аддитивно инъективными.

Для тех векторов, которые остались «неотмеченными», примем значения $\alpha_{2i}=0$, для остальных векторов необходимо получить значения α_{2j} так, чтобы рассматриваемые вектора остались инъективны. Для получения этих воспользуемся любым из алгоритмов получения инъективных аддитивных обобщенных рюкзачных векторов. В данном алгоритме воспользуемся итерацией, соответствующей получению вектора размерности (2). Отметим, что авторами разработано несколько алгоритмов получения инъективных АОРВ, [23–25]. Возможно воспользоваться любым из данных алгоритмов. Отметим, что разработаны программные реализации всех указанных алгоритмов.

После формирования системы векторов сформируем новые векторы $P_\alpha^{\,k}(2)=(0,\alpha_{2k})$ для новых простых значений p_k.

Для этого выберем случайным образом число $m_2'\in\{0\}\cup N$. После этого выберем m_2' простых чисел, которые не входят в вектор $P^1=\left(p_1,p_2,\ldots,p_{m_1}\right)$. Сформируем таким образом новый вектор P^2 размерности $m_2=m_2'+m_1$ $P^2=\left(p_1,p_2,\ldots,p_{m_2}\right)$. После этого дополним систему векторов следующим образом:

$$P_\alpha^{\,1}(2)=(\alpha_{11},\alpha_{21});$$
$$P_\alpha^{\,2}(2)=(\alpha_{12},\alpha_{22});$$
...
$$P_\alpha^{\,m_1}(2)=\left(\alpha_{1m_1},\alpha_{2m_1}\right);$$
$$P_\alpha^{\,m_1+1}(2)=\left(\alpha_{1(m_1+1)},\alpha_{2(m_1+1)}\right);$$
...
$$P_\alpha^{\,m_2}(2)=\left(\alpha_{1m_2},\alpha_{2m_2}\right).$$

В данной системе

$$\alpha_{1(m_1+1)} = 0, \ldots, \alpha_{1m_2} = 0,$$

а значения

$$\alpha_{2(m_1+1)}, \ldots, \alpha_{2m_2}$$

выбираются произвольным образом.

В результате сформирована система рюкзачных векторов

$$P_\alpha^{\,1}(2) = (\alpha_{11}, \alpha_{21});$$
$$P_\alpha^{\,2}(2) = (\alpha_{12}, \alpha_{22});$$
$$\ldots$$
$$P_\alpha^{\,m_2}(2) = (\alpha_{1m_2}, \alpha_{2m_2}).$$

Среди данных векторов есть векторы, в которых первая компонента нулевая, есть векторы, в которых вторая компонента нулевая, значит соответствующие им векторы из $Q_\chi^{\,1}(2), Q_\chi^{\,2}(2), Q_\chi^{\,m_2}(2)$ инъективны. Те же те из векторов $Q_\chi^{\,1}(2), Q_\chi^{\,2}(2), Q_\chi^{\,m_2}(2)$, которые состоят из двух компонент, остаются инъективны согласно алгоритму их формирования.

Далее из аддитивных рюкзачных векторов

$$P_\alpha^{\,1}(2) = (\alpha_{11}, \alpha_{21});$$
$$P_\alpha^{\,2}(2) = (\alpha_{12}, \alpha_{22});$$
$$\ldots$$
$$P_\alpha^{\,m_2}(2) = (\alpha_{1m_2}, \alpha_{2m_2})$$

и вектора $P^2 = (p_1, p_2, \ldots, p_{m_2})$ формируется мультипликативный обобщенный рюкзачный вектор $A_{MP}^2 = (a_1, a_2)$, где $a_1 = p_1^{\alpha_{11}} \cdot p_2^{\alpha_{12}} \cdot \ldots \cdot p_{m_2}^{\alpha_{1m_2}}, a_2 = p_1^{\alpha_{21}} \cdot p_2^{\alpha_{22}} \cdot \ldots \cdot p_{m_2}^{\alpha_{2m_2}}$.

Таким образом, сформирован алгоритм получения МОРВ $A_{MP}^2 = (a_1, a_2)$, на основании этого алгоритма предположим, что уже сформированы векторы $A_{MP}^2, A_{MP}^3, A_{MP}^4, \ldots, A_{MP}^n$. Требуется разработать алгоритм формирования вектора A_{MP}^{n+1}.

Для вектора $A_{MP}^n = (a_1, \ldots, a_n)$ существует разложение в систему инъективных аддитивных рюкзачных векторов

$$P_\alpha^{\,1} = (\alpha_{11}, \alpha_{21}, \ldots, \alpha_{n1})$$
$$P_\alpha^{\,2} = (\alpha_{12}, \alpha_{22}, \ldots, \alpha_{n2})$$
$$\ldots$$
$$P_\alpha^{\,i} = (\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ni})$$
$$\ldots$$
$$P_\alpha^{\,m} = (\alpha_{1m}, \alpha_{2m}, \ldots, \alpha_{nm})$$

по компонентам вектора $P = (p_1, p_2, \ldots, p_m)$. Необходимо построить инъективный мультипликативный обобщенный рюкзачный вектор размерности $n+1$ $A_{MP}^{n+1} = (a_1, \ldots, a_n, a_{n+1})$.

Для расширения рюкзачного вектора необходимо построить новую компоненту так, чтобы искомый вектор удовлетворял сформулированному ранее достаточному условию инъективности МОРВ (утверждение 2).

Формирование нового элемента будет происходить с помощью двух шагов.

Первый шаг состоит в дополнении вектора простых чисел $P=(p_1, p_2,..., p_m)$. Для этого выберем произвольное число $m_n \in \{0\} \cup N$. Далее выберем случайным образом $m_n \in \{0\} \cup N$ простых чисел, с учетом использования в данной таблице готовой таблицы простых чисел. Важно, что выбранные значения до этого не встречались в векторе $P=(p_1, p_2,..., p_m)$. Алгоритм выбора простых чисел из таблицы будет исследован позднее. Алгоритм проверки выбираемого простого числа на то, использовался ли он ранее будет рассмотрен авторами позже. С учетом модификации вектор $P=(p_1, p_2,..., p_m)$ станет равным $P=(p_1, p_2,..., p_m,..., p_{m'}), m'=m+m_n$.

Тогда изменится разложение МОРВ $A_{MP}^n=(a_1, \dots, a_n)$ на векторы

$$
\begin{aligned}
&P_\alpha{}^1=(\alpha_{11},\alpha_{21},...,\alpha_{n1})\\
&P_\alpha{}^2=(\alpha_{12},\alpha_{22},...,\alpha_{n2})\\
&\quad\dots\\
&P_\alpha{}^m=(\alpha_{1m},\alpha_{2m},...,\alpha_{nm})\\
&P_\alpha{}^{m+1}=(\alpha_{1(m+1)},\alpha_{2(m+1)},...,\alpha_{n(m+1)})\\
&\quad\dots\\
&P_\alpha{}^{m'}=(\alpha_{1m'},\alpha_{2m'},...,\alpha_{nm'})
\end{aligned}
.
$$

При этом важно, что последние m+1 векторы являются нулевыми. Соответственно вектора

$$
\begin{aligned}
&Q_\chi{}^1=(\chi_{11},\chi_{21},...,\chi_{k_1 1})\\
&Q_\chi{}^2=(\chi_{12},\chi_{22},...,\chi_{k_2 2})\\
&\quad\dots\\
&Q_\chi{}^m=(\chi_{1m},\chi_{2m},...,\chi_{k_m m})\\
&\quad\dots\\
&Q_\chi{}^{m'}=(\chi_{1m'},\chi_{2m'},...,\chi_{k_{m'} m'})
\end{aligned}
$$

остаются инъективными, причем выполняются равенства

$$k_{m+1}=0, k_{m+2}=0,..., k_{m'}=0.$$

Далее переходим к выполнению второго шага.

Для каждого из векторов

$$
\begin{aligned}
&P_\alpha{}^1=(\alpha_{11},\alpha_{21},...,\alpha_{n1})\\
&\quad\dots\\
&P_\alpha{}^{m'}=(\alpha_{1m'},\alpha_{2m'},...,\alpha_{nm'})
\end{aligned}
$$

проведем следующие действия.

Рассмотрим вектор $P_{\alpha}^{\ i} = (\alpha_{1i}, \alpha_{2i}, ..., \alpha_{ni})$.

Если $i \le m$, тогда выберем произвольным образом значение $\alpha_{(n+1)i} \in \{0\} \cup N$ так, что если $\alpha_{(n+1)i} > 0$, то соответствующий ему АОРВ $Q_{\chi}^{\ i}(n+1) = (\chi_{1i}, \chi_{2i}, ..., \chi_{(k_i+1)i})$ оставался инъективен. Напомним, что для формирования инъективного АОРВ следует воспользоваться одним из двух известных ранее алгоритмов, при условии, что вектор $Q_{\chi}^{\ i}(n) = (\chi_{1i}, \chi_{2i}, ..., \chi_{k_i i})$ на данной итерации мог удовлетворять любому из условий

$$k_i = 1$$
$$k_i = 2 .$$
$$k_i > 2$$

Об этом важно помнить, потому что алгоритм построения инъективного АОРВ работает по-разному в зависимости от указанных значений.

Если же $i > m$, то выберем произвольное значение $\alpha_{(n+1)i} \in N$. Тогда вновь построенные векторы $Q_{\chi}^{\ m+1}(n+1), Q_{\chi}^{\ m+2}(n+1), Q_{\chi}^{\ m'}(n+1)$ будут иметь размерность 1 и будут тривиально аддитивно инъективны.

В результате сформируем значение $a_{n+1} = p_1^{\alpha_{(n+1)1}} \cdot p_2^{\alpha_{(n+1)2}} \cdot ... \cdot p_{m'}^{\alpha_{(n+1)m'}}$ и инъективный мультипликативный обобщенный рюкзачный вектор размерности $n+1$ $A_{MP}^{n+1} = (a_1, ..., a_n, a_{n+1})$.

Таким образом, в данной статье разработан алгоритм построения инъективного обобщенного мультипликативного рюкзачного вектора. Приведенный алгоритм является рекурсивным алгоритмом, а значит он будет не эффективен с точки зрения используемой оперативной памяти. Это не позволит использовать данный алгоритм для построения мультипликативного рюкзака целиком, но такая особенность алгоритма позволяет в произвольный момент времени для инъективного мультипликативного рюкзака добавлять ещё одну компоненту так, чтобы новый вектор оставался инъективным. Такое свойство позволит обеспечить выполнение одного из основных требований к иерархической системе защиты от НСД, а именно возможность динамического расширения системы [1–4]. Далее этот алгоритм будет использован для добавления объектов и субъектов в иерархическую модель управления доступом и для динамического обновления структуры объектов и субъектов в проектируемой модели.

Заключение. Таким образом, получены следующие результаты:

- приведено доказанное автором ранее достаточное условие инъективности мультипликативного вектора и показано, что данное условие покрывает гораздо большее количество векторов, чем сформулированные на данный момент достаточные условия инъективности;
- на основании данного условия разработан рекурсивный алгоритм построения инъективного МОРВ.

В работе показано, что данный алгоритм имеет перспективы применения для обеспечения возможности динамического расширения иерархической системы защиты информации от НСД с криптографическим распределением ключей. Проанализирована возможность его применения для моделирования иерархической мандатной модели защиты информации от несанкционированного доступа. Анализ показывает, как можно применять уже известные алгоритмы построения рюкзачных векторов, как часть разработанного алгоритма. Итерационный алгоритм далее будет применятся для динамического расширения разрабатываемой системы как в ширину, так и в глубину. Полученные результаты позволят в рамках общей цели исследования разработать искомую модель защиты от НСД.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Лернер В.Д.* Криптографическое распределение ключей для защиты информации в иерархических системах // Информационно-управляющие системы. – 2012. – № 5 (60). – С. 37-43.
2. *Chen M., Mao S., Zhang Y., Leung C.M.* Big data. Related technologies, challenges, and future prospects. – Springer, 2014. – 100 p.
3. *Akl S.G., Taylor P.D.* Cryptographic solution to a problem of access control in hierarchy // ACM Transactions on computer systems. – 1983. – No. 1 (3). – P. 239-248.
4. *Лернер В.Д., Беззатеев С.В.* Основные принципы распределения ключей для доступа к информации в облачных хранилищах данных // Информационная безопасность регионов России (ИБРР-2011): VII Санкт-Петербургская межрегион. конф., Санкт-Петербург, 26-28 октября 2011 г.: Матер. конф. – СПОИСУ. – СПб., 2011. – С. 120.
5. *Жук А.С., Головской В.А.* Синтез иерархической системы защиты информации от несанкционированного доступа на основании модели Белла-ЛаПадулы // Тр. Северо-Кавказского филиала Московского технического университета связи и информатики. Ч. II. – Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2017. – С. 90-97.
6. *Щеглов А.Ю.* Модели, методы и средства контроля доступа к ресурсам вычислительных систем. – СПб.: Университет ИТМО, 2014. – 95 с.
7. *Bell D.E.* Looking Back at the Bell-LaPadula Model // 21st Annual Computer Security Applications Conference. Tucson, Arizona, USA, 2005. – P. 337-351.
8. *Усов С.В.* О связи между объектно-ориентированной дискреционной и субъектно-объектной мандатной моделями безопасности // Математические структуры и моделирование. – 2016. – № 4 (40). – С. 151-163.
9. *Жук А.С., Осипян В.О.* Условия инъективности мультипликативного обобщенного рюкзачного вектора // Специальная связь и безопасность информации (ССБИ-2016): Сб. трудов. Международная НПК. – Краснодар: Краснодарский центр научно-технической информации (ЦНТИ), 2016. – С. 92-97.
10. *Жук А.С., Головской В.А.* Исследование возможности применения обобщенных инъективных рюкзачных векторов для моделирования системы защиты информации от НСД // Тр. Северо-Кавказского филиала Московского технического университета связи и информатики. – 2018. – № 2. – С. 110-115. – EDN WALPYX.
11. *Martello S.T.P.* Knapsack problems: algorithms and computer implementations. – Chichester: JOHN WILEY & SONS, 1990. – P. 137-138.
12. *Shamir A.* A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem // Information Theory, IEEE Transactions. – 1984. – Vol. 30, No. 5. – P. 699-704.
13. *Odlyzhko A.O.* Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme // IEEE Transactions on Information Theory. – Jul 1984. – Vol. IT-30, No. 4. – P. 594-601.
14. *Осипян В.О.* Моделирование систем защиты информации содержащих диофантовы трудности. Разработка методов решений многостепенных систем диофантовых уравнений. Разработка нестандартных рюкзачных криптосистем: монография. – LAP, 2012. – 344 с.
15. *Осипян В.О.* О системе защиты информации на основе проблемы рюкзака // Известия ТПУ. – 2006. – № 2. – URL: https://cyberleninka.ru/article/n/o-sisteme-zaschity-informatsii-na-osnove-problemy-ryukzaka (дата обращения: 28.01.2019).
16. *Осипян В.О., Лейман А.В., Чесебиев А.А., Жук А.С., Арутюнян А.Х., Карпенко Ю.А.* Математическое моделирование нестандартных мультипликативных ранцевых криптосистем // Экологический вестник научных центров Черноморского экономического сотрудничества. – 2017. – № 2. – С. 57-64.
17. *Osipyan V.O.* Buiding of alphabetic data protection cryptosystems on the base of equal power knapsacks with Diophantine problems // ACM. – 2012. – P. 124-129.
18. *Животова А.Е., Зюляркина Н.Д., Костыгина Ю.О.* Модификация криптосистемы с открытым ключом на основе «задачи о рюкзаке // Вестник УрФО. Безопасность в информационной сфере. – 2014. – № 1 (11). – С. 16-20.
19. *Шевляков Т.Н.* Мультипликативная рюкзачная криптосистема // Вестник ОмГУ. – 2011. – № 4. – URL: https://cyberleninka.ru/article/n/multiplikativnaya-ryukzachnaya-kriptosistema (дата обращения: 28.01.2019).
20. *Osipyan V.O., Zhuk A.S., Lukashchik E.P. [et al.].* Multiplicative knapsack injectivity as condition of effective unauthorized access protection // Journal of Physics: Conference Series. – 2021. – Vol. 2131, No. 2. – P. 022084. – DOI: 10.1088/1742-6596/2131/2/022084.
21. *Жук А.С., Головской В.А.* Анализ вычислительной сложности решения задачи о мультипликативном рюкзаке. Т. 78 // Тр. Северо-Кавказского филиала Московского технического университета связи и информатики. Ч. II. – Ростов-на-Дону: ПЦ «Университет» СКФ МТУСИ, 2017. – 441 с. – С. 81-90.

22. *Жук А.С., Кисленко И.А.* Разработка математических моделей условий снижения вычислительной сложности алгоритмов решения задачи об обобщенном мультипликативном рюкзаке // Сб. статей XVIII военно-научной конференции курсантов и операторов научной роты Краснодарского высшего военного училища имени генерала армии С.М. Штеменко. – Краснодар: КВВУ, 2016. – С. 86-96.
23. *Осипян В.О., Жук А.С., Арутюнян А.Х., Карпенко Ю.А.* Построение криптосистем с открытым ключом на основе задач о нестандартном рюкзаке // ММиИТС: Тр. V Всерос. н/п конф.24 июня 2011, КУ МВД России. – С. 12-15.
24. *Подколзин В.В., Осипян В.О.* О свойствах рюкзачных систем защиты информации с открытым ключом в Zp // Вестник СибГУ им. М.Ф. Решетнева. – 2010. – № 3. – С. 51-55.
25. *Осипян В.О., Мирзаян А.В.* Сравнительный анализ криптостойкости классической и обобщенной рюкзачной криптосистем // Математические методы и информационно-технические средства: Тр. Всерос. науч.-практич. конф. Краснодар, 24 июня 2005. – С. 34-36.

REFERENCES

1. *Lerner V.D.* Kriptograficheskoe raspredelenie klyuchey dlya zashchity informatsii v ierarkhicheskikh sistemakh [Cryptographic key distribution for information protection in hierarchical systems], *Informatsionno-upravlyayushchie sistemy* [Information and Control Systems], 2012, No. 5 (60), pp. 37-43.
2. *Chen M., Mao S., Zhang Y., Leung C.M.* Big data. Related technologies, challenges, and future prospects. Springer, 2014, 100 p.
3. *Akl S.G., Taylor P.D.* Cryptographic solution to a problem of access control in hierarchy, *ACM Transactions on computer systems*, 1983, No. 1 (3), pp. 239-248.
4. *Lerner V.D., Bezzateev S.V.* Osnovnye printsipy raspredeleniya klyuchey dlya dostupa k informatsii v oblachnykh khranilishchakh dannykh [Basic principles of key distribution for access to information in cloud data storage], *Informatsionnaya bezopasnost' regionov Rossii (IBRR-2011): VII Sankt-Peterburgskaya mezhregion. konf., Sankt-Peterburg, 26-28 oktyabrya 2011 g.: Mater. konf.* [Information security of Russian regions (ISRR-2011): VII St. Petersburg interregional conference, St. Petersburg, October 26-28, 2011: Conference materials]. SPOISU. Saint Petersburg, 2011, pp. 120.
5. *Zhuk A.S., Golovskoy V.A.* Sintez ierarkhicheskoy sistemy zashchity informatsii ot nesanktsionirovannogo dostupa na osnovanii modeli Bella-LaPaduly [Synthesis of a hierarchical information protection system against unauthorized access based on the Bell-LaPadula model], *Tr. Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki* [Proceedings of the North Caucasus Branch of the Moscow Technical University of Communications and Informatics]. Part II. Rostov-on-Don: PTS «Universitet» SKF MTUSI, 2017, pp. 90-97.
6. *Shcheglov A.Yu.* Modeli, metody i sredstva kontrolya dostupa k resursam vychislitel'nykh system [Models, methods and means of access control to resources of computing systems]. Saint Petersburg: Universitet ITMO, 2014, 95 p.
7. *Bell D.E.* Looking Back at the Bell-LaPadula Model, *21st Annual Computer Security Applications Conference*. *Tucson, Arizona, USA, 2005*, pp. 337-351.
8. *Usov S.V.* O svyazi mezhdu ob"ektno-orientirovannoy diskretsionnoy i sub"ektno-ob"ektnoy mandatnoy modelyami bezopasnosti [On the relationship between object-oriented discretionary and subject-object mandatory security models], *Matematicheskie struktury i modelirovanie* [Mathematical structures and modeling], 2016, No. 4 (40), pp. 151-163.
9. *Zhuk A.S., Osipyan V.O.* Usloviya in"ektivnosti mul'tiplikativnogo obobshchennogo ryukzachnogo vektora [Injectivity conditions of the multiplicative generalized backpack vector], *Spetsial'naya svyaz' i bezopasnost' informatsii (SSBI-2016): Sb. trudov. Mezhdunarodnaya NPK* [Special Communications and Information Security (SSBI-2016): Collection of Works. International Scientific and Practical Conference]. Krasnodar: Krasnodarskiy tsentr nauchno-tekhnicheskoy informatsii (TSNTI), 2016, pp. 92-97.
10. *Zhuk A.C., Golovskoy V.A.* Issledovanie vozmozhnosti primeneniya obobshchennykh in"ektivnykh ryukzachnykh vektorov dlya modelirovaniya sistemy zashchity informatsii ot NSD [Study of the possibility of using generalized injective backpack vectors for modeling an information security system against unauthorized access], *Tr. Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki* [Proceedings of the North Caucasian branch of the Moscow Technical University of Communications and Informatics], 2018, No. 2, pp. 110-115. EDN WALPYX.
11. *Martello S.T.P.* Knapsack problems: algorithms and computer implementations. Chichester: JOHN WILEY & SONS, 1990, pp. 137-138.
12. *Shamir A.* A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem, *Information Theory, IEEE Transactions*, 1984, Vol. 30, No. 5, pp. 699-704.

13. *Odlyzhko A.O.* Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme, *IEEE Transactions on Information Theory*, Jul 1984, Vol. IT-30, No. 4, pp. 594-601.
14. *Osipyan V.O.* Modelirovanie sistem zashchity informatsii soderzhashchikh diofantovy trudnosti. Razrabotka metodov resheniy mnogostepennykh sistem diofantovykh uravneniy. Razrabotka nestandartnykh ryukzachnykh kriptosistem: monografiya. LAP, 2012, 344 p.
15. *Osipyan V.O.* O sisteme zashchity informatsii na osnove problemy ryukzaka [On the information security system based on the backpack problem], *Izvestiya TPU* [Bulletin of the Tomsk Polytechnic University], 2006, No. 2. Available at: https://cyberleninka.ru/article/n/o-sisteme-zaschity-informatsii-na-osnove-problemy-ryukzaka (accessed 28 January 2019).
16. *Osipyan V.O., Leĭman A.V., Chesebiev A.A., Zhuk A.S., Arutyunyan A.Kh., Karpenko Yu.A.* Matematicheskoe modelirovanie nestandartnykh mul'tiplikativnykh rantsevykh kriptosistem [Mathematical modeling of non-standard multiplicative knapsack cryptosystems], *Ekologicheskiy vestnik nauchnykh tsentrov Chernomorskogo ekonomicheskogo sotrudnichestva* [Ecological Bulletin of Scientific Centers of the Black Sea Economic Cooperation], 2017, No. 2, pp. 57-64.
17. *Osipyan V.O.* Buiding of alphabetic data protection cryptosystems on the base of equal power knapsacks with Diophantine problems, *ACM*, 2012, pp. 124-129.
18. *Zhivotova A.E., Zyulyarkina N.D., Kostygina Yu.O.* Modifikatsiya kriptosistemy s otkrytym klyuchom na osnove «zadachi o ryukzake [Modification of a public-key cryptosystem based on the "knapsack problem"], *Vestnik UrFO. Bezopasnost' v informatsionnoy sfere* [Bulletin of the Ural Federal District. Information Security], 2014, No. 1 (11), pp. 16-20.
19. *Shevlyakov T.N.* Mul'tiplikativnaya ryukzachnaya kriptosistema [Multiplicative backpack cryptosystem], *Vestnik OmGU* [Bulletin of Omsk State University], 2011, No. 4. Available at: https://cyberleninka.ru/article/n/multiplikativnaya-ryukzachnaya-kriptosistema (accessed 28 January 2019).
20. *Osipyan V.O., Zhuk A.S., Lukashchik E.P. [et al.].* Multiplicative knapsack injectivity as condition of effective unauthorized access protection, *Journal of Physics: Conference Series*, 2021, Vol. 2131, No. 2, pp. 022084. DOI: 10.1088/1742-6596/2131/2/022084.
21. *Zhuk A.S., Golovskoy V.A.* Analiz vychislitel'noy slozhnosti resheniya zadachi o mul'tiplikativnom ryukzake [Analysis of the computational complexity of solving the multiplicative knapsack problem]. Vol. 78, *Tr. Severo-Kavkazskogo filiala Moskovskogo tekhnicheskogo universiteta svyazi i informatiki* [Proceedings of the North Caucasus Branch of Moscow Technical University of Communications and Informatics]. Part II. Rostov-on-Don: PTS «Universitet» SKF MTUSI, 2017, 441 p., pp. 81-90.
22. Zhuk A.S., Kislenko I.A. Razrabotka matematicheskikh modeley usloviy snizheniya vychislitel'noy slozhnosti algoritmov resheniya zadachi ob obobshchennom mul'tiplikativnom ryukzake [Development of mathematical models of conditions for reducing the computational complexity of algorithms for solving the generalized multiplicative knapsack problem], *Sb. statey XVIII voenno-nauchnoy konferentsii kursantov i operatorov nauchnoy roty Krasnodarskogo vysshego voennogo uchilishcha imeni generala armii S.M. Shtemenko* [Collection of articles of the XVIII military-scientific conference of cadets and operators of the scientific company of the Krasnodar Higher Military School named after General of the Army S.M. Shtemenko]. Krasnodar: KVVU, 2016, pp. 86-96.
23. *Osipyan V.O., Zhuk A.S., Arutyunyan A.Kh., Karpenko Yu.A.* Postroenie kriptosistem s otkrytym klyuchom na osnove zadach o nestandartnom ryukzake [Construction of public-key cryptosystems based on non-standard knapsack problems], *MMiITS: Tr. V Vseros. n/p konf.24 iyunya 2011, KU MVD Rossii* [MMiITS: Proceedings of the V All-Russian scientific conference. June 24, 2011, KU MVD of Russia], pp. 12-15.
24. *Podkolzin V.V., Osipyan V.O.* O svoystvakh ryukzachnykh sistem zashchity informatsii s otkrytym klyuchom v Zp [On the properties of backpack information security systems with an open key in Zp], *Vestnik SibGU im. M.F. Reshetneva* [Bulletin of the Siberian State University named after M.F. Reshetnev], 2010, No. 3, pp. 51-55.
25. *Osipyan V.O., Mirzayan A.V.* Sravnitel'nyy analiz kriptostoykosti klassicheskoy i obobshchennoy ryukzachnoy kriptosistem [Comparative analysis of cryptographic resistance of classical and generalized backpack cryptosystems], *Matematicheskie metody i informatsionno-tekhnicheskie sredstva: Tr. Vseros. nauch.-praktich. konf. Krasnodar, 24 iyunya 2005* [Mathematical methods and information technology tools: Proceedings of the All-Russian scientific and practical conference. Krasnodar, June 24, 2005], pp. 34-36.

Жук Арсений Сергеевич – Кубанский государственный университет; e-mail: arseniyzhuck@mail.ru; г. Краснодар, Россия, тел.: 89384754442; старший преподаватель кафедры вычислительных технологий.

Zhuck Arseniy Sergeevich – Kuban State University; e-mail: arseniyzhuck@mail.ru; Krasnodar, Russia, phone: +79384754442; senior lecturer; the Department of Computer Technologies.