Алгоритм разработки математической модели дисимметричной биграммной криптосистемы, содержащих диофантовы трудности

В.О. Осипян[1], К.И., Литвинов[1], А.С. Жук[1], С.Г. Синица[1], Р. Х. Багдасарян[2]

[1]Кубанский государственный университет, г. Краснодар, Россия
[2]Краснодарский государственный институт культуры, г. Краснодар, Россия

Аннотация: Показана объективная необходимость совершенствования систем защиты информации в условиях развития информационно-телекоммуникационных технологий. В рукописи впервые задействована новая область NP-полных задач из диофантова анализа, а именно - многостепенные системы диофантовых уравнений заданной размерности и степени типа Тарри-Эскотта.
На основании принципиально нового теоретико-числового метода разработана математическая модель алфавитной системы защиты информации, обобщающая принцип построения криптосистем с открытым ключом – так называемую диссимметричную биграммную криптосистему. В ней предлагается прямое и обратное преобразования реализовать по заданному алгоритму на основе двупараметрического решения многостепенной системы диофантовых уравнений.
Разработан формализованный алгоритм для указанной модели дисимметричной биграммной криптосистемы.
Ключевые слова: *NP*-полная задача, симметричная (дисимметричная) криптосистема, генерация ключей, многостепенная система диофантовых уравнений, параметрическое решение, диофантовы трудности.

Введение

В условиях стремительного развития компьютерных, сетевых и телекоммуникационных технологий, включая технологии мобильной связи, роботизированных систем, интернета вещей, цифровой экономики и технологии распределенного реестра (блокчейн), актуальными становятся задачи теории и практики защиты информации на всех уровнях её хранения, обработки и передачи по открытым каналам связи. Для решения этих задач, в силу их специфики и характера, требуются все более совершенные математические модели и методы, так как оппоненты несанкционированного доступа разрабатывают свои, не менее эффективные методы взлома систем, предназначенных для защиты информации. На практике считается, что

разработчики систем защиты информации (СЗИ) будут в выигрыше, если они успеют разработать новую модель СЗИ до взлома их оппонентами старой.

Согласно теоретическим истокам построения математических моделей эффективных систем защиты информации СЗИ (криптосистем), мы исходим из необходимости использования сложных математических NP-полных задач, решение которых потребует от нелегального пользователя больших затрат машинного времени и ресурсов [1–3]. Особое место, следуя К. Шеннону, занимают задачи, содержащие диофантовы трудности [4], применение которых при разработке СЗИ препятствует возможности нелегальному пользователю сократить множество перебираемых ключей (К. Шенноном отмечалось, что наибольшей неопределённостью при подборе ключей, обладают криптосистемы, содержащие диофантовы трудности). Следует отметить также целый ряд современных подходов применения таких задач, рассмотренные в работах авторов [5–6] и обратить внимание также на следующие работы [7–9].

На данном этапе развития теории защиты информации уровень прикладных достижений не соответствует уровню достижений современной науки, недостаточно полно используются современные нейро-сетевые технологии и результаты исследований новых NP-полных задач [10–12]. Характерной особенностью этих работ является разработка новых, наиболее эффективных математических моделей и методов, позволяющих повысить надёжность и стойкость реальных систем связи. Следует отметить также целый ряд новых подходов, включающих методы современной алгебры и геометрии, комбинаторики и теории чисел, предложенных различными авторами для решения вышеперечисленных задач. Центральное место в данной работе занимает диофантовый анализ и теория построения систем параметрических решений многостепенных систем диофантовых уравнений (МСДУ), позволяющих разработать СЗИ на их основе.

Подчеркнём, что в целом детали комбинированного использования теории защиты информации с теорией кодирования ещё недостаточно проработаны, хотя на практике такие модели имеются. Так, например, разработанная Мак-Элисом [13] математическая модель защиты информации имеет сходство с моделями рюкзачного типа, основанными на плотных рюкзаках, в которой используются коды Гоппы, обнаруживающие и исправляющие $t \geq 1$ ошибок.

Как известно, в системах связи проблема защиты информации от канальных ошибок на достаточно высоком уровне решается классическими методами теории помехоустойчивого кодирования [14]. Также известно, что почти во всех теоретических работах прикладного характера исследуются автономные системы кодирования, допускающие обнаружение и исправление заданного числа случайных независимых ошибок, отдельно – системы безопасной передачи информации, обеспечивающие конфиденциальность, целостность и доступность информации. Отметим особо: проблемы передачи и защиты информации данных по дискретным каналам связи с заданными характеристиками являются составляющими одной общей проблемы – надёжной и безопасной передачи информации.

Изучая литературу современных источников нашего направления, мы не обнаружили других работ, кроме авторских разработок [4, 5, 9]. Изучая аналогичные работы зарубежных авторов [15–17], мы пришли к выводу, что у этих авторов нет единого научного подхода. Отдельные работы [18–21] имеют частный характер, а именно, в них рассматриваются диофантовы уравнения и криптосистемы на их основе, используется лишь диофантов язык. Так, например, автор работы [18] строит рюкзачную 0-1-2 криптосистему на основе линейного диофантового уравнения с пороговым значением p, равным трём. Заметим, что аналогичная задача об обобщённом рюкзаке впервые была рассмотрена в исследовании автора [22], в котором

была разработана математическая модель обобщённой рюкзачной криптосистемы для произвольных пороговых значений p.

Наш подход к разработке криптосистем и протоколов, содержащих диофантовы трудности [23–25], существенно отличается от всех других работ. Нами предлагается новая область NP-полных задач из диофантова анализа, а именно - МСДУ типа Тарри – Эскотта (ТЭ) [26–28]. Особенность таких систем диофантовых уравнений заключается в том, что, во-первых, неизвестны общие неперебoрные методы их решения на основе отрицательного решения 10-й проблемы Гильберта [29, 30], а, во-вторых, если для заданной МСДУ существуют параметрические и числовые решения, то эти решения адекватны соответствующим по размеру ранцам [22, 31].

Отметим, что для решения вышеуказанных проблем авторы мирового научного сообщества ограничиваются рассмотрением сравнительно простых математических моделей при различных упрощающих ограничениях из-за трудностей исследования NP-полных задач для более общих случаев, в том числе алгоритмов и методов решений этих задач, зачастую напрямую зависящих от основных размеров задач.

В данной работе предлагается алгоритм разработки математических моделей стойких и эффективных СЗИ, содержащих диофантовы трудности на основе параметрических решений МСДУ типа ТЭ, обобщающий принцип построения криптосистем с открытым ключом. Приводится математическая модель дисимметричной биграммной криптосистемы (ДБК) и алгоритм её реализации на основе результатов, полученных автором [23].

Некоторые факты и определения из диофантова анализа

Основные утверждения, факты и понятия, используемые при построении математической модели ДБК на основе параметрического решения МСДУ, содержащие диофантовы трудности, можно найти в работах

автора [23, 24]. Тем не менее для удобства приведём некоторые обозначения и определения, которые можно найти также в следующих работах [22, 25].

Как известно [32], под алгебраическим диофантовым уравнением понимают полиномиальное уравнение:

$$f(x_1, x_2, \ldots, x_n) = 0, \qquad (1)$$

коэффициенты которого суть целые числа, и решения требуется найти тоже в целых или целых неотрицательных числах. Задача решения диофантова уравнения (1) или систем таких уравнений, как правило, заключается в поиске целочисленных решений или доказательства того, что таких решений нет [32, 27].

В работе рассматривается МСДУ типа ТЭ размерности m порядка (или степени) n вида [27]:

$$X_1^k + X_2^k + \cdots + X_m^k = Y_1^k + Y_2^k + \cdots Y_m^k, \qquad k = 1..n$$

или в компактной записи:

$$X_1, X_2, \ldots, X_m \overset{n}{=} Y_1, Y_2, \ldots, Y_m. \qquad (2)$$

Для краткости эту запись мы представим ещё в виде:

$$X \overset{n}{=} Y,$$

а её целое параметрическое решение – в виде:

$$A \overset{n}{=} B,$$

где $A = a_1, a_2, \ldots, a_m$, $B = b_1, b_2, \ldots, b_m$, a_i, b_i– целые числовые параметры.

Утверждения относительно параметрических решений МСДУ (2) можно найти в работах [33–35] или в работе авторов [36–38]. Рассмотрим возможность применения МСДУ для математического моделирования алфавитных СЗИ, если установлены условия, при которых МСДУ допускают параметризацию по одному, двум и более параметрам $t_1, t_2, \ldots, t_r$ в виде [23–25]:

$$X_i = X_i\,(t_1, t_2, \ldots, t_r), Y_i = Y_i\,(t_1, t_2, \ldots, t_r),\ i = 1..m,$$

из которых можно получить решения в натуральных или целых числах $a_1, a_2, \ldots, a_m,\ b_1, b_2, \ldots, b_m$ таких, что для всех $n < m$ имеют место числовые тождества [23]: $a_1, a_2, \ldots, a_m \overset{n}{=} b_1, b_2, \ldots, b_m$.

Если $A = a_1, a_2, \ldots, a_m,\ B = b_1, b_2, \ldots, b_m$ – два числовых вектора (рюкзаки или ранцы), или наборы параметров размерности m (функциональные рюкзаки или ранцы) [23, 37, 38], то для заданных целых чисел a, b, c и d определим:

1. $A_k^i = a_k, a_{k+1}, \ldots, a_i,\ k \le i$, в частности, при $k = 1$, считаем, что $A_k^i = A^i$ для $i = 1..m$;
2. $aA = aa_1, aa_2, \ldots, aa_m$;
3. $A \pm B = a_1 \pm b_1, a_2 \pm b_2, \ldots, a_m \pm b_m$;
4. $A \pm a = a_1 \pm a, a_2 \pm a, \ldots, a_m \pm a$;
5. $A^m, B^m = a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_m$;
6. $aA \pm c, bB \pm d = aa_1 \pm c, aa_2 \pm c, \ldots, aa_m \pm c, bb_1 \pm d, bb_2 \pm d, \ldots, bb_m \pm d$.

(3)

Определение. Два упорядоченных набора чисел (числовые рюкзаки) или наборы параметров $A^m = a_1, a_2, \ldots, a_m$ и $B^m = b_1, b_2, \ldots, b_m$ (функциональные рюкзаки) размерности m равносильны со степенью (или порядком) n, что мы запишем, как: $A^m \overset{n}{=} B^m$, если они удовлетворяют МСДУ размерности m степени n:

$$X_1, X_2, \ldots, X_m \overset{n}{=} Y_1, Y_2, \ldots, Y_m,$$

то есть, выполняются следующие равенства для всех значений $1..n$:

$$a_1, a_2, \ldots, a_m \overset{n}{=} b_1, b_2, \ldots, b_m.$$

Другими словами, из равносильности $A^m \overset{n}{=} B^m$ следует, что набор A^m, B^m является корнем уравнения (2) размерности m степени n:

$$X^m \overset{n}{=} Y^m.$$

Рассмотренные в работе [23] теоремы относительно параметрических решений МСДУ устанавливают равносильность числовых наборов или наборов упорядоченных параметров и позволяют разработать эффективные СЗИ на основании следующей теоремы [23].

Теорема. Из равносильности двух целых числовых упорядоченных наборов (или наборов упорядоченных параметров) размерности m степени n:

$$A^m \underset{=}{}^{n} B^m$$

следует равносильность также следующих наборов:

$$A^m, -B^{m-1} \underset{=}{}^{n} b^m \tag{4}$$

или в более общем случае для любого натурального $i = 1..m$:

$$A^m, -B^{i-1} \underset{=}{}^{n} B_i^m, \qquad i \le m. \tag{5}$$

Для разработки СЗИ применяются равносильности (5) следующим образом: по заданному алгоритму (мы рассмотрим ниже) (5) разбивается на две части – одна часть используется при прямом преобразовании открытого текста, а другая часть – при обратном преобразовании закрытого текста с помощью блоков заданной длины, что представляет с собой количество параметров в решении соответствующей МСДУ [39–41].

Алгоритм математического моделирования дисимметричной биграммной криптосистемы

Приведём модели аддитивной ДБК, содержащие диофантовы трудности, которые строятся на основе двупараметрического решения МСДУ, полученных ранее в работах [23, 25, 33].

Пусть исходная МСДУ -й степени (или порядка n) размерности $m, m > n$ имеет вид:

$$X_1, X_2, \ldots, X_m \underset{=}{}^{n} Y_1, Y_2, \ldots, Y_m. \tag{6}$$

Как уже было отмечено [23], особенность таких уравнений заключается в том, что неизвестны общие неперебо́рные методы их решения для любых m и n [29, 30]. В то же время для отдельных значений m и n эти уравнения допускают параметризацию по одному, двум и более параметрам [42, 43], из которых можно получить конкретные решения в целых или натуральных числах $a_1, a_2, \ldots, a_m,\ b_1, b_2, \ldots, b_m$таких, что выполняются равенства:

$$a_1, a_2, \ldots, a_m \overset{n}{=} b_1, b_2, \ldots, b_m. \quad (7)$$

Заметим, что по найденному решению (2) МСДУ восстановить числовые значения её параметров за приемлемое время не представляется возможным. Кроме того, на практике вычисления производятся для достаточно больших натуральных чисел, так что стандартные средства вычислений зачастую неприменимы. Для разработки эффективной СЗИ на основе МСДУ необходимо в зависимости от основных параметров m и n учитывать либо сложность решения системы (1), либо сами решения, либо и то и другое одновременно.

В данном пункте рассмотрим математическую модель системы защиты информации M_D, в основе синтеза которой лежат диофантовы трудности, возникающие при параметрическом решении МСДУ высоких степеней.

Как известно [23], математическую модель произвольной алфавитной криптосистемы можно представить в виде следующего кортежа:

$$\sum_0 = \langle M^*, Q, C^*, E(m), D(c) | V(E(m), D(c)) \rangle, \quad (8)$$

где M^* – множество всех сообщений $m = m_1\, m_2 \ldots m_k$ (открытых текстов) над алфавитом M; Q – множество всех числовых эквивалентов элементарных сообщений m_i (в частности, буквы или конкатенация букв из алфавита M); C^* – множество всех шифртекстов (криптограмм) $c = c_1\, c_2 \ldots c_k$ над алфавитом C; $E(m)$ – алгоритм прямого преобразования открытого текста $m = m_1\, m_2 \ldots m_k$; $D(c)$ – алгоритм обратного

преобразования шифртекста $c = c_1\, c_2 \ldots c_k; V(E(m),\, D(c))$ – связь однозначности между алгоритмами E(m) и D(c).

Проиллюстрируем предложенный автором [23] подход для построения математической модели алфавитной ДБК на основе двупараметрического решения заданной МСДУ. Прежде всего, определяем размерность l и порядок k необходимой МСДУ (1), а затем и её двупараметричское решение:

$$X_i = v_i(a,b) = v_i, \qquad i = 1..l,$$
$$Y_i = v_j(a,b) = v_j,\ j = (l+1)..2l,$$

что можно представить в виде следующего упорядоченного набора длины $2l$:

$$V^{2l} = v_1, v_2, \ldots, v_{2l},$$

для которого выполняются следующие равенства для всех значений отрезка $1..k$:

$$v_1, v_2, \ldots, v_l \overset{k}{=} v_{l+1}, v_{l+2}, \ldots, v_{2l}. \qquad (9)$$

Далее при фиксированной степени $d, 1 \le d \le k$ генерируем функцию прямого преобразования по заданному алгоритму $E(m)$ на основе (5) из пункта 2 (см. Теорему), как:

$$E(m_{2i-1}m_{2i}) = C_L(a,b) = v_1^d + v_2^d + \cdots + v_r^d = c_i, r < 2l$$

считая, что a шифр элементарного сообщения биграммы $m_{2i}m_{2i-1}$, b – закрытый ключ. Соответственно *D(c)* – алгоритм обратного преобразования шифртекста *c* определяем на основе соотношения:

$$C_R(a,b) = v_{r+1}^d + v_{r+2}^d + \cdots + v_{2l}^d = c_i,$$

где $D(c_i)$ – решения уравнения $v_{r+1}^d + v_{r+2}^d + \cdots + v_{2l}^d = c_i$.

Количество слагаемых для функции обратного преобразования $C_R(a,b)$ можно довести до минимума, например, до одного слагаемого, как это представлено в (4) из пункта 2 (см. Теорему).

I. Формализованный алгоритм прямого и обратного преобразований

Определим формализованный алгоритм прямого и обратного преобразования для демонстрации разработанной модели [23]. Также сопроводим его примером, демонстрирующим работу алгоритма на каждом этапе:

а) алгоритм кодирования и декодирования биграмм исходного сообщения.

Прежде всего определим логику кодирования биграмм исходного сообщения в последовательность символов, которая и будет использоваться в процессах прямого и обратного преобразований.

Пусть задано исходное сообщение m над алфавитом M – заглавных букв английского *27*-буквенного алфавита от *A* до *Z* и пробела с множеством Q всех числовых эквивалентов q биграмм элементарных сообщений m_i из M^* с числовыми эквивалентами от 0 до 26.

Числовой эквивалент $\widetilde{q_i}$ биграммы $m_{2i-1}m_{2i}$ сообщения m, состоящий из двух букв m_{2i-1} и m_{2i} с числовыми эквивалентами q_{2i-1} и $q_{2i} \in Q$ определяем, как целое число:

$$\widetilde{q_i} = 27q_{2i-1} + q_{2i} \in \{0, 1, \dots, 728\}$$

(предварительно исходное сообщение m разбиваем на биграммы с добавлением пробела, если m содержит нечётное число элементарных сообщений, в частности букв). Таким образом, сообщение m длины t разбивается на $\lceil \frac{t}{2} \rceil$ чисел, соответствующих биграммам исходного сообщения.

Алгоритм Inf_Coding. *Алгоритм кодирования исходного сообщения*

Вход: исходное сообщение m чётной длины t.

Выход: набор чисел $\tilde{Q} = \{\widetilde{q_1}, \dots, \widetilde{q_{\lceil \frac{t}{2} \rceil}}\}$.

Метод:

1) разбиение m на отдельные блоки по 2 символа – биграммы;

2) соответствие каждой букве m_i в биграмме ее порядкового номера q_i в алфавите M;

3) расчёт числового эквивалента биграммы $\tilde{q} = 27q_1 + q_2$ для каждой биграммы;

4) формирование последовательности числовых эквивалентов биграмм $\tilde{Q} = \{\widetilde{q_1}, \dots, \widetilde{q_{\lceil \frac{t}{2} \rceil}}\}$.

Алгоритм De_Coding. *Алгоритм декодирования шифртекста*

Вход: набор чисел $\tilde{Q} = \{\widetilde{q_1}, \dots, \widetilde{q_{\lceil \frac{t}{2} \rceil}}\}$.

Выход: исходное сообщение m длины t.

Метод:

1) вычисление исходных числовых эквивалентов символов из значения элемента $\tilde{q}$ каждой биграммы по правилу:

$q_1 = \tilde{q}\ div\ 27$ – целая часть от деления на 27;

$q_2 = \tilde{q}\ mod\ 27$ – остаток от деления на 27;

2) каждому вычисленному числовому эквиваленту символа q_i ставим в соответствие символ m_i из алфавита M;

3) последовательно формируем сообщение $m = \{m_1 m_2 \dots m_t\}$.

b) Генерация ключа и функций преобразования

Для генерации ключа необходимо выбрать решение уравнения (4), определив при этом параметры l и k с помощью теорем 1–6, приведённых в [23], что позволит получить необходимое решение с указанными параметрами на основе некоторого изначального уравнения. Вопрос генерации подобного изначального уравнения остаётся открытым и будет рассмотрен в дальнейших работах.

В данном примере будут использоваться следующие векторы, определяемые (3). Допустим, определены следующие равносильные векторы:

$$A^l = (a_1, \dots, a_l),\ \ B^l = (b_1, \dots, b_l), A^l \overset{k}{=} B^l, 1 < k < l.$$

На их основе построим параметрическое решение МСДУ (1) с параметрами a и b по следующему правилу:

$$v_i = \begin{cases} a_i a + b_i b, i = 1..l, \\ b_{i-l} a + a_{i-l} b, \ \ i = (l+1)..2l. \end{cases}$$

С помощью этого параметрического решения, определим функции прямого преобразования $C_L(a,b)$ открытого текста m и обратного преобразования $C_R(a,b)$ криптограммы c:

$$C_L(a,b) = v_1(a,b)^d + \cdots + v_l(a,b)^d - v_{l+1}(a,b)^d - \ldots - v_{2l-1}(a,b)^d,$$
$$C_R(a,b) = v_{2l}(a,b)^d, 1 < d \le k.$$

Параметр a – числовой эквивалент исходного элементарного сообщения, в частности, буквы или конкатенация букв из алфавита M, параметр b – выбирается произвольно и является ключом СЗИ.

Алгоритм Gen_Keys. *Алгоритм генерации ключей и функций преобразования*

Вход: параметры l и k.

Выход: функции преобразования $C_L(a,b)$, $C_R(a,b)$ и секретный ключ b.

Метод:

1) выбор решения уравнения (1) с параметрами l и k в виде

$A^l \overset{k}{=} B^l,\ 1 < k < l,\ A^l = (a_1, \ldots, a_l),\ B^l = (b_1, \ldots, b_l)$;

2) расчёт функций $v_i(a,b)$по следующему правилу:

$$v_i = \begin{cases} a_i a + b_i b, i = 1..l, \\ b_{i-l} a + a_{i-l} b, \ \ i = (l+1)..2l; \end{cases}$$

3) расчёт функций преобразования $C_L(a,b)$ и $C_R(a,b)$ по правилу:

$$C_L(a,b) = v_1(a,b)^d + \cdots + v_l(a,b)^d - v_{l+1}(a,b)^d - \cdots - v_{2l-1}(a,b)^d,$$
$$1 < d \le k,$$
$$C_R(a,b) = v_{2l}(a,b)^d;$$

4) выбор значения секретного ключа b.

c) Прямое преобразование

Закодируем исходное сообщение m длины t по правилу из пункта **а)**. Таким образом мы получаем последовательность $\tilde{Q} = \{\widetilde{q_1}, \dots, \widetilde{q_{\lceil \frac{t}{2} \rceil}}\}$ числовых эквивалентов биграмм сообщения m. Тогда прямое преобразование исходного текста с помощью ключа b будет иметь вид последовательности $C = \{c_1, \dots, c_{\lceil \frac{t}{2} \rceil}\}$, определяемой, как:

$$\begin{cases} c_1 = C_L(\widetilde{q_1}, b) = v_1(\widetilde{q_1}, b)^d + \dots - v_{2l-1}(\widetilde{q_1}, b)^d, \\ c_2 = C_L(\widetilde{q_2}, b) = v_1(\widetilde{q_2}, b)^d + \dots - v_{2l-1}(\widetilde{q_2}, b)^d, \\ \dots \\ c_{\lceil \frac{t}{2} \rceil} = C_L\left(\widetilde{q_{\lceil \frac{t}{2} \rceil}}, b\right) = v_1\left(\widetilde{q_{\lceil \frac{t}{2} \rceil}}, b\right)^d + \dots - v_{2l-1}\left(\widetilde{q_{\lceil \frac{t}{2} \rceil}}, b\right)^d. \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} c_1 = (a_1\widetilde{q_1} + b_1 b)^d + \dots - (b_{2l-1}\widetilde{q_1} + a_{2l-1}b)^d, \\ c_2 = (a_1\widetilde{q_2} + b_1 b)^d + \dots - (b_{2l-1}\widetilde{q_2} + a_{2l-1}b)^d, \\ \dots \\ c_{\lceil \frac{t}{2} \rceil} = \left(a_1\widetilde{q_{\lceil \frac{t}{2} \rceil}} + b_1 b\right)^d + \dots - \left(b_{2l-1}\widetilde{q_{\lceil \frac{t}{2} \rceil}} + a_{2l-1}b\right)^d. \end{cases}$$

Последовательность $C = \{c_1, \dots, c_{\lceil \frac{t}{2} \rceil}\}$ – результат прямого преобразования исходного текста m.

Алгоритм Encryption. *Алгоритм прямого преобразования*

Вход: исходное сообщение m и ключ прямого преобразования $(C_L(a, b), b)$.

Выход: последовательность $C = \{c_1, \dots, c_{\lceil \frac{t}{2} \rceil}\}$.

Метод:

1) формируем сообщение m' по правилу: если длина t исходного сообщения m – четное число, то $m' = m$, иначе $m' = m + \text{" "}$;

2) алгоритм кодирования исходного сообщения m';

3) расчёт последовательности $C = \{c_1, \dots, c_{\lceil \frac{t}{2} \rceil}\}$ на основе последовательности числовых эквивалентов биграмм;

4) $\tilde{Q} = \{\widetilde{q_1}, \dots, \widetilde{q_{\lceil \frac{t}{2} \rceil}}\}$ по правилу $c_i = C_L(\widetilde{q_i}, b)$ отдельно для каждой биграммы.

d) Обратное преобразование

Для обратного преобразования шифртекста c следует использовать функцию $C_R(a, b)$. В этом случае алгоритм обратного преобразования для числа c будет состоять в решении уравнения $C_R(a, b) = c$ относительно неизвестного a.

$$C_R(a,b) = c \;\Leftrightarrow\; v_{2l}(a,b)^d = c \;\Leftrightarrow\; (b_l a + a_l b)^d = c \;\Leftrightarrow$$

$$\Leftrightarrow\; b_l a + a_l b = \sqrt[d]{c} \;\Leftrightarrow\; a = \frac{\sqrt[d]{c} - a_l b}{b_l}. \qquad (10)$$

Тогда обратное преобразование будет состоять в применении формулы (5) к элементам последовательности $C = \{c_1, \dots, c_{\lceil \frac{t}{2} \rceil}\}$, и в дальнейшем разделении полученных элементов $\widetilde{q_i}$ на q_{2i-1} и q_{2i}

$$\begin{cases} \widetilde{q_1} = \dfrac{\sqrt[d]{c_1} - a_l b}{b_l}, \\ \widetilde{q_2} = \dfrac{\sqrt[d]{c_2} - a_l b}{b_l}, \\ \dots \\ \widetilde{q_{\lceil \frac{t}{2} \rceil}} = \dfrac{\sqrt[d]{c_{\lceil \frac{t}{2} \rceil}} - a_l b}{b_l}. \end{cases} \Rightarrow \begin{cases} q_1 = \widetilde{q_1} \text{ div } 27, \\ q_2 = \widetilde{q_1} \text{ mod } 27, \\ \dots \\ q_{t-1} = \widetilde{q_{\lceil \frac{t}{2} \rceil}} \text{ div } 27, \\ q_t = \widetilde{q_{\lceil \frac{t}{2} \rceil}} \text{ mod } 27. \end{cases}$$

Далее, элементам $q_1, \dots, q_t$ ставим в соответствие символы $m_1, \dots, m_t$ из алфавита M и получим открытый текст $m_1, \dots, m_t$ – как результат обратного преобразования.

Алгоритм Decryption. *Алгоритм обратного преобразования:*

Вход: последовательность $C = \{c_1, \dots, c_{\lceil \frac{t}{2} \rceil}\}$ и ключ обратного преобразования $(C_R(a, b), b)$.

Выход: исходное сообщение m.

Метод:

1) расчёт последовательности $\tilde{Q} = \{\widetilde{q_1}, \dots, \widetilde{q_{\lfloor \frac{t}{2} \rfloor}}\}$ на основе результата прямого преобразования $C = \{c_1, \dots, c_{\lfloor \frac{t}{2} \rfloor}\}$ по правилу $\widetilde{q_l} = \frac{\sqrt[d]{c_i} - a_l b}{b_l}$ отдельно для каждого элемента последовательности;

2) алгоритм декодирования исходного сообщений для $\tilde{Q} = \{\widetilde{q_1}, \dots, \widetilde{q_{\lfloor \frac{t}{2} \rfloor}}\}$;

3) если полученное сообщение m' оканчивается на " ", то для получения m отбрасываем его, иначе $m = m$'.

II. Пример прямого и обратного преобразований:

a) кодирование биграмм исходного сообщения.

Пусть исходное сообщение $m = HELLOWORLD$. Преобразуем его в последовательность $\tilde{Q} = \{\widetilde{q_1}, \dots, \widetilde{q_{\lfloor \frac{t}{2} \rfloor}}\}$

$$\begin{cases} m_1 = H \\ m_2 = E \\ m_3 = L \\ m_4 = L \\ m_5 = O \\ m_6 = W \\ m_7 = O \\ m_8 = R \\ m_9 = L \\ m_{10} = D \end{cases} \Rightarrow \begin{cases} q_1 = 8 \\ q_2 = 5 \\ q_3 = 12 \\ q_4 = 12 \\ q_5 = 15 \\ q_6 = 23 \\ q_7 = 15 \\ q_8 = 18 \\ q_9 = 12 \\ q_{10} = 4 \end{cases} \Rightarrow \begin{cases} \widetilde{q_1} = 27q_1 + q_2 = 221 \\ \widetilde{q_2} = 27q_3 + q_4 = 336 \\ \widetilde{q_3} = 27q_5 + q_6 = 428 \\ \widetilde{q_4} = 27q_7 + q_7 = 423 \\ \widetilde{q_5} = 27q_9 + q_8 = 328 \end{cases}$$

Последовательность $\tilde{Q} = \{221, 336, 428, 423, 328\}$ будет использоваться для прямого преобразования.

b) Генерация ключа и функций преобразования

Для простоты и демонстрации будем брать небольшие значения исходного решения и ключа.

Пусть $l = 6, k = 5$ и исходное решение $A^l \overset{k}{=} B^l$ имеет вид:

$$1, 6, 7, 17, 18, 23 \overset{5}{=} 2, 3, 11, 13, 21, 22.$$

Тогда параметрические решения $v_i(a, b)$ определяются, как:

$$\begin{cases} v_1(a,b) = a + 2b, & v_5(a,b) = 18a + 21b, & v_9(a,b) = 11a + 7b, \\ v_2(a,b) = 6a + 3b, & v_6(a,b) = 23a + 22b, & v_{10}(a,b) = 13a + 17b, \\ v_3(a,b) = 7a + 11b, & v_7(a,b) = 2a + b, & v_{11}(a,b) = 21a + 18b, \\ v_4(a,b) = 17a + 13b, & v_8(a,b) = 3a + 6b, & v_{12}(a,b) = 22a + 23b. \end{cases}$$

На основе данного параметрического решения определим $C_L(a,b)$ и $C_R(a,b)$:

$C_L(a,b) = (a+2b)^5 + \cdots + (23a+22b)^5 - (2a+b)^5 - \cdots - (21a+18b)^5$,

$C_R(a,b) = (22a+23b)^5$.

c) Прямое преобразование

Возьмем в качестве ключа $b = 3$. Тогда рассчитаем прямое преобразование элементов последовательности:

$$\tilde{Q} = \{221, 336, 428, 423, 328\}$$

$$\begin{cases} c_1 = C_L(221{,}3) = (221 + 2*3)^5 + \cdots - (21*221 + 18*3)^5, \\ c_2 = C_L(336{,}3) = (336 + 2*3)^5 + \cdots - (21*221 + 18*3)^5, \\ c_3 = C_L(428{,}3) = (428 + 2*3)^5 + \cdots - (21*221 + 18*3)^5, \\ c_4 = C_L(423{,}3) = (423 + 2*3)^5 + \cdots - (21*221 + 18*3)^5, \\ c_5 = C_L(328{,}3) = (328 + 2*3)^5 + \cdots - (21*221 + 18*3)^5. \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} c_1 = 2\,915\,244\,687\,863\,990\,000, \\ c_2 = 23\,119\,860\,000\,976\,300\,000, \\ c_3 = 76\,769\,140\,112\,716\,400\,000, \\ c_4 = 72\,419\,643\,402\,099\,600\,000, \\ c_5 = 20\,518\,602\,614\,059\,500\,000. \end{cases}$$

$C = \{2\,915\,244\,687\,863\,990\,000, 23\,119\,860\,000\,976\,300\,000,$

$76\,769\,140\,112\,716\,400\,000, 72\,419\,643\,402\,099\,600\,000,$

$20\,518\,602\,614\,059\,500\,000\}$ – результат прямого преобразования.

d) Обратное преобразование

Для обратного преобразования исходного сообщения следует использовать функцию $C_R(a,b)$. Рассчитаем значения $\widetilde{q_i}$ исходного текста:

$$\begin{cases} \widetilde{q_1} = (\sqrt[5]{2915244687863990000} - 23 * 3)/22 = 221, \\ \widetilde{q_2} = (\sqrt[5]{23119860000976300000} - 23 * 3)/22 = 336, \\ \widetilde{q_3} = (\sqrt[5]{76769140112716400000} - 23 * 3)/22 = 428, \\ \widetilde{q_4} = (\sqrt[5]{72419643402099600000} - 23 * 3)/22 = 423, \\ \widetilde{q_5} = (\sqrt[5]{20518602614059500000} - 23 * 3)/22 = 328. \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} q_1 = 221 \text{ div } 27 = 8 \\ q_2 = 221 \bmod 27 = 5 \\ q_3 = 336 \text{ div } 27 = 12 \\ q_4 = 336 \bmod 27 = 12 \\ q_5 = 428 \text{ div } 27 = 15 \\ q_6 = 428 \bmod 27 = 23 \\ q_7 = 423 \text{ div } 27 = 15 \\ q_8 = 423 \bmod 27 = 18 \\ q_9 = 328 \text{ div } 27 = 12 \\ q_{10} = 328 \bmod 27 = 4 \end{cases} \Rightarrow \begin{cases} m_1 = H \\ m_2 = E \\ m_3 = L \\ m_4 = L \\ m_5 = O \\ m_6 = W \\ m_7 = O \\ m_8 = R \\ m_9 = L \\ m_{10} = D \end{cases}$$

Таким образом, мы получили исходное сообщение:

$$\text{m} = HELLOWORLD.$$

Заключение

Таким образом, для практических приложений следует выбрать подходящую МСДУ и соответствующие модифицированные соотношения на основе теоремы пункта 2 с учётом степеней равносильностей. В рассмотренном выше примере ДБК был выбран простой вариант функции прямого преобразования, в самом же деле можно предложить сложный алгоритм для выбора указанной функции с соответствующими равносильностями. В дальнейшем их можно отождествлять с числовыми и функциональными ранцами [39], причём все решения МСДУ, числовые или параметрические, при некоторых ограничениях можно рассмотреть, как числовые или функциональные ранцы, относительно которых следует применить теорию ранцевых СЗИ.

Итак, авторами разработана математическая модель ДБК, содержащая диофантовы трудности при решении МСДУ заданной размерности и порядка, и разработан алгоритм реализации этой криптосистемы. Как отмечено выше, для определения числовых эквивалентов элементарных сообщений легальный пользователь решает простое уравнение заданной степени, а нелегальный – многовариативную МСДУ заданной размерности и порядка.

Решение поставленных в рукописи задач позволит получить научно-технический задел для разработки и дальнейшей реализации стойких и эффективных математических моделей алфавитных систем защиты информации, а также дать новый импульс в развитии математического моделирования криптосистем, содержащих диофантовы трудности.

Работа поддержана грантом РФФИ № 19-01-00596

Литература

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. – 2-е изд., испр. и доп. – Москва: Гелиос АРВ, 2002. – 480 с.

2. Koblitz N. A Course in Number Theory and Cryptography. – New York: Springer-Verlag, 1987. – 235 p.

3. Введение в криптографию. / Под ред. Ященко В. В. — 2-е изд., испр. — М.: МЦНМО: «ЧеРо», 1998–272 с.

4. Shannon C. Communication theory of secrecy systems // Bell System Techn. J. – 1949. – Vol. 28, № 4. – p. 656–715.

5. Романьков В. А. Криптографический анализ некоторых известных схем шифрования, использующих автоморфизмы // Прикладная дискретная математика. 2013. № 3(21). С. 35–51.

6. Ерофеев С. Ю. Диофантовость дискретного логарифма, ПДМ, 2011, Приложение № 4, с. 31–32.

7. Ерофеев С. Ю., Романьков В. А. О построении возможно односторонних функций на основе алгоритмической неразрешимости проблемы эндоморфной сводимости в группах. ПДМ, 2012, № 3(17), с.13–24.

8. Романьков В. А. Алгебраическая криптография. Омск: Изд-во Ом. ун-та, 2013. 136 с.

9. Романьков В. А., Диофантова криптография на бесконечных группах, ПДМ, 2012, № 2(16), с.15–42.

10. Романьков В. А., Криптографический анализ аналога схемы Диффи–Хеллмана, использующего сопряжение и возведение в степень, на матричной платформе, ПДМ. Приложение, 2014, выпуск 7, с.56–58.

11. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). – Уфа: Лето, 2011. - С. 8-13.

12. Круглов В. В., Борисов В. В. Искусственные нейронные сети. Теория и практика. – М.: Горячая линия. - Телеком, 2002. 382 с.

13. McEliece R.J. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report, Jet Propulsion Laboratory, Pasadena. 1978. pp. 114–116.

14. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. Изд. "Мир", 1976. 594 с.

15. Shuhong Gao, Raymond Heindl. Multivariate public key cryptosystems from Diophantine equations. Designs Codes and Cryptography 67(1):1–18 April 2011.

16. Harry Yosh. The key exchange cryptosystem used with higher order Diophantine equations. International Journal of Network Security & Its Applications (IJNSA), Vol.3, № 2, March 2011, pp. 43–50.

17. Berczes A., Hajdu L., Hirata-Kohno N., Kovaces T.;Petho A. A key exchange protocol based on Diophantine equations and S-integers //JSIAM Lett. 6, 2014. pp.85–88.

18. Bagheri Mohammad A public-key cryptosystem based on Diophantine equations // International Journal of Pure and Applied Mathematics. – 2003. – Vol.5. – № 2. – pp. 135–140.

19. Hirata-Kohno N., Petho A. On a key exchange protocol based on Diophantine equations // Information J 5(3): 17–21, 2013.

20. Okumura S., A public key cryptosystem based on Diophantine equations of degree increasing type // Pacific Journal of Mathematics for Industry, 7 (4), pp. 33–45, Springer, Berlin Heidelberg, 2015.

21. Ding J., Kudo M., Okumura S., Takagi T., Tao C., Cryptanalysis of a Public Key Cryptosystem Based on Diophantine Equations via Weighted LLL Reduction, IWSEC 7, 2016.

22. 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. twirpx.com/file/2085412

23. Осипян В. О. Разработка математической модели дисимметричной биграммной криптосистемы на основе параметрического решения многостепенной системы диофантовых уравнений // Инженерный вестник Дона, 2020, № 6.URL: ivdon.ru/ru/magazine/archive/N6y2020/6534

24. Osipyan V. O. Development of the mathematic model of dissymmetric bigram cryptosystem based on a parametric solution family of multi-degree system of Diophantine equations, 2020. dl.acm.org/doi/10.1145/3433174.3433596

25. Осипян В. О. Математическое моделирование систем защиты данных на основе диофантовых уравнений // Прикаспийский журнал: управление и высокие технологии. – 2018. – № 1 (41). – с. 151–160.

26. Choudhry, A. Ideal solutions of the Tarry-Escott problem of degrees four and five and related diophantine systems, L'Enseignement Mathematique, 49 (2003), pp.101–108.

27. Dorwart, H.L. and Brown O. E. The Tarry-Escott problem, Amer. Math. Monthly 44 (1937), pp. 613–626.

28. Chernick J. Ideal solutions of the Tarry-Escott problem //Amer. Monthly, 1937, 5, 44n.10, pp.626-633.

29. Матиясевич Ю. В. Десятая проблема Гильберта. – М.: Издательская фирма "Физико-математическая литература" ВО Наука, 1993.– 224 с.

30. Матиясевич Ю. В. Диофантовы множества // Успехи матем. наук. – 1972.– т. 26. – вып.– 5(167). – с.185-222.

31. Chor B., Rivest R. A knapsack-type public key cryptosystem based on arithmetic in finite fields // IEEE Transactions on Information Theory. 1988. Vol. IT – 34. pp. 901-909.

32. Айерленд К., Роузен М. Классическое введение в современную теорию чисел. М.: "Мир", 1987. – 416 с.

33. Dickson L. E. History of the Theory of Numbers. – New York, 1971. Vol. 2. Diophantine Analysis.

34. Carmichael R. D. The Theory of Numbers and Diophantine Analysis. – New York, 1959. – 118 p.

35. Gloden A. Mehgradige Gleichungen. – Groningen, 1944. – p. 104.

36. Cassels J. W. S. On a Diophantine Equation //Acta Arithmetica. – 1960. – Vol. 6. – pp. 47–52.

37. Osipyan V.O. Mathematical modelling of cryptosystems based on Diophantine problem with gamma superposition method // SIN '15 Proceedings of the 8th International Conference on Security of Information and Networks ACM, 2015. Pp. 338–341.

38. Осипян В. О., Литвинов К. И., Жук А.С., Разработка математических моделей систем защиты информации на основе многостепенных систем диофантовых уравнений // Экологический вестник научных центров черноморского экономического сотрудничества, т.3, №16. Кубанский государственный университет (Краснодар), 2019, с.6–15.

39. Osipyan V. O. Building of alphabetic data protection cryptosystems on the base of equal power knapsacks with Diophantine problems // dl.acm.org/citation.cfm?id=2388593 2012, pp.124-129.

40. Osipyan V. O., Litvinov K. I. A mathematical model of the cryptosystem based on the linear Diophantine equation, 2018. sinconf.org/sin2018/accepted-papers.php.

41. Осипян В. О. Математическое моделирование систем защиты данных на основе диофантовых уравнений // Прикаспийский журнал: управление и высокие технологии, 2018, № 1 (41). С.152-160.

42. Осипян В. О., Григорян Э. С. Метод параметризации диофантовых уравнений и математическое моделирование систем защиты данных на их основе // Прикаспийский журнал: управление и высокие технологии. – 2019. – № 1 (45), с. 164–172.

43. Osipyan V. O., Litvinov K. I., Bagdasaryan R. Kh., Lukashchik E. P., Sinitsa S. G., Zhuk A. S. Development of information security system mathematical models by the solutions of the multigrade Diophantine equation systems / SIN '19 Proceedings of the 12th International Conference on Security of Information and Networks. ACM Press, 2019, pp.1–8.

References

1. Alferov A. P., Zubov A. Ju., Kuz'min A. S., Cheremushkin A. V. Osnovy kriptografii [Fundamentals of cryptography]. 2nd izd., isprav. i dop. Moskva: Gelios ARV, 2002. 480 p.

2. Koblitz N. A Course in Number Theory and Cryptography. New York: Springer-Verlag, 1987. 235 p.

3. Vvedenie v kriptografiju. [Introduction to cryptography]. Red. Jashhenko V. V. 2-e. izd. M.: MCNMO: «CheRo», 1998. 272 p.

4. Shannon C. Bell System Techn. J. 1949. Vol. 28, № 4. pp. 656–715.

5. Roman'kov V. A. Prikladnaja diskretnaja matematika. 2013. № 3(21). Pp.35–51.

6. Erofeev S. Ju. PDM, 2011. Prilozhenie № 4, pp.31–32.

7. Erofeev S. Ju., Roman'kov V. A. PDM, 2012, № 3(17), pp.13–24.

8. Roman'kov V. A. Algebraicheskaja kriptografija [Algebraic cryptography]. Omsk: Izdatelstvo Om. Universiteta, 2013. 136 p.

9. Roman'kov V. A., PDM, 2012, № 2(16), pp.15–42.

10. Roman'kov V. A., PDM. Prilozhenie, 2014, issue7, pp. 56–58.

11. Borshevnikov A. E. Sovremennye tendencii tekhnicheskih nauk: materialy Mezhdunar. nauch. konf. (g. Ufa, oktyabr' 2011 g.). Ufa: Leto, 2011. pp. 8-13.

12. Kruglov V. V., Borisov V. V. Iskusstvennye nejronnye seti. Teorija i praktika [Artificial neural networks. Theory and practice]. M.: Gorjachaja linija, Telekom, 2002. 382 p.

13. McEliece R.J. DSN Progress Report, Jet Propulsion Laboratory, Pasadena. 1978. pp. 114–116.

14. Piterson U., Ujeldon Je. Kody, ispravljajushhie oshibki [Error-correcting codes.]. Izd. "Mir", 1976. 594 p.

15. Shuhong Gao, Raymond Heindl. Designs Codes and Cryptography 67(1):1–18 April 2011.

16. Harry Yosh. International Journal of Network Security & Its Applications (IJNSA), Vol.3, № 2, March 2011, pp.43–50.

17. Berczes A., Hajdu L., Hirata-Kohno N., Kovaces T.; Petho A. JSIAM Lett. 6, 2014. pp.85–88.

18. Bagheri Mohammad International Journal of Pure and Applied Mathematics. 2003. Vol.5. № 2. pp. 135–140.

19. Hirata-Kohno N., Petho A. Information J 5(3): pp.17–21, 2013.

20. Okumura S., Pacific Journal of Mathematics for Industry, 7 (4), pp. 33–45, Springer, Berlin Heidelberg, 2015.

21. Ding J., Kudo M., Okumura S., Takagi T., Tao C, Cryptanalysis of a Public Key Cryptosystem Based on Diophantine Equations via Weighted LLL Reduction, IWSEC 7, 2016.

22. Osipjan V. O. Modelirovanie sistem zashhity informacii soderzhashhih diofantovy trudnosti. Razrabotka metodov reshenij mnogostepennyh sistem diofantovyh uravnenij. Razrabotka nestandartnyh rjukzachnyh kriptosistem: Monografija [Modeling of information security systems containing Diophantine difficulties. Development of methods for solving multi-degree systems of Diophantine equations. Development of non-standard backpack cryptosystems]. LAP, 2012. 344 p. URL: twirpx.com/file/2085412

23. Osipjan V. O., Inzhenernyj vestnik Dona, 2020, № 6. URL: ivdon.ru/ru/magazine/archive/N6y2020/6534

24. Osipyan V. O. Development of the mathematic model of dissymmetric bigram cryptosystem based on a parametric solution family of multi-degree system of Diophantine equations, 2020.URL: dl.acm.org/doi/10.1145/3433174.3433596

25. Osipjan V. O. Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii. 2018. № 1 (41). pp. 151–160.

26. Choudhry, A. L'Enseignement Mathematique, 49 (2003), pp. 101–108.

27. Dorwart, H.L. and Brown O. E. The Tarry-Escott problem, Amer. Math. Monthly 44 (1937), pp. 613–626.

28. Chernick J. Amer. Monthly, 1937, 5, 44n.10, pp. 626-633.

29. Matijasevich Ju. V. Desjataja problema Gil'berta [Hilbert's tenth problem]. M.: Izdatelstvo “Fiziko-matematicheskaja literatura” VO Nauka, 1993. 224 p.

30. Matijasevich Ju. V. Uspehi matem. nauk. 1972. t. 26. issue 5(167). Pp.185-222 p.

31. Chor B., Rivest R. EEE Transactions on Information Theory. 1988. Vol. IT – 34. Pp.901-909.

32. Ajerlend K., Rouzen M. Klassicheskoe vvedenie v sovremennuju teoriju chisel [Classical introduction to modern number]. M.: “Mir”, 1987. 416 p.

33. Dickson L. E. History of the Theory of Numbers. New York, 1971. Vol. 2. Diophantine Analysis.

34. Carmichael R. D. The Theory of Numbers and Diophantine Analysis. New York, 1959. 118 p.

35. Gloden A. Mehgradige Gleichungen. Groningen, 1944. 104 p.

36. Cassels J. W. S. Acta Arithmetica. 1960. Vol. 6. pp. 47–52.

37. Osipyan V.O. SIN '15 Proceedings of the 8th International Conference on Security of Information and Networks ACM, 2015. Pp. 338–341.

38. Osipjan V. O., Litvinov K. I., Zhuk A.S., Jekologicheskij vestnik nauchnyh centrov chernomorskogo jekonomicheskogo sotrudnichestva t.3, №16. Kubanskij gosudarstvennyj universitet (Krasnodar), 2019, s.6–15.

39. Osipyan V. O. Building of alphabetic data protection cryptosystems on the base of equal power knapsacks with Diophantine problems. URL: acm.org/citation.cfm?id=2388593 2012, pp.124-129.

40. Osipyan V. O., Litvinov K. I. A mathematical model of the cryptosystem based on the linear Diophantine equation, 2018. URL: sinconf.org/sin2018/accepted-papers.php.

41. Osipjan V. O. Prikaspijskij zhurnal: upravlenie i vysokie tehnologii, 2018, № 1 (41). pp.152-160.

42. Osipjan V. O., Grigorjan Je. S. Prikaspijskij zhurnal: upravlenie i vysokie tehnologii. 2019. № 1 (45), pp.164–172.

43. Osipyan V. O., Litvinov K. I., Bagdasaryan R. Kh., Lukashchik E. P., Sinitsa S. G., Zhuk A. S. SIN '19 Proceedings of the 12th International Conference on Security of Information and Networks. ACM Press, 2019, pp.1–8.