БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ernst M. Gabidulin*, Public-key cryptosystems based on linear codes, Report DUT-TWI-95-30, Delft University of Technology, Delft, The Netherlads, 1995.
2. *Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. – М., 2002. – 480 с.
3. *Бабаш А. В., Глухов М.М., Шанкин Г.П.* О преобразованиях множества слов в конечном алфавите, не размножающих искажений // Дискретная математика. – М., 1997. – Т. 9. – Вып. 3. – С. 3-19.
4. *Levenshtein V. I.* Binary codes capable of correcting deletions, insertions, and reversals // Sov. Phys. Dokl., February, 1966. – P. 707-710.
5. *Гаврилова Т.А., Хорошевский В.Ф.* Базы знаний интеллектуальных систем: Учебник для вузов. – СПб., 2000. – 384 с.

Минаков Сергей Викторович
Краснодарское высшее военное училище (ВИ).
E-mail: MinakovSergey1973@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79184102497.

Финько Олег Анатольевич
Кубанский государственный технологический университет.
Институт информационных технологий и безопасности.
E-mail: ofinko@yandex.ru.
350072, г. Краснодар, ул. Московская, 2.
Тел.: +79615874848.

Minakov Sergey Viktorovich
Krasnodar higher military school (MI).
E-mail: MinakovSergey1973@yandex.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: 79184102497.

Finko Oleg Anatol'evich
Kuban state technological university.
Institute of information technologies and safety.
E-mail: ofinko@yandex.ru.
2, Moscow, Krasnodar, 350072, Russia.
Phone: +79615874848.

УДК 511+519.719.2

Д.В. Самойленко, О.А. Финько

ПОМЕХОУСТОЙЧИВАЯ КРИПТОСИСТЕМА, ОСНОВАННАЯ НА КИТАЙСКОЙ ТЕОРЕМЕ ОБ ОСТАТКАХ, ДЛЯ *N* КАНАЛОВ С ШУМОМ И ИМИТИРУЮЩИМ ЗЛОУМЫШЛЕННИКОМ

Рассматривается помехоустойчивая модулярная криптографическая система, функционирующая в кольце Z_p положительных целых чисел по модулю p. Предложен алгоритм расширения системы оснований криптографической системы. Представлена оценка помехоустойчивости предложенной криптографической системы по отношению к традиционным (раздельным) методам помехо- и криптозащиты.

Достоверность; избыточное кодирование; Китайская теорема об остатках; криптоаналитик; криптосистема; модулярная арифметика; помехоустойчивость.

D.V. Samoylenko, O.A. Finko

NOISE-IMMUNITY CRYPTOSYSTEM BASED ON THE CHINESE REMAINDER THEOREM, FOR N NOISE CHANNELS AND SIMULATES A CRACKER

We consider the interference proof modular cryptographic system functioning in the ring Z_p positive integers modulo p. The algorithm of expansion of system of the bases of cryptographic system is offered. An estimation of the noise immunity of the proposed cryptographic system in relation to traditional (separate) methods of error- and encryption.

Reliability; error correcting coding; Chinese remainder theorem; cryptanalyst; cryptographic system; modular arithmetic; performance in terms of error probability.

Криптографические методы, предназначенные для защиты данных от несанкционированных изменений при передаче их по общедоступным каналам связи или другим видам использования, чувствительны к искажениям различного происхождения (помехи, имитация злоумышленника). Изменение одного бита зашифрованных данных (криптограмм) может нарушить взаимно-однозначное соответствие между передаваемыми и принимаемыми криптограммами и, как следствие, уменьшить достоверность передачи. В информационном аспекте уменьшение достоверности передачи эквивалентно потере некоторого количества информации. Вследствие чего возникает потребность в использовании таких систем, которые были бы устойчивы к воздействию таких искажений. Как правило, наиболее часто применяют две различные системы: одну для обнаружения (исправления) ошибок, другую – для защиты информации от несанкционированного доступа. При этом возникает ряд проблем, требующих оперативного решения. Так, например, одной из них является согласование методов, обеспечивающих защиту от искажений в системе защиты от ошибок с применяемой криптосистемой. Криптосистема не должна получать искаженные криптограммы, в противном случае результат расшифрования заведомо не совпадет с открытым текстом. Некорректная работа или возникновение сбоя в системе защиты от ошибок может привести к тому, что она не обнаружит (не исправит) ошибку или выдаст отказ в обработке принимаемых данных и т.д. Что приведет к снижению производительности и, как следствие, потере управления и контроля при выполнении различных задач [1].

Вследствие этого возникает необходимость применения помехоустойчивых криптосистем (КС), которые лишены вышеперечисленных недостатков. Это обстоятельство является важным достоинством и превосходством помехоустойчивых КС по сравнению с традиционным (раздельным) использованием помехо- и криптозащиты [1, 2].

Цель статьи – исследование КС, функционирующей в кольце Z_p неотрицательных целых чисел по модулю p, которая способна противостоять мешающему действию различных деструктивных воздействий (преднамеренных и непреднамеренных).

Рассмотрим КС, функционирующую в кольце Z_p. Правила зашифрования и расшифрования определены как

$$E_k: M \to C, \tag{1}$$

$$D_k: C \to M. \tag{2}$$

Пусть $C_i = c_{63}^{(i)} 2^{63} + c_{62}^{(i)} 2^{62} + \ldots + c_1^{(i)} 2^1 + c_0^{(i)}$, $(c_j \in \{0,1\},\ j = 0,1,\ldots,63)$. Тогда число C_i можно ассоциировать с наименьшим неотрицательным вычетом по

основанию $m^{(i)}$, причем $0 \le C_i < m^{(i)}$, где $m^{(i)} \ge 2^{64}$ $(i = 1, 2, \dots, n)$. Соответственно преобразование (1) и (2) можно переписать в виде

$$\begin{cases} C^{(1)} = \left| E_{k^{(1)}}\left(M^{(1)}\right)\right|_{m^{(1)}}, \\ C^{(2)} = \left| E_{k^{(2)}}\left(M^{(2)}\right)\right|_{m^{(2)}}, \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \\ C^{(n)} = \left| E_{k^{(n)}}\left(M^{(n)}\right)\right|_{m^{(n)}}, \end{cases}$$

$$\begin{cases} M^{(1)} = \left| D_{k^{(1)}}\left(C^{(1)}\right)\right|_{m^{(1)}}, \\ M^{(2)} = \left| D_{k^{(2)}}\left(C^{(2)}\right)\right|_{m^{(2)}}, \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \\ M^{(n)} = \left| D_{k^{(n)}}\left(C^{(n)}\right)\right|_{m^{(n)}}, \end{cases}$$

где $M^{(i)}$ – открытые тексты, $C^{(i)}$ – криптограммы, $k^{(i)}$ – ключи, $i = 1, 2, \dots, n$.

При передаче последовательности криптограмм $C^{(1)}, C^{(2)}, \dots, C^{(n)}$ влияние искажений проявляется в том, что вместо одних переданных криптограмм принимаются другие $C^{*(1)}, C^{*(2)}, \dots, C^{*(n)}$. Таким образом, получатель получит открытые тексты $M^{*(1)}, M^{*(2)}, \dots, M^{*(n)}$, отличающиеся от исходных $M^{(1)}, M^{(2)}, \dots, M^{(n)}$.

Следует отметить, что блоки открытого текста $M^{(1)}, M^{(2)}, \dots, M^{(n)}$ могут быть образованы из сообщения, принадлежащего одному пользователю или из независимых сообщений, принадлежащих n пользователям. Для зашифрования и расшифрования может использоваться как один ключ, так и n ключей, соответствующих количеству блоков открытого текста. Способ выбора и распространения ключа(ей) не рассматривается, а предполагается, что ключ(и) уже задан.

Способность КС к обнаружению и исправлению ошибок сводится к рассмотрению множества криптограмм $\left\{C^{(1)}, C^{(2)}, \dots, C^{(n)}\right\}$ как единого информационного блока модулярного кода (МК) по системе оснований $m^{(1)}, m^{(2)}, \dots, m^{(n)}$ [3-7]. В соответствии с Китайской теоремой об остатках [8] для заданного множества целых положительных попарно взаимно простых оснований $m^{(1)}, m^{(2)}, \dots, m^{(n)}$ и множества вычетов $C^{(1)}, C^{(2)}, \dots, C^{(n)}$ при $C^{(i)} < m^{(i)}$ система сравнений

$$\begin{cases} C \equiv \left| C^{(1)}\right|_{m^{(1)}}, \\ C \equiv \left| C^{(2)}\right|_{m^{(2)}}, \\ \dots\ \dots\ \dots\ \dots \\ C \equiv \left| C^{(n)}\right|_{m^{(n)}} \end{cases} \tag{3}$$

имеет не более одного решения в интервале $0 \le C < \prod_{i=1}^{n} m^{(i)}$.

Выполняется операция расширения МК $\left\{C^{(1)}, C^{(2)}, \dots, C^{(n)}\right\}$ путем введения r избыточных оснований $m^{(n+1)}, m^{(n+2)}, \dots, m^{(n+r)}$ и получения r избыточных вычетов $C^{(n+1)}, C^{(n+2)}, \dots, C^{(n+r)}$:

$$\begin{cases} C^{(n+1)} \equiv |C|_{m^{(n+1)}}, \\ C^{(n+2)} \equiv |C|_{m^{(n+2)}}, \\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \\ C^{(n+r)} \equiv |C|_{m^{(n+r)}}, \end{cases}$$

причем $\gcd\left(m^{(i)}, m^{(j)}\right) = 1,\ i \neq j$, где $i, j = 1, 2, \ldots, n + r$. Также необходимо выполнение следующего условия:

$$m^{(1)},\ m^{(2)}, \ldots, m^{(n)} < m^{(n+1)} < m^{(n+2)} < \ldots < m^{(n+r)}.$$

В совокупности элементы информационного блока $\left\{C^{(1)}, C^{(2)}, \ldots, C^{(n)}\right\}$ и полученная последовательность избыточных криптограмм $\left\{C^{(n+1)}, C^{(n+2)}, \ldots, C^{(n+r)}\right\}$ образуют расширенный МК в кольце Z_p. В соответствии с [3-7] расширенная система криптограмм представляет расширенный МК, способный обнаруживать и исправлять ошибки.

Введем метрику МК и линейного двоичного кода (ЛДК).

Метрика МК: *весом кодового вектора* $\{C\}$ в МК является количество ненулевых криптограмм (вычетов) и обозначается $w(\{C\})$.

Кодовое расстояние между $\{C\}$ и $\{D\}$ определяется как вес их разности $w(\{C - D\})$.

Минимальное кодовое расстояние МК – наименьшее расстояние между двумя любыми кодовыми векторами по Хэммингу с учетом данного определения веса.

Под одиночной ошибкой в кодовом слове МК будем понимать произвольное искажение одной из криптограмм кодового слова МК. Соответственно q-кратная ошибка определяется как произвольное искажение q криптограмм кодового слова МК.

Полученный код обнаруживает все одиночные ошибки, если количество избыточных криптограмм $r \geq 1$ и исправляет q или менее ошибок, если $2q \leq r$.

Обнаружение ошибок в принятой последовательности криптограмм $\left\{C^{*(1)}, \ldots, C^{*(n)}, \ldots, C^{*(n+r)}\right\}$ осуществляется путем сравнения числа C^* с числом $M = \prod_{i=1}^{n} m^{(i)}$, где C^* – решение системы сравнений (3) для принятой последовательности криптограмм $C^{*(1)}, \ldots, C^{*(n)}, \ldots, C^{*(n+r)}$; $*$ – указывает на возможные искажения.

При этом, если $0 \leq C^* < M$, то принимается решение о том, что принятая последовательность криптограмм $C^{*(1)}, \ldots, C^{*(n)}, \ldots, C^{*(n+r)}$ не содержит обнаруживаемых ошибок. В противном случае фиксируется ошибка, предельная кратность которой определяется обнаруживающими способностями кода [9, 10].

Метрика ЛДК соответствует метрике Хэмминга. *Нормой (или весом)* кодового слова $x = (x_1, x_2, \ldots, x_n)$ называется число ненулевых символов.

Кодовое расстояние между словами $x = (x_1, x_2, \ldots, x_n)$ и $y = (y_1, y_2, \ldots, y_n)$ линейного двоичного кода над $GF(q)$ равно весу их разности.

Минимальное кодовое расстояние ЛДК – минимальное из всех попарных расстояний между его кодовыми словами, равно $d_{\min}$.

Под одиночной ошибкой в метрике ЛДК понимается искажение одного бита криптограммы $C^{(i)}$. Соответственно *t*-кратная ошибка определяется, как произвольное искажение *t* битов криптограммы $C^{(i)}$.

Пример *n*-канальной КС с одним избыточным каналом представлен на рис. 1.

Таким образом, вводимая избыточность в виде избыточных криптограмм обеспечивает свойства КС контролировать ошибки кодового слова МК (количество искаженных криптограмм) и корректировать ошибки в отдельно взятой криптограмме (количество искаженных битов).

Расширение МК является одной из основных операций, выполняемых в указанной КС. В [11] рассматривается алгоритм расширения МК применительно для КС. Суть его состоит в решении системы сравнений (3). В соответствии с Китай-

ской теоремой об остатках [8], решению системы сравнений (3) будет соответствовать выражение

$$C = \sum_{i=1}^{n} \oplus_M C^{(i)} B^{(i)} = \sum_{i=1}^{n} C^{(i)} B^{(i)} - R_C M\,, \tag{4}$$

где $M_i = \frac{M}{m^{(i)}}$, $B^{(i)} = k_i M_i$ – ортогональные базисы, $M = \prod_{i=1}^{n} m^{(i)}$, $k_i = \left|M_i^{-1}\right|_{m^{(i)}}$, R_C – ранг числа C для $i = 1, 2, \dots, n$.

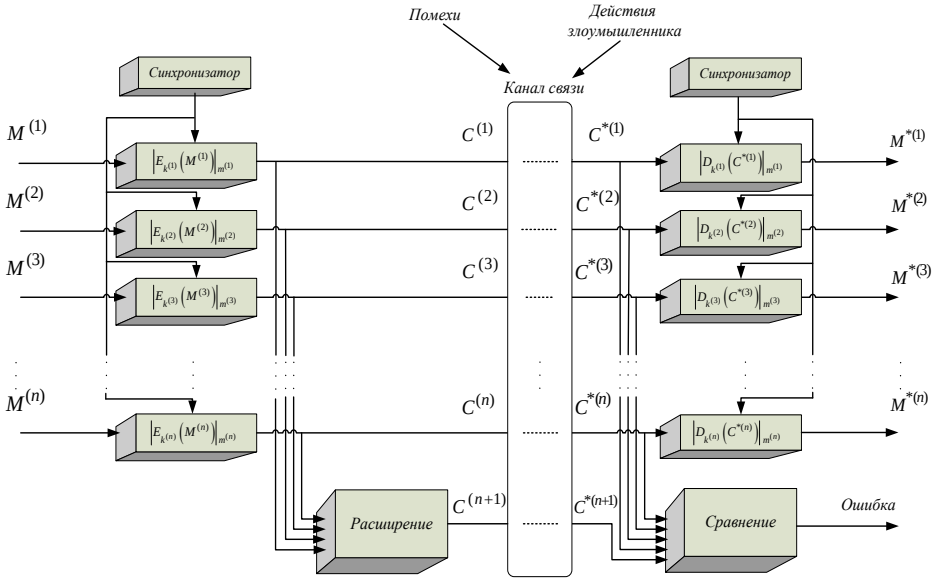

Рис. 1. КС с обнаружением однократных ошибок

В соответствии с [12] запишем:

$$R_C = \left\lfloor \sum_{i=1}^{n} \frac{C^{(i)} k_i}{m^{(i)}} \right\rfloor, \tag{5}$$

где $\lfloor x \rfloor$ – наибольшее целое число $\leq x$.

Для получения $C_{n+1}(x)$ выражение (4) с учетом (5) примет вид

$$C^{(n+1)} = \sum_{i=1}^{n} \oplus_{m^{(n+1)}} C^{(i)} \beta^{(i)} - \left|R_C \mu\right|_{m^{(n+1)}},$$

где $\beta^{(i)} = \left|B^{(i)}\right|_{m^{(n+1)}}$ и $\mu = \left|M\right|_{m^{(n+1)}}$ для $i = 1, 2, \dots, n$.

Представим $\beta^{(i)}$ и μ в двоичной системе счисления:

$$\beta^{(i)} = \left|B^{(i)}\right|_{m^{(n+1)}} = (b_{t-1} \dots b_2 b_1 b_0)_2 = \sum_{j=0}^{t-1} b_j^{(i)} 2^j\,,$$

$$\mu = \left|M\right|_{m^{(n+1)}} = (p_{t-1} \dots p_2 p_1 p_0)_2 = \sum_{j=0}^{t-1} p_j 2^j\,,$$

где $b_j^{(i)}$, $p_j \in \{0, 1\}$ – разрядные цифры двоичной системы счисления, для $i = 1, 2, \dots, n$.

Тогда получим:

$$C^{(n+1)} = \left| C^{(1)} \sum_{j=0}^{t-1} b_j^{(1)} 2^j \right|_{m^{(n+1)}} + \left| C^{(2)} \sum_{j=0}^{t-1} b_j^{(2)} 2^j \right|_{m^{(n+1)}} + \ldots$$
$$\ldots + \left| C^{(n)} \sum_{j=0}^{t-1} b_j^{(n)} 2^j \right|_{m^{(n+1)}} - \left| R_C \sum_{j=0}^{t-1} p_j 2^j \right|_{m^{(n+1)}} =$$
$$= \left| 2^{t-1} \sum_{i=1}^{n} b_{t-1}^{(i)} C^{(i)} \varepsilon_{t-1} \right|_{m^{(n+1)}} + \left| 2^{t-2} \sum_{i=1}^{n} b_{t-2}^{(i)} C^{(i)} \varepsilon_{t-2} \right|_{m^{(n+1)}} + \ldots$$
$$\ldots + \left| 2 \sum_{i=1}^{n} b_1^{(i)} C^{(i)} \varepsilon_1 \right|_{m^{(n+1)}} + \left| \sum_{i=1}^{n} b_0^{(i)} C^{(i)} \varepsilon_0 \right|_{m^{(n+1)}},$$

где $\varepsilon_j = -p_j R_C$ для $j = 0, 1, \ldots, t-1$.

Приведенные выше преобразования позволяют без прямого вычисления C окончательно получить итоговое выражение для определения $C^{(n+1)}$:

$$C^{(n+1)} = \sum_{i=1}^{n} \oplus_{m^{(n+1)}} \sum_{j}^{t-1} \otimes_{m^{(n+1)}} 2^j C^{(i)} b_j^{(i)} \varepsilon_j .$$

Алгоритм 1: *Расширение системы оснований МК.*

Ввод: $C^{(1)}, C^{(2)}, \ldots, C^{(n)}$; $m^{(1)}, m^{(2)}, \ldots, m^{(n)}$; $m^{(n+1)}$.

Вывод: $C^{(n+1)}$.

Предвычисление: $M = \prod_{i=1}^{n} m^{(i)}$, $M_i = \frac{M}{m^{(i)}}$, $B^{(i)} = k_i M_i$, $k_i = \left| M_i^{-1} \right|_{m^{(i)}}$,

$$\beta^{(i)} = \left| B^{(i)} \right|_{m^{(n+1)}} = (b_{t-1} \ldots b_2 b_1 b_0)_2 = \sum_{j=0}^{t-1} b_j^{(i)} 2^j,$$
$$\mu = |M|_{m^{(n+1)}} = (p_{t-1} \ldots p_2 p_1 p_0)_2 = \sum_{j=0}^{t-1} p_j 2^j,$$
$$1 \le i \le n.$$

Шаг 1: Определить ранг: $R_C = \left\lfloor \sum_{i=1}^{n} C^{(i)} l_i \right\rfloor$, где $l_i = k_i / m^{(i)}$.

Шаг 2: Выполнить:

$$\begin{array}{cccc} C_{t-1}^{(1)} = C^{(1)} b_{t-1}^{(1)} & \cdots & C_1^{(1)} = C^{(1)} b_1^{(1)} & C_0^{(1)} = C^{(1)} b_0^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ C_{t-1}^{(n)} = C^{(n)} b_{t-1}^{(n)} & \cdots & C_1^{(n)} = C^{(n)} b_1^{(n)} & C_0^{(n)} = C^{(n)} b_0^{(n)} \\ r_{C_{t-1}} = R_C p_{t-1} & \cdots & r_{C_1} = R_C p_1 & r_{C_0} = R_C p_0 \end{array}$$

Шаг 3: Вычислить:

$$\zeta_{t-1} = \left| -r_{C_{t-1}} + \sum_{i=1}^{n} C^{(i)} b_{t-1}^{(i)} \right|_{m^{(n+1)}},$$
$$\vdots$$
$$\zeta_1 = \left| -r_{C_1} + \sum_{i=1}^{n} C^{(i)} b_1^{(i)} \right|_{m^{(n+1)}},$$
$$\zeta_0 = \left| -r_{C_0} + \sum_{i=1}^{n} C^{(i)} b_0^{(i)} \right|_{m^{(n+1)}}.$$

Шаг 4: Вычислить:

$$\zeta_{t-1}^{*} = |\zeta_{t-1}2^{t-1}|_{m^{(n+1)}}, \ldots, \zeta_1^{*} = |\zeta_1 2^1|_{m^{(n+1)}}, \ \zeta_0^{*} = \zeta_0.$$

Шаг 5: Вычислить: $C^{(n+1)} = |\sum_{i=0}^{t-1} \zeta_i^{*}|_{m^{(n+1)}}$.

Структура алгоритма 1 поясняется с помощью рис. 2.

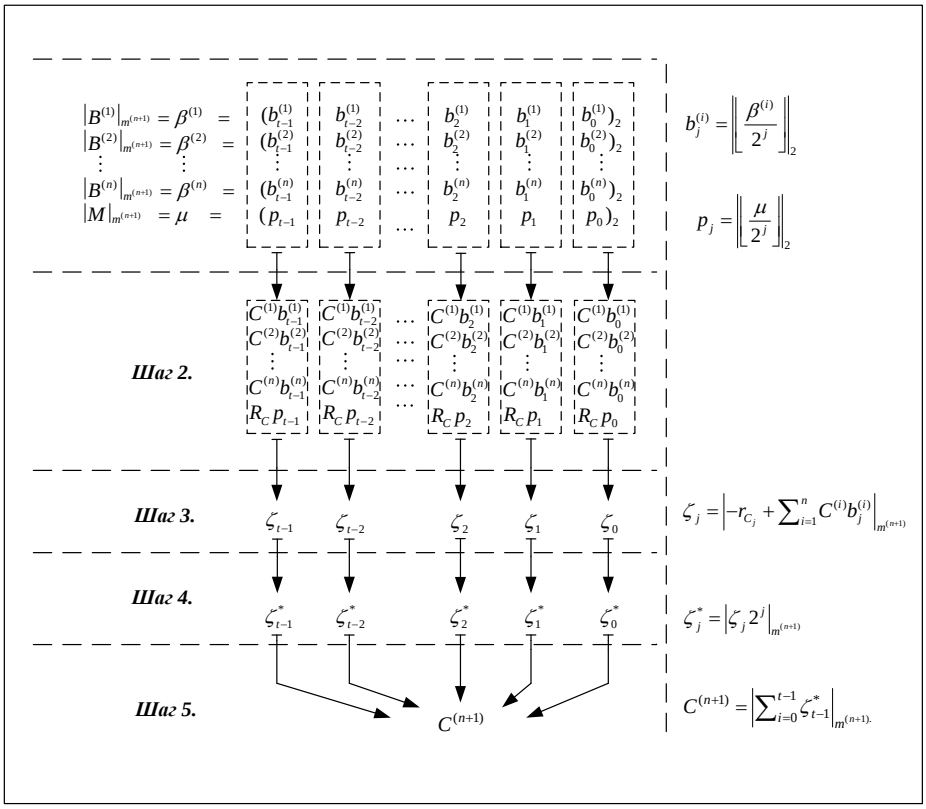

Рис. 2. Пояснения к алгоритму расширения МК

Так как КС способна обнаруживать и исправлять ошибки, возникает необходимость в оценке достоверности передачи данных. Для этого выполним расчет достоверности для КС, основанной на расширенном МК и КС-прототипа, использующей линейные коды при передаче по каналу связи.

Численно достоверность передачи данных будем характеризовать вероятностью необнаруживаемой ошибки в криптограммах на приемной стороне.

Мерой избыточности КС будем считать относительное число лишних битов в передаваемом множестве криптограмм:

$$r_i = 1 - \frac{n}{l} = \frac{l-n}{l},$$

где n – количество информационных криптограмм, $l = n + r$ – общее количество криптограмм.

Будем предполагать, что ошибки кратности q в передаваемой последовательности криптограмм $C^{(1)}, \ldots, C^{(n)}, \ldots, C^{(n+r)}$ происходят независимо друг от друга и их распределение подчиняется биномиальному закону. Пусть p – вероятность

ошибочного приема криптограммы $C^{(i)}$ (вероятность правильного приема $1-p$). Правильный прием открытого текста M возможен только в том случае, если вся последовательность криптограмм $C^{(1)}, C^{(2)}, \dots, C^{(n)}$, поступившая из канала связи, не подверглась искажениям.

Согласно теореме о совместимых и независимых событиях вероятность правильного приема последовательности криптограмм $C^{(1)}, C^{(2)}, \dots, C^{(n)}$ равна $(1-p)^n$. Вероятность ошибочного приема последовательности криптограмм $C^{(1)}, C^{(2)}, \dots, C^{(n)}$ равна

$$P(q) = 1 - (1-p)^n.$$

Применяя формулу бинома Ньютона, получим

$$1 - (1-p)^n = P(q) = \binom{n}{1}(1-p)^{n-1} + \\ + \binom{n}{2}p^2(1-p)^{n-2} + \binom{n}{3}p^3(1-p)^{n-3} + \dots \\ \dots + \binom{n}{q}p^q(1-p)^{n-q}.$$

Получаем, что первый член разложения равен вероятности p_1 однократной ошибки в последовательности криптограмм $C^{(1)}, C^{(2)}, \dots, C^{(n)}$, второй член – вероятности p_2 двукратной ошибки в последовательности криптограмм $C^{(1)}, C^{(2)}, \dots, C^{(n)}$, третий член – вероятности p_3 трехкратной ошибки в последовательности криптограмм $C^{(1)}, C^{(2)}, \dots, C^{(n)}$ и q-й – вероятность p_q ошибки кратностью q.

Таким образом:

$$P(q) = p_1 + p_2 + p_3 + \dots + p_q + \dots + p_n = \sum_{q=1}^{n}\binom{n}{q}p^q(1-p)^{n-q}. \quad (6)$$

Полученный ряд вероятностей (6) есть биномиальный закон распределения [13].

Для того чтобы оценить степень деструктивных воздействий на передаваемую последовательность криптограмм $C^{(1)}, \dots, C^{(n)}, \dots, C^{(n+r)}$, необходимо знать величину p вероятности ошибочного приема криптограммы $C^{(i)}$. Вероятность p ошибочного приема криптограммы $C^{(i)}$ является величиной постоянной и вычисляется, если известна закономерность возникновения искажений, вызванных помехой и(или) действиями криптоаналитика.

Воздействия криптоаналитика на криптограмму $C^{(i)}$ носят аналитический характер, поэтому последствия таких воздействий являются *непредсказуемыми и носят случайный характер* [14, 15]. Такое влияние криптоаналитика указывает на то, что искажения произойдут или нет. Примем в качестве гипотезы следующие допущение: искажения, вызванные воздействиями криптоаналитика на криптограмму $C^{(i)}$, носят равновероятный характер, а искажения, вызванные помехами в криптограмме $C^{(i)}$, независимы и подчиняются биномиальному распределению.

Пусть p_{noise} – вероятность искажения бита криптограммы $C^{(i)}$, вызванного помехами, а p_{cr} – вероятность искажения бита криптограммы $C^{(i)}$, вызванного действиями криптоаналитика. На основании принятых допущений, а также с учетом $d_{\min}$, определим для КС-прототипа вероятность искажения криптограммы $C^{(i)}$, вызванной действиями криптоаналитика:

$$p = \frac{p_{cr}\sum_{t=i+1}^{h}\binom{h}{t}}{2^n},$$

где $\sum_{t=i+1}^{h}\binom{h}{t}$ – общее количество искажений в криптограмме $C^{(i)}$, не обнаруживаемых данным методом контроля; $i+1 \le t < h$ – кратность ошибок, которые не будут обнаружены данным методом контроля; h – длина блока криптограммы; 2^h – общее количество возможных искажений; вероятность искажения криптограммы $C^{(i)}$, вызванной помехами:

$$p_{noise_1} = 1 - \sum_{t=0}^{d_{\min}-1}\binom{h}{t} p_{noise}^{t}\,(1-p_{noise})^{h-t}.$$

Для многоканальной КС вероятность искажения криптограммы $C^{(i)}$, вызванной действиями криптоаналитика, равна

$$p_{cr_2} = \frac{p_{cr}\binom{h}{1} + \binom{h}{2} + \ \ldots + \binom{h}{t}}{2^h} = \frac{p_{cr}\,2^h}{2^h} = p_{cr},$$

вероятность искажения криптограммы $C^{(i)}$, вызванной помехами:

$$p_{noise_2} = \sum_{t=i+1}^{h}\binom{h}{t} p_{noise}^{t}\,(1-p_{noise})^{h-t},$$

что обусловлено способностью КС обнаруживать (исправлять) ошибки любой кратности (в метрике ЛДК) в криптограмме $C^{(i)}$.

Вероятность появления искажений, вызванных помехами в криптограмме $C^{(i)}$, не зависит от результата воздействия на криптограмму $C^{(i)}$ криптоаналитика. А вероятность появления искажений в криптограмме $C^{(i)}$, вызванных криптоаналитиком, не исключает появления искажений, вызванных помехами. Причем вносимые помехой и криптоаналитиком искажения в криптограмму $C^{(i)}$ являются совместными и независимыми событиями. Тогда в соответствии с [16] искомая вероятность ошибочного приема криптограммы $C^{(i)}$ (при одновременном воздействии криптоаналитика и помех), вызванная или помехами, или криптоаналитиком, примет вид:

а) для КС-прототипа;

$$p_1 = p_{cr_1} + p_{noise_1} - p_{cr_1}p_{noise_1}, \tag{7}$$

б) для многоканальной КС:

$$p_2 = p_{cr_2} + p_{noise_2} - p_{cr_2}p_{noise_2}. \tag{8}$$

Таким образом, подставив выражения (7) и (8) в (6), окончательно получим итоговые выражения для оценки достоверности передачи данных:

а) для КС-прототипа:

$$P_{er_1} = \sum_{q=1}^{n}\binom{n}{q} p_1^{q}(1-p_1)^{n-q}, \tag{9}$$

б) для многоканальной КС:

$$P_{er_2} = 1 - \sum_{q=0}^{d_{\min}-1}\binom{l}{q} p_2^{q}(1-p_2)^{l-q}. \tag{10}$$

Полученные соотношения дают возможность определить вероятности необнаруживаемых ошибок P_{er_1} и P_{er_2} в зависимости от различных параметров КС и канала связи.

Поставим исследуемые КС в равные условия по вводимой избыточности, как основного показателя корректирующей способности. Определим необходимое количество избыточных битов для КС-прототипа. Для этого общее количество битов избыточных криптограмм $C^{(i)}$ многоканальной КС разделим на количество информационных криптограмм $C^{(i)}$. Полученные избыточные биты добавим к информационным битам криптограмм $C^{(i)}$ КС-прототипа. Таким образом, получаем равные КС по корректирующей способности.

Выполним расчет P_{er_1} и P_{er_2} для КС-прототипа и многоканальной КС по формулам (9) и (10). Полученные зависимости аппроксимируем и изобразим графически. В качестве аппроксимирующей функции используем полином третьей степени.

На рис. 3 представлены расчетные данные зависимости вероятностей необнаруживаемой ошибки от коэффициента избыточности с параметрами КС $p_{noise} = 4.2 \times 10^{-5}$, $l = 12$, $h = 11$.

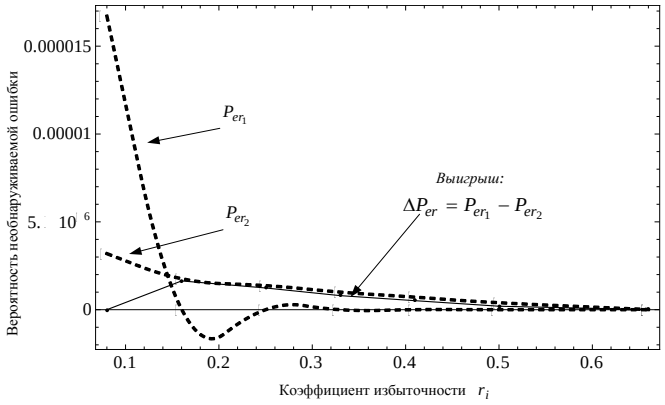

Рис. 3. Зависимость вероятности необнаруживаемой ошибки от коэффициента избыточности r_i

Значение вероятности ошибки в бите криптограммы $C^{(i)}$, вызванной криптоаналитиком, соответствует $p_{cr} = 1.5 \times 10^{-7}$. Также получены и представлены расчетные значения выигрыша ΔP_{er}, т.е. преимущества сравниваемых КС. На рис. 4 представлены расчетные зависимости вероятностей необнаруживаемых ошибок от вероятности ошибки, вызванной криптоаналитиком, с параметрами КС $p_{noise} = 4.2 \times 10^{-5}$, $d_{\min} = 2$, $l = 12$.

Таким образом, предложен метод объединения процедур кодирования и шифрования для защиты данных от воздействия искажений различного происхождения при передаче их по общедоступным каналам связи. Как видно из представленных зависимостей, исследуемая КС является более эффективной с точки зрения повышения достоверности передачи данных по сравнению с традиционным (раздельным) использованием помехо- и криптозащиты, в которых шифрование и кодирование выполняются независимо, с использованием разных алгоритмических методов.

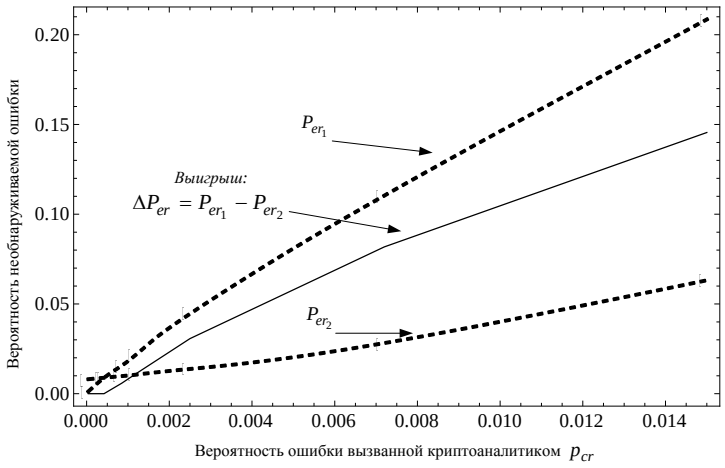

Рис. 4. Зависимость вероятности необнаруживаемой ошибки от вероятности ошибки p_{cr}

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Godoy W., Periera D.* A proposal of a cryptography algorithm with techniques of error correction // Computer Communications. – 1997. – № 20 (15). – P. 1374-1380.
2. *Самохина М.А*. Модификации криптосистемы Нидеррайтера, их стойкость и практические применения // Тр. МФТИ. – М., 2009. – Т. 1, № 2.– С. 121-127.
3. *Финько О.А.* Групповой контроль ассиметричных криптосистем методами модулярной арифметики // Материалы XIV Международной школы-семинара «Синтез и сложность управляющих систем» / Нижегород. пед. ун-т. – Н. Новгород, 2003. – С. 85-86.
4. *Финько О.А.* Многоканальные модулярные системы, устойчивые к искажениям криптограмм // Материалы Международной научной конференции «50 лет модулярной арифметике». – М.: «Ангстрем», МИЭТ, 2006. – С. 552–558. URL: http://www.computer-museum.ru/books/arc-hiv/sokcon18.pdf
5. *Финько О.А., Самойленко Д.В.* Конструкции, контролирующие ошибки, на основе действующих криптографических стандартов // Материалы VIII Международной конференция «Дискретные модели в теории управляющих систем». – М., 2009. – С. 318-320.
6. *Финько О.А.* Многоканальные системы, устойчивые к искажению криптограмм // Криптографические методы защиты информации: Монография / Под ред. Е.А. Сухарева. Кн. 4. – М.: Радиотехника, 2007. – С. 91-96.
7. *Самойленко Д.В., Финько О.А.* Оценка помехоустойчивости криптосистемы, основанной на Китайской теореме об остатках, для N каналов с шумом и имитирующим злоумышленником // Материалы XI Международной конференции «Информационная безопасность». Ч. 3. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 154–159.
8. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. – М.: Мир, 1989. – 448 с.
9. *Амербаев В.М.* Теоретические основы машинной арифметики. – Алма-Ата: Наука, 1976. – 324 с.
10. *Торгашев В.А.* Система остаточных классов и надежность ЦВМ. – М.: Сов. радио, 1973. – 120 с
11. *Самойленко Д.В., Финько О.А.* Алгоритм расширения системы больших оснований модулярной арифметики // Материалы XI Международной конференции «Информационная безопасность». Ч. 3. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 151–154.
12. *Shinichi Kawamura, Masanobu Koike, Fumihiko Sano, Atsushi Shimbo*. Cox-Rower architecture for fast parallel Montgomery multiplication, Proceedings of the 19th international conference on Theory and application of cryptographic techniques, May 14-18, 2000, Bruges, Belgium.
13. *Зелигер Н.Б.* Основы передачи данных. – М.: Связь, 1974. – 200 с.
14. *Бабаш А.В., Шанкин Г.П.* Криптография. – М.: Солон-Р, 2002. – 512 с.

15. *Алферов А.П., Зубов А.Ю.* Основы криптографии: Учеб. пособие. – 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002. – 480 с.
16. *Мостеллер Ф., Рурке Р.* Вероятность. – М.: Мир, 1969. – 435 с.

Самойленко Дмитрий Владимирович
Краснодарское высшее военное училище (ВИ).
E-mail: sam-0019@yandex.ru.
350035, г. Краснодар, ул. Красина, 4.
Тел.: +79183624109.

Финько Олег Анатольевич
Кубанский государственный технологический университет.
Институт информационных технологий и безопасности.
E-mail: ofinko@yandex.ru.
350072, г. Краснодар, ул. Московская, 2.
Тел.: +79615874848.

Samoylenko Dmitry Vladimirovich
Krasnodar higher military school (MI).
E-mail: sam-0019@yandex.ru.
4, Krasina, Krasnodar, 350035, Russia.
Phone: +79183624109.

Finko Oleg Anatol'evich
Kuban state technological university.
Institute of information technologies and safety.
E-mail: ofinko@yandex.ru.
2, Moscow, Krasnodar, 350072, Russia.
Phone: +79615874848.

УДК 519.7

А.К. Вишневский, В.А. Шарай

РЕАЛИЗАЦИЯ ОПЕРАЦИИ ПОДСТАНОВКИ ЛИНЕЙНЫМИ ЧИСЛОВЫМИ ПОЛИНОМАМИ

Исследована возможность представления операции подстановки степени $k = 2^{\log k}$ *двумя линейными числовыми полиномами на примере первой подстановки криптоалгоритма ГОСТ 28.147-89.*

Линейный числовой полином; криптоалгоритм; криптография; подстановка; числовая нормальная форма; полином Жегалкина; алгебраическая нормальная форма; булева функция; булева формула.

A.K. Vishnevsky, V.A. Sharai

REALIZATION OF OPERATION OF SUBSTITUTION BY THE LINEAR NUMERICAL POLYNOMS

Possibility of representation by two linear numerical polynoms of operation of substitution of degree $k = 2^{\log k}$ *is investigated on example of the first substitution of crypto algorithm GOST 28.147-89.*

Linear numerical polynom; cryptoalgorithm; cryptography; substitution; a numerical normal form; polynom of Gegalkin, an algebraic normal form; boollean function; boollean formula.