JOURNAL OF BAKU ENGINEERING UNIVERSITY- MATHEMATICS AND COMPUTER SCIENCE
2017. Volume 1, Number 1 *Pages 3-13*

УДК 004.056.5

КОНТРОЛЬ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ НА ОСНОВЕ ФАКТОРИАЛЬНОЙ СИСТЕМЫ СЧИСЛЕНИЯ

Э.В. ФАУРЕ, В.В. ШВЫДКИЙ, А.И. ЩЕРБА

Черкасский государственный технологический университет

Черкассы / УКРАИНА

faureemil@gmail.com

РЕЗЮМЕ

В работе предложен метод контроля целостности информации, обеспечивающий защиту от навязывания ложных данных, обнаружение ошибок в канале связи и защиту информации от несанкционированного чтения. В соответствии с этим методом проверочная часть блока данных представляется в виде перестановки, формируемой по секретному ключу из символов сообщения, преобразованных в последовательность взаимосвязанных чисел в факториальной системе счисления. Для предложенного метода оценен энергетический выигрыш при передаче сообщения по каналу связи, выполнено его сравнение с соответствующей оценкой циклического избыточного кода.

Ключевые слова: обнаружение модификации, повышение достоверности, помехоустойчивых код, избыточность, перестановка, факториальное число.

INFORMATION INTEGRITY CONTROL BASED ON THE FACTORIAL NUMBER SYSTEM

ABSTRACT

It is proposed a method for information integrity control that provides protection against intentional alteration of data, communication channel error detection, and data protection from unauthorized access. In accordance with this method, a data block check sum is a permutation formed by a secret key from a sequence of message symbols converted into a sequence of interrelated numbers in factorial notation. An estimation of coding gain of the proposed method for information integrity control is made and compared with the corresponding estimation of cyclic redundancy codes.

Keywords: detection of modifications, increasing of reliability, error-detecting code, redundancy, permutation, factorial number.

1. Введение

Рост объемов передачи конфиденциальной информации в сферах обороны, дистанционного управления финансовыми операциями и электронного документооборота приводит к необходимости повышения эффективности контроля целостности информации (КЦИ), который предусматривает защиту от навязывания ложных данных и обнаружение ошибок, вносимых каналом связи в процессе передачи сообщения.

Известны способы криптографической защиты информации от несанкционированного чтения и модификации [1, 2] и способы обнаружения ошибок в канале связи [3-5], каждый из которых решает одну из перечисленных задач КЦИ. Вместе с тем известны способы КЦИ, обеспечивающие обнаружение модификации данных как в результате действий злоумышленника, так и помех в канале связи [6-8]. Эти способы требуют повышенной избыточности, что приводит к потерям пропускной способности. Поэтому представляет значительный интерес исследование новых методов КЦИ, в частности, на основе факториальной системы счисления (ФСС) [9, 10].

В соответствии с [10], контрольная сумма представляется в виде перестановки (упорядоченного набора) чисел $\{0;1;...;M-1\}$, где M-порядок перестановки. При этом контрольной сумме соответствует точка отрезка $[0;M!-1]$, определяющая номер перестановки, который в ФСС имеет вид: $B=\sum_{i=0}^{M-1} b_{M-1-i}\cdot(M-1-i)!$, где $0\le b_{M-1-i}\le M-1-i$.

Формирование перестановки π производится в соответствии с базовой перестановкой $\pi(0)$ и синдромом перестановки $S_F = \{b_{M-1}; b_{M-2}; ...; b_0\}$, полученным из факториальной записи числа B. Базовая перестановка может быть открытой, в частности, тривиальной: $\pi(0) = \{0; 1; ...; M-1\}$, или скрытой – нетривиальной и хранящейся в тайне.

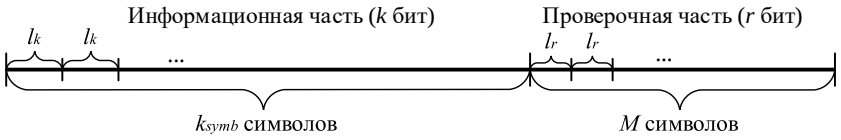
Целью работы является разработка метода КЦИ на основе факториальной системы счисления и оценка эффективности его способности обнаруживать ошибки в канале связи.

2. Структура блока данных

Настоящее исследование широко использует основные положения теории передачи дискретных сообщений [11] и направлено на ее дальнейшее развитие.

Примем, что КЦИ используется в простейшей системе передачи данных с решающей обратной связью (РОС), где прямой канал – двоичный симметричный, обратный канал – идеальный (ошибки в нем отсутствуют), а символы, составляющие сообщение, являются элементами поля $F_2 = \{0; 1\}$. Пусть k и r – число двоичных символов в информационной и проверочной частях блока соответственно, $n = k + r$ – полная длина блока. Структура блока данных системы КЦИ на основе ФСС показана на рис. 1.

Рис. 1. Структура блока данных



Информационная часть содержит k_{symb} укрупненных символов, каждый из которых образуется группой из l_k бит и соответствует элементу поля $F_{2^{l_k}}$. Длина информационной части $k = l_k \cdot k_{symb}$ бит. Примем, что символы перестановки кодируются равномерным двоичным кодом с длиной кодовой комбинации $l_r = \text{entier}(\log_2 M) + 1$ бит, где $\text{entier}(a)$ определяет наибольшее целое, меньшее, чем a. Поэтому проверочная часть содержит $r = l_r \cdot M$ бит. Значение M выбирается исходя из требований по степени повышения достоверности. Его влияние на энергетический выигрыш в результате применения системы КЦИ приводится ниже.

3. Оценка достоверности передачи данных

3.1. Оценка достоверности передачи при использовании КЦИ на основе ФСС

Далее используем широко принятый [5, с. 232; 12, с. 601] подход к рассмотрению наборов (векторов) над полем F_2 в виде элементов алгебры многочленов с коэффициентами из F_2. Так, блок данных $C(x)$, состоящий из информационной $A(x)$ и проверочной $R(x)$ частей, выводится в канал в виде $C(x) = A(x) \text{C } R(x)$, где C -символ конкатенации (присоединения), т.е. $C(x) = x^r \cdot A(x) + R(x)$. При передаче по каналу на блок данных воздействует вектор ошибки $\varepsilon_n(x) = \varepsilon_k(x) \text{C } \varepsilon_r(x)$ с мощностью множества векторов $\mu\{\varepsilon_n(x)\} = 2^n$, где $\varepsilon_k(x)$ и $\varepsilon_r(x)$-вектора ошибки, воздействующие на информационную и проверочную части блока. Тогда принятый из канала связи вектор $D(x) = C(x) \oplus \varepsilon_n(x) = (A(x) \oplus \varepsilon_k(x)) \text{C } (R(x) \oplus \varepsilon_r(x))$.

В приемнике по последовательности $A(x)\oplus\varepsilon_k(x)$ вычисляется контрольная сумма, которую можно представить в виде $R(x)\oplus\varepsilon_r^{\wedge}(x)$, где $\varepsilon_r^{\wedge}(x)$ – ошибка, возникающая на выходе блока формирования перестановки. Вектор разности $\varepsilon_r^{\wedge}(x)$ преобразует перестановку $R(x)$ в перестановку и статистически не связан с $\varepsilon_r(x)$. Синдром ошибки $S(x)=\left(R(x)\oplus\varepsilon_r^{\wedge}(x)\right)\oplus\left(R(x)\oplus\varepsilon_r(x)\right)=\varepsilon_r^{\wedge}(x)\oplus\varepsilon_r(x)$. Если $\varepsilon_n(x)=0$, то $S(x)=0$, что является признаком немодифицированных данных. Если $\varepsilon_n(x)\neq 0$ и $S(x)=0$, то ошибка $\varepsilon_n(x)$ не обнаруживается декодером, что при $\varepsilon_k(x)\neq 0$ и $\varepsilon_r(x)=0$ является следствием коллизий.

Вероятность необнаруженной ошибки в результате применения КЦИ на основе ФСС (факториального кода – *FC*) $P_{ud}(FC,p_0)=P\left\{\varepsilon_r^{\wedge}(x)=\varepsilon_r(x)\right\}$ зависит от способа формирования контрольной суммы. Согласно [10], контрольная сумма вычисляется с помощью процедуры $S_F(j)=f\left(S_F(j-1)\right)*s(j)$, где $S_F(j)$ – синдром перестановки после обработки *j*-го укрупненного символа информационной части $s(j)\in F_2^{l_k}$, $j\le k_{symb}$; $S_F(0)$ – вектор начальной загрузки; $f\left(S_F(j-1)\right)$ – функция модификации синдрома; символ $*$ обозначает сложение чисел различных систем счисления по [9]. Выбор функции $f\left(S_F(j-1)\right)$ представляет собой важный этап проектирования системы КЦИ, однако выходит за рамки рассмотрения этой работы. Далее примем, что данные на входе и выходе блока формирования перестановки статистически независимы, а закон распределения ошибок $\varepsilon_r^{\wedge}(x)$ при $\varepsilon_k(x)\neq 0$ – равномерный.

Оценим вероятность необнаруженной ошибки $P_{ud}(FC,p_0)$ для двух случаев: $M!<2^k$ – отображение $f:\{A(x)\}\to\{R(x)\}$ сюръективно, что приводит к коллизиям; $M!\ge 2^k$ – отображение $f:\{A(x)\}\to\{R(x)\}$ инъективно или биективно, что исключает коллизии.

3.1.1. Оценка вероятности необнаруженной ошибки для факториального кода при $M!<2^k$

При $\varepsilon_k(x)\neq 0$ вероятность появления каждого из *M*! векторов $\varepsilon_r^{\wedge}(x)$, включая нулевой,

$$p_r^{\wedge}=\left(1-q_0^k\right)/M!. \tag{1}$$

Пусть p_r – вероятность появления ошибки $\varepsilon_r(x)$ (включая нулевую), способной преобразовать перестановку $R(x)$ в какую-либо из *M*! перестановок (т.е. разрешенную комбинацию проверочной части в разрешенную). Тогда по теореме умножения вероятностей для вероятности необнаруженной ошибки факториальным кодом имеем:

$$P_{ud}(FC,p_0)=p_r^{\wedge}\cdot p_r. \tag{2}$$

Ошибка $\varepsilon_r(x)$ распределена по биномиальному закону: вероятность появления вектора с весом Хэмминга $i\in[0;r]$ равна

$$p_r(i)=C_r^i p_0^i q_0^{r-i}. \tag{3}$$

Пусть случайное событие *A*={ошибка $\varepsilon_r(x)$ преобразует перестановку $R(x)$ в перестановку}, $P(A)=p_r$; случайное событие B_i ={появление ошибки $\varepsilon_r(x)$ веса *i*}, $P(B_i)=p_r(i)$; $f_{per}(i)$ – количество ошибок веса $i\in[0;r]$, порождающих событие *A*. Тогда $P(A|B_i)=f_{per}(i)/C_r^i$ указывает вероятность преобразования перестановки в перестановку при появлении ошибки веса *i*. Из формулы полной вероятности и (3),

$$p_r=P(A)=\sum_{i=0}^{r}p_r(i)\cdot f_{per}(i)/C_r^i=\sum_{i=0}^{r}f_{per}(i)p_0^i q_0^{r-i}. \tag{4}$$

Теорема 1. Вероятность p_r появления ошибки $\varepsilon_r(x)$, способной преобразовать разрешенную комбинацию проверочной части факториального кода в разрешенную комбинацию (включая саму в себя), определяется выражением

$$p_r=\sum_{i=0}^{\text{entier}(r/2)}f_{per}(2i)p_0^{2i}q_0^{r-2i}, \tag{5}$$

где $\sum_{i=0}^{\text{entier}(r/2)}f_{per}(2i)=M!$ и

$$f_{per}(0)=1;\ f_{per}(2)\le l_r\cdot M/2;\ f_{per}(4)\le l_r\cdot M\cdot\left(l_r\cdot(M+8)-10\right)/8. \tag{6}$$

Доказательство. Вначале покажем, что вес ошибок $\varepsilon_r(x)$, переводящих перестановку в перестановку, четен. Не ограничивая общности рассмотрения, примем перестановку $\pi(0)=\{0;1;...;M-1\}$ в качестве исходной. Представим символы перестановки в двоичном коде и запишем их последовательно, как показано на рис. 2.

Рис. 2. Символы проверочной части

$\pi(0)=\{0$	;	1	;	2	;	3	;	…	;	M-1$\}$	$\sum$(mod 2)
↓		↓		↓		↓				↓	
0		1		0		1		...		1	$=w_0$
0		0		1		1		...		1	$=w_1$
0		0		0		0		...		1	$=w_2$
⋮		⋮		⋮		⋮				⋮	⋮
0		0		0		0		...		1	$=w_{lr-1}$

Значение $w_j\in\{0;1\}$, равное сумме по mod 2 бит *j*-ой строки, $j\in[0,l_r-1]$, инвариантно по отношению к перестановке символов. Это означает, что помеха в каждой строке и, следовательно, $\varepsilon_r(x)$ имеют четный вес. Поэтому $f_{per}(2i+1)=0$, а $p_r=\sum_{i=0}^{\text{entier}(r/2)}f_{per}(2i)p_0^{2i}q_0^{r-2i}$.

При $M!<2^k$ мощность множества разрешенных комбинаций проверочной части $\mu(R(x))=M!$, поэтому $\sum_{i=0}^{\text{entier}(r/2)}f_{per}(2i)=M!$. Ошибка нулевого веса переводит перестановку саму в себя: $f_{per}(0)=1$. Ошибка веса 2 преобразует перестановку в перестановку, если она порождает транспозицию. При $M=2^{l_r}$ количество таких ошибок $f_{per}(2)=l_r\cdot M/2$. При $2^{l_r-1}<M<2^{l_r}$ имеем: $f_{per}(2)<l_r\cdot M/2$. Ошибка веса 4 может преобразовать перес-

тановку в перестановку, если она поражает 2, 3 или 4 укрупненных символа. Поочередно определяя вероятности этих событий, несложно видеть, что $f_{per}(4) \le l_r \cdot M \cdot \left(l_r \cdot (M+8) - 10\right)/8$.

Пример. *Для* $M = 8$ $f_{per}(2)/C_{24}^2 \approx 0{,}043$ и $f_{per}(4)/C_{24}^4 \approx 0{,}011$, что подтверждает эффективность применения оценок (6).

Замечание 1. При $\log_2 M \in \not\subset$ справедливо равенство $f_{per}(i) = f_{per}(r-i)$.

Выполним оценку сверху вероятности p_r. *Для* этого введем следующее определение.

Определение 1. Вероятность появления ошибки $\varepsilon_r(x)$, преобразующей перестановку чисел $\{0;1;2;\text{K};M-1\}$ в другую перестановку или саму в себя, равна сумме:

$$p_r = \sum_{i=0}^{m_1} f_{per}(2i)\, p_0^{2i} q_0^{r-2i} + \Delta_{per}(m_1), \tag{7}$$

$$\Delta_{per}(m_1) = \sum_{i=m_1+1}^{\text{entier}(r/2)} f_{per}(2i)\, p_0^{2i} q_0^{r-2i}, \quad 0 \le m_1 \le \text{entier}(r/2) - 1. \tag{8}$$

Теорема 2. *Для* вероятности $\Delta_{per}(m_1)$ имеет место следующая оценка:

$$\Delta_{per}(m_1) \le \sum_{i=m_1+1}^{m_2} p_r(2i) + \left(z/C_r^{2(m_2+1)}\right) p_r\left(2(m_2+1)\right), \tag{9}$$

где $z = M! - \sum_{i=0}^{m_1} f_{per}(2i) - \sum_{i=m_1+1}^{m_2} C_r^{2i}$, число $m_2 \in ¥ : \sum_{i=m_1+1}^{m_2} C_r^{2i} \le M! - \sum_{i=0}^{m_1} f_{per}(2i) < \sum_{i=m_1+1}^{m_2+1} C_r^{2i}$, а $p_r(i)$ вычисляется по (3).

Доказательство. В правой части (8) проведем последовательно группировку слагаемых вида $p_0^j q_0^{r-j}$ по C_r^i штук $\left(i = 2(m_1+1), 2(m_1+2), \text{K}\right)$. Учитывая, что $\sum f_{per}(2i) = M!$, $f_{per}(i) \le C_r^i$ и $p_0^i q_0^{r-i} > p_0^j q_0^{r-j}$ при $i < j$, получим:

$$\Delta_{per}(m_1) \le \underbrace{p_0^{2(m_1+1)} q_0^{r-2(m_1+1)} + \text{K} + p_0^{2(m_1+1)} q_0^{r-2(m_1+1)}}_{C_r^{2(m_1+1)}\ \text{слагаемых}} + \underbrace{p_0^{2(m_1+2)} q_0^{r-2(m_1+2)} + \text{K} + p_0^{2(m_1+2)} q_0^{r-2(m_1+2)}}_{C_r^{2(m_1+2)}\ \text{слагаемых}} + \text{K} +$$

$$+ \underbrace{p_0^{2m_2} q_0^{r-2m_2} + \text{K} + p_0^{2m_2} q_0^{r-2m_2}}_{C_r^{2m_2}\ \text{слагаемых}} + \underbrace{p_0^{2(m_2+1)} q_0^{r-2(m_2+1)} + \text{K} + p_0^{2(m_2+1)} q_0^{r-2(m_2+1)}}_{z\ \text{слагаемых}},$$ откуда следует (9).

Замечание 2. Так как $z < C_r^{2(m_2+1)}$, то $\Delta_{per}(m_1) \le \sum_{i=m_1+1}^{m_2+1} p_r(2i) \le \sum_{i=m_1+1}^{\text{entier}(r/2)} p_r(2i) \le \sum_{i=m_1+1}^{\infty} p_r(2i)$.

Следствие 1. В условиях применимости аппроксимационной формулы Пуассона *для* биномиального распределения при $\lambda = r \cdot p_0$ и $m_1 > (\lambda - 3)/2$ имеет место оценка:

$$\Delta_{per}(m_1) \le e^{-\lambda} \cdot \left(\lambda^{2(m_1+1)} / \left(2(m_1+1)\right)!\right) \cdot \left((2m_1+3)^2 / \left((2m_1+3)^2 - \lambda^2\right)\right). \tag{10}$$

Доказательство. Согласно замечанию 2 и аппроксимационной формулы Пуассона $p_r(i)$; $\left(\lambda^i / i!\right) e^{-\lambda}$, $\lambda = r \cdot p_0$, имеем: $\Delta_{per}(m_1) \le \sum_{i=m_1+1}^{\infty} p_r(2i)$; $e^{-\lambda} \cdot \left(\lambda^{2(m_1+1)} / \left(2(m_1+1)\right)!\right) \times$

$\times\left(1+\lambda^2/(2m_1+3)^2+\lambda^4/(2m_1+3)^4+\mathrm{K}\right)$. При $m_1>(\lambda-3)/2$ выполняется $\lambda^2/(2m_1+3)^2<1$. Вычисляя сумму бесконечной геометрической прогрессии, приходим к (10).

Замечание 3. Значение p_r вычисляется по (7), где $\Delta_{per}(m_1)$ оценивается по (9) или (10) и не превышает максимальной абсолютной погрешности вычислений ε.

Следствие 2. Ниже в табл. 1 для каждой пары значений $(m_1;p_0)$ и заданной точности ε указано максимальное значение M_0, для которого $\Delta_{per}(m_1)\le\varepsilon$ при всех $M\le M_0$.

Таблица 1. Диапазоны значений M в зависимости от $(m_1;p_0)$, при которых $\Delta_{per}(m_1)\le\varepsilon=10^{-3}$

m_1 \ p_0	10^{-3}	10^{-4}	10^{-5}
0	$M\le 11$	$M\le 65$	$M\le 508$
1	$M\le 64$	$M\le 487$	$M\le 3652$
2	$M\le 142$	$M\le 1036$	$M\le 8192$

Как следует из табл. 1, для оценки p_r по (7) при $\varepsilon=10^{-3}$ достаточно $m_1\le 2$.

3.1.2. Оценка вероятности необнаруженной ошибки для факториального кода при $M!\ge 2^k$

При $\varepsilon_k(x)\ne 0$ и отсутствии коллизий вероятность появления каждого из (2^k-1) ненулевых векторов ошибок $\varepsilon_r^{\wedge}(x)$ равна

$$p_r^{\wedge}=\left(1-q_0^k\right)/\left(2^k-1\right). \tag{11}$$

По аналогии с подходом при получении оценки (7) можно показать, что при $M!\ge 2^k$ вероятность p_r появления ошибки $\varepsilon_r(x)$ (не включая нулевую), способной преобразовать перестановку $R(x)$ в какую-либо из (2^k-1) других перестановок, ограничена сверху:

$$p_r\le\sum_{i=1}^{m_1}f_{per}(2i)p_0^{2i}q_0^{r-2i}+\Delta_{per}(m_1), \tag{12}$$

где $\Delta_{per}(m_1)$ оценивается по (9) или (10).

Выбор m_1 в (12) при вычислении p_r определяется относительной погрешностью $\delta_{per}(m_1)=\Delta_{per}(m_1)\Big/\sum_{i=1}^{m_1}f_{per}(2i)p_0^{2i}q_0^{r-2i}$, которая не должна превышать значения δ_{per}.

Следствие 3. Ниже в табл. 2 для каждой пары значений $(m_1;p_0)$ и заданной точности δ_{per} указано максимальное значение M_0, для которого $\delta_{per}'(m_1)\le\delta_{per}$ $\left(\delta_{per}'(m_1)=\Delta_{per}(m_1)/(l_r\cdot M/2)p_0^2q_0^{r-2}\right)$ при всех $M\le M_0$.

Таблица 2. Диапазоны значений M в зависимости от $(m_1;p_0)$, при которых $\delta_{per}'(m_1)\le\delta_{per}=10^{-2}$

m_1 \ p_0	10^{-3}	10^{-4}	10^{-5}
1	$M\le 12$	$M\le 38$	$M\le 132$
2	$M\le 54$	$M\le 255$	$M\le 1174$

3.2. Оценка вероятности необнаруженной ошибки для циклического избыточного кода

Ошибка $\varepsilon_n(x) \neq 0$ не обнаруживается кодом, если $\left|\varepsilon_n(x)\right|_{G_{r+1}(x)} = 0$, где $G_{r+1}(x)$ – кодовый полином степени *r*. Это условие выполняется, если $\varepsilon_n(x) = Q_{n-r}(x)G_{r+1}(x)$, где $Q_{n-r}(x) \neq 0$ – произвольный ненулевой полином степени, не большей *k*-1. Поэтому число не обнаруживаемых циклическим избыточным кодом (CRC) векторов ошибки $\mu\{Q_{n-r}(x) \neq 0\} = 2^{n-r} - 1$, а $\sum_{i=d_0}^{n} f_{CRC}(i) = 2^{n-r} - 1$, где $f_{CRC}(i)$ – число ошибок веса $i \in [0; n]$, не обнаруживаемых кодом (наиболее полно $f_{CRC}(i)$ представлены в [13]), d_0 – минимальное кодовое расстояние. Вероятность не обнаруженной CRC-кодом ошибки

$$P_{ud}(CRC, p_0) = \sum_{i=d_0}^{n} f_{CRC}(i) p_0^i q_0^{n-i} . \tag{13}$$

Используя тот же подход, что и при выводе оценки $P_{ud}(FC, p_0)$, с учетом оценки $f_{CRC}(i) \le C_n^{i-t} / C_i^t$ [11, с. 681], $t = \text{entier}\left((d_0 - 1)/2\right)$, можно показать, что

$$P_{ud}(CRC, p_0) = \sum_{i=d_0}^{d_1} f_{CRC}(i) p_0^i q_0^{n-i} + \Delta_{CRC}(d_1), \tag{14}$$

$$\Delta_{CRC}(d_1) \le \sum_{i=d_1+1}^{n} p_n(i) / C_{n-i+t}^t . \tag{15}$$

В условиях применимости аппроксимационной формулы Пуассона для биномиального распределения и $d_1 > \lambda(t+1) - 2$, где $\lambda = n \cdot p_0$, имеет место оценка

$$\Delta_{CRC}(d_1) \le \left(1 / C_{n+t-d_1-1}^t\right) \cdot e^{-\lambda} \cdot \left(\lambda^{d_1+1} / (d_1+1)!\right) \cdot \left((d_1+2) / (d_1+2-\lambda(t+1))\right). \tag{16}$$

Выбор d_1 в (14) при вычислении $P_{ud}(CRC, p_0)$ определяется относительной погрешностью $\delta_{CRC}(d_1) = \Delta_{CRC}(d_1) \Big/ \sum_{i=d_0}^{d_1} f_{CRC}(i) p_0^i q_0^{n-i}$, которая не должна превышать δ_{CRC}.

3.3. Характеристики системы передачи данных с РОС при использовании помехоустойчивого кодирования

3.3.1. Относительная скорость передачи

Согласно [11, с. 676], под относительной скоростью передачи ν_0 системы с РОС понимается отношение математического ожидания числа поступивших к получателю информационных символов к общему числу кодовых символов, поступивших в прямой канал. Поэтому $\nu_0 = B / C$, где *C* – пропускная способность канала данных (скорость передачи в канале без ошибок); *B* – фактическая скорость (скорость передачи в канале с ошибками). Представим ν_0 в виде $\nu_0 = \nu_1 \nu_2$, где $\nu_1 = k / n$ – скорость кода (статическая составляющая потери скорости); ν_2 – динамическая составляющая потери скорости вследствие переспросов.

В системах с РОС исправление ошибок достигается переспросом блоков. При превышении числа переспросов некоторого порога канал переводится в аварийное состояние.

Утверждение 1. Пусть $\nu_{2\min}$ – порог между состояниями нормы и аварии канала связи. Тогда при заданных p_0 и $\nu_{2\min}$ существует максимальное значение длины блока

$$n_{\max} \approx -\ln \nu_{2\min} / p_0 , \tag{17}$$

такое, что для $\forall n \le n_{\max}$ справедливо $\nu_2 \ge \nu_{2\min}$.

Доказательство. Согласно [11, с. 676], для простейшей системы с РОС $\nu_2 = Q + P_{ud}$, где $Q = (1-p_0)^n$ – вероятность приема блока данных без ошибок, P_{ud} – вероятность необнаруженной ошибки. Учтем, что выполнение неравенства $P_{ud} = Q$ является условием целесообразности применения помехоустойчивого кода. Тогда $\nu_2 \approx Q$. Поскольку $Q(p_0, n) = (1-p_0)^n$ монотонно убывает по n, при заданном p_0 $\exists n_{\max}: \nu_2 \ge \nu_{2\min}$ для $\forall n \le n_{\max}$. Решая неравенство $Q \ge \nu_{2\min}$, легко видеть, что $n_{\max} = \ln \nu_{2\min} / \ln(1-p_0)$. С учетом $p_0 = 1$, что имеет место в большинстве реальных каналов связи, $\ln(1-p_0) \approx -p_0$, откуда следует (17). ■

Следствие 4. Для каналов телефонной сети общего пользования с $p_0 = 10^{-3}$ при $\nu_{2\min} = 0.2 \div 0.3$ значение $n_{\max} \approx 1609 \div 1203$. Для каналов худшего качества (к примеру, радио-каналов ДВ, СВ, КВ) $n_{\max}$ уменьшается, а при уменьшении ν_1 уменьшается ν_0. Для каналов лучшего качества (микроволновых, спутниковых, оптических) $n_{\max}$ увеличивается, а $\nu_0 \to 1$.

3.3.2. Энергетический выигрыш

Вероятность битовой ошибки для некогерентного приемника определяется выражением $p = 0.5 \cdot e^{-0.5h^2}$ [14, с. 45], где h^2-соотношение сигнал/шум. Тогда энергетический выигрыш при применении помехоустойчивого кодирования

$$\Delta P = 10 \lg\left(\ln(2p_{0eq}) / \ln(2p_0)\right), \tag{18}$$

где $p_{0eq} \approx P_{ud} / \left(k(Q + P_{ud})\right)$ – эквивалентная вероятность битовой ошибки, определенная в [11, с. 677] как вероятность ошибки в гипотетическом симметричном постоянном двоичном канале, при которой вероятность безошибочного приема достаточно длинного сообщения такая же, как и в рассматриваемой системе. Далее энергетический выигрыш ΔP будем оценивать снизу, используя при вычислении формулы (18) оценку сверху для P_{ud}.

3.4. Оценка эффективности КЦИ на основе ФСС

1. Ниже в табл. 3 представлены примеры факториальных кодов для $n = 1400$ и их характеристики при $p_0 = 10^{-3}$ (где $k = n - r$ и $r = l_r \cdot M = \left(\text{entier}(\log_2 M) + 1\right) \cdot M$).

Таблица 3. Примеры факториальных кодов для $n = 1400$

n	k	M	ν_0	$P_{ud}(FC, p_0)$	ΔP
1400	1392	4	0,276	0,031	1,478
1400	1376	8	0,242	$1{,}811 \cdot 10^{-5}$	4,121
1400	1336	16	0,235	$3{,}305 \cdot 10^{-14}$	7,646

1400	1240	32	0,218	$2,302 \cdot 10^{-36}$	11,465
1400	1016	64	0,179	$3,429 \cdot 10^{-90}$	15,305
1400	504	128	0,089	$3,641 \cdot 10^{-156}$	17,653

2. Факториальный код обладает свойством криптостойкости и решает комплексную задачу выявления модификации данных вследствие действий злоумышленника и ошибок канала связи. Выполним все же его сравнение с систематическим двоичным CRC-кодом по критерию эффективности обнаружения ошибок канала связи. Графики зависимостей оценок ΔP от k в результате применения кодов при $p_0 = 10^{-3}$ представлены на рис. 3.

Рис. 3. Графики зависимостей оценок энергетического выигрыша от длины информационной части при $p_0 = 10^{-3}$ а) $r = 6$; б) $r = 8$; в) $r = 15$; г) $r = 24$

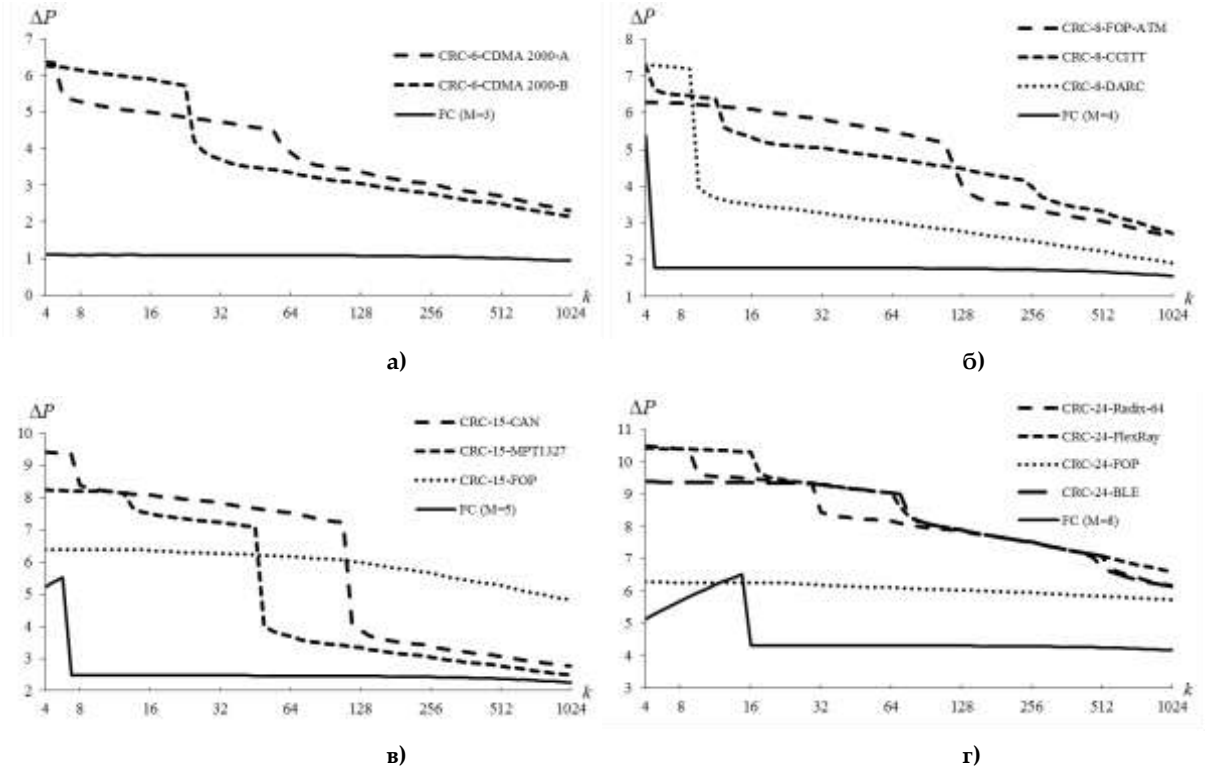
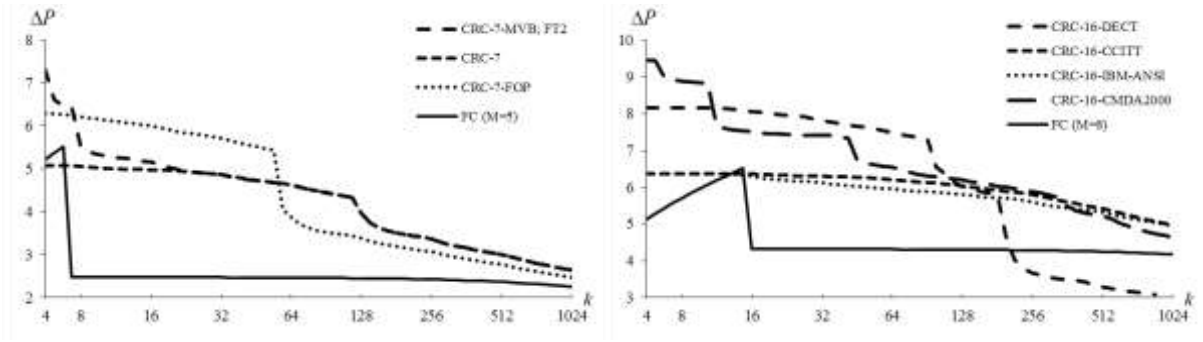


Рис. 3 показывает, что факториальный код уступает CRC-коду. Вместе с тем разность оценок их энергетических выигрышей $\Delta P_{отн} = \Delta P_{CRC} - \Delta P_{FC}$ уменьшается по мере увеличения длины информационной части k. Так, при $k = 1024$ и $p_0 = 10^{-3}$ $\Delta P_{отн} \le 1.336\,дБ$ для $r = 6$, $\Delta P_{отн} \le 1.121\,дБ$ для $r = 8$, $\Delta P_{отн} \le 1.889\,дБ$ для $r = 15$, $\Delta P_{отн} \le 1.920\,дБ$ для $r = 24$. Заметим, что оценку ΔP_{FC} можно выполнить более точно, если для $k > \log_2 M!$ определить значения $f_{per}(i)$, приводящие к коллизиям, а для $k \le \log_2 M!$ – значения $f_{per}(i)$, переводящие разрешенную комбинацию проверочной части в разрешенную (или хотя бы минимальное расстояние Хэмминга между ними). Улучшение оценки ΔP_{FC}, а также повышение эффективности обнаружения ошибок в канале связи факториальным кодом являются направлением дальнейших исследований.

3. Факториальный код самосинхронизирующийся и не требует наличия флага для цикловой синхронизации. Это свойство обусловлено тем, что символы $\{0;1;...;M-1\}$ встре-

чаются в перестановке ровно по одному разу, а их сумма равна $\sigma = 0,5M(M-1)$. Поэтому длину проверочной части факториального кода r_{FC} можно увеличивать на длину флага, сохраняя неизменными длину информационной части и общую длину кадра (с учетом флага). Для этого случая на рис. 4 представлены примеры зависимостей оценок ΔP от k в результате применения факториального кода и CRC-кода при $p_0 = 10^{-3}$ и размере флага в 8 бит.

Рис. 4. Графики зависимостей оценок энергетического выигрыша от длины информационной части при $p_0 = 10^{-3}$ и а) $r_{CRC} = 7$, $r_{FC} = 15$; б) $r_{CRC} = 16$, $r_{FC} = 24$



а) **б)**

Рис. 4 показывает, что увеличение длины проверочной части факториального кода за счет флага цикловой синхронизации позволяет повысить эффективность обнаружения ошибок и еще более приблизиться к энергетическому выигрышу CRC-кода (при $k = 1024$ и $p_0 = 10^{-3}$ $\Delta P_{отн} \le 0.384\,дБ$ для $r_{CRC} = 7$, $r_{FC} = 15$; $\Delta P_{отн} \le 0.811\,дБ$ для $r_{CRC} = 16$, $r_{FC} = 24$), а в некоторых случаях и превысить его (см., к примеру, CRC-16-DECT и FC (M=8), где $\Delta P_{отн} = -1.089\,дБ$).

4. Использование свойства самосинхронизации факториального кода исключает возможность совместной работы абонентов, у которых организация кадра соответствует изложенному выше способу, с абонентами, имеющими стандартную структуру и организацию кадра (содержащего маркер начала блока). Это обстоятельство создает возможность на предложенной основе организовать замкнутую группу (подсеть) абонентов в открытой сети.

4. Заключение

Построение системы КЦИ на основе факториальной системы счисления и использования в качестве контрольной суммы перестановки позволяет обеспечить комплексную защиту информации: защиту от навязывания ложных данных, обнаружение ошибок в канале связи и защиту информации от несанкционированного чтения. При этом полученный код самосинхронизирующийся, а его длина и скорость регулируются исходя из требований к стойкости системы и степени повышения достоверности передачи данных.

СПИСОК ЛИТЕРАТУРЫ

1. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб: Лань, 2001. – 224 с.
2. Schneier B. Applied cryptography: protocols, algorithms, and source code in C. – Wiley, 1996. – 758 p.
3. Morelos-Zaragoza R.H. The Art of Error Correcting Coding. – Wiley, 2006. – 278 p.

4. Berlekamp E.R. Algebraic coding theory. – McGraw-Hill, 1968. – 466 p.
5. Peterson W.W., Weldon E.J.. Error-correcting Codes. – MIT Press, 1972. – 560 p.
6. Пат. 75935 Україна, МПК H03M13/31 (2006.01). Спосіб забезпечення цілісності інформації на базі коду умовних лишків / Василенко В.С, Чунарьова А.В., Василенко М.Ю, Чунарьов А.В.; заявник та патентовласник Національний авіаційний університет. – №u2012103515; заявл. 26.03.2012; опубл. 25.12.2012, Бюл. №24. – 4 с.
7. Пат. 75938 Україна, МПК H03M13/31 (2006.01). Спосіб забезпечення цілісності інформації на базі лишково-хеммінгового коду / Василенко В.С, Чунарьова А.В., Василенко М.Ю, Чунарьов А.В.; заявник та патентовласник Національний авіаційний університет. – №u2012103518; заявл. 26.03.2012; опубл. 25.12. 2012, Бюл. №24. – 4 с.
8. Пат. 67988 Україна, МПК H03M13/31 (2006.01). Спосіб забезпечення цілісності інформації на базі завадостійкого коду умовних лишків / Василенко М.Ю, Василенко В.С, Чунарьов А.В.; заявник та патентовласник Національний авіаційний університет. – №u201110207; заявл. 19.08.2011; опубл. 12.03.2012, Бюл. №5. – 5 с.
9. Фауре Э.В., Швыдкий В.В., Щерба А.И. Метод формирования воспроизводимой непредсказуемой последовательности перестановок // Безпека інформації. – 2014. – №3. – Т.20. – С. 253-258.
10. Фауре Э.В., Швыдкий В.В., Щерба В.А. Метод формирования имитовставки на основе перестановок // Захист інформації. – 2014. – №4. – Т. 16. – С. 334-340.
11. Финк Л.М. Теория передачи дискретных сообщений. – Изд. 2-е. – М.: Советское радио, 1970. – 728 с.
12. Lidl R., Niederreiter H. Finite fields. – Cambridge: Cambridge University Press, 1985. – 407 p.
13. Koopman P. Best CRC Polynomials. – http://users.ece.cmu.edu/~koopman/crc/index.html.
14. Теплов Н.Л. Помехоустойчивость систем передачи дискретной информации. – М.: Связь, 1964. – 360 с.