УДК 004.056

Фауре Э. В.

Канд. техн. наук, доцент, докторант, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета, Черкассы, Украина

ФАКТОРИАЛЬНОЕ КОДИРОВАНИЕ С ИСПРАВЛЕНИЕМ ОШИБОК

Актуальность. Факториальное кодирование данных позволяет совмещать операции крипто- и имитозащиты, а также помехоустойчивого кодирования, что приводит к уменьшению вносимой передатчиком избыточности, повышению быстродействия и увеличению эффективной пропускной способности. Вместе с тем описанные методы факториального кодирования не позволяют исправлять ошибки, что ограничивает область их использования.

Целью данной работы является разработка метода факториального кодирования с восстановлением данных по перестановке, обеспечивающего комплексное решение задач криптографической защиты и помехоустойчивого кодирования и позволяющего совместить функции исправления и обнаружения ошибок канала связи.

Метод. Основная идея предложенного метода кодирования состоит в увеличении расстояния между разрешенными кодовыми словами, представляющими собой перестановки, вычисленные по всем информационным битам блока данных и представленные в двоичном виде. Исследованы методы увеличения расстояния на основе метрик Эвклида и Хэмминга. Для каждого из этих методов определены основные свойства факториального кода с исправлением ошибок, в том числе выполнена оценка достоверности передачи при независимости и биномиальном распределении возникающих в канале связи ошибок, разработаны структурные схемы приемника. Правила декодирования, реализованные в приемнике, основываются на критерии максимального правдоподобия и предусматривают как прямое исправление ошибок, так и их обнаружение с последующим исправлением путем переспроса поврежденного блока.

Результаты. Реализованы факториальные коды с исправлением ошибок, использующие метрики Эвклида и Хэмминга. Для этих кодов выполнен сравнительный анализ вероятности необнаруженной ошибки, остаточной вероятности ошибочного приема, энергетического выигрыша и относительной скорости передачи. Показано, что характеристики кода не являются инвариантными по отношению к множеству разрешенных кодовых слов, а из рассмотренных в работе кодов более эффективными являются коды, использующие метрику Хэмминга.

Выводы. Получил дальнейшее развитие метод факториального кодирования с восстановлением данных по перестановке, который за счет совмещения функций исправления и обнаружения ошибок позволяет повысить динамическую составляющую потери скорости и, как следствие, относительную скорость передачи, по сравнению с обнаруживающим ошибки факториальным кодированием за счет снижения его помехоустойчивости. Проведенные эксперименты подтвердили эффективность факториальных кодов с исправлением ошибок.

Ключевые слова: избыточность, факториальный код, перестановка, помехоустойчивое кодирование, исправление ошибок, обнаружение ошибок, достоверность передачи, относительная скорость передачи.

НОМЕНКЛАТУРА

FCDR – Factorial Code with Data Recovery by permutation;

FCDRec – FCDR with error correction;

РОС – решающая обратная связь;

СКК – сигнально-кодовая конструкция;

ФКВД – факториальный код с восстановлением данных по перестановке;

ФКВДио – факториальный код с восстановлением данных и исправлением ошибок;

ΔP – энергетический выигрыш при применении помехоустойчивого кода;

α – показатель избыточности кода (по мощности);

ν_2 – динамическая составляющая потери скорости;

$A(x)$ – представленное в двоичном виде информационное слово;

D_i – эвклидово расстояние от нуля до сигнальной точки i;

$D_{i,j}$ – эвклидово расстояние между сигнальными точками i и j;

$D_{\min}$ – минимальное эвклидово расстояние между сигнальными точками;

$d_{i,j}$ – расстояние Хэмминга между сигнальными точками i и j;

$d_{\min}$ – минимальное расстояние Хэмминга между кодовыми словами;

$f_{per}^{EC}(i,t)$ – количество ошибок веса t, исправляемых для i-ой сигнальной точки;

$f_{per}^{ud}(i,t)$ – количество ошибок веса t, приводящих к ошибочному декодированию i-ого сигнального вектора

k – число двоичных символов в информационном блоке данных;

l_r – число бит для кодирования одного символа перестановки;

M – порядок перестановки;

P_{det} – вероятность обнаруженной ошибки;

P_{EC} – вероятность того, что ошибка будет исправлена, а кодовая комбинация принята верно;

P_{res} – остаточная вероятность ошибочного приема;

P_{ud} – вероятность необнаруженной ошибки;

$P_{ud}(FCDR(ec), p_0)$ – вероятность не обнаруженной ФКВД (или ФКВДио) ошибки;

$P_w(i)$ – вероятность применения источником i-ого слова;

p_0 – переходная вероятность симметричного двоичного постоянного канала;

p_{0eq} – эквивалентная вероятность битовой ошибки;

Q – вероятность приема блока данных без ошибок

DOI 10.15588/1607-3274-2017-3-15

$R_{FCDR}(x)$ – представленное в двоичном виде кодовое слово ФКВД;

r – длина кодового слова;

r_i – расстояние Хэмминга между принятым вектором и i-ым сигнальным вектором;

S_F – синдром перестановки.

ВВЕДЕНИЕ

Проблемы повышения эффективности систем передачи данных, включая повышение достоверности передачи и пропускной способности, всегда привлекали внимание специалистов информационных технологий и телекоммуникаций. В данном контексте перспективными являются методы факториального кодирования информации [1–6], позволяющие совместить операции помехоустойчивого кодирования, крипто- и имитозащиты и тем самым уменьшить вносимую передатчиком избыточность, повысить быстродействие и увеличить эффективную пропускную способность. Вместе с тем возможности факториального кодирования, изложенные в [1–6], далеко не исчерпаны, что и определяет круг решаемых в данной работе задач.

В работе [4] предложен, а в работе [5] получил дальнейшее развитие метод факториального кодирования с восстановлением данных по перестановке (ФКВД, FCDR). Данный метод направлен на комплексную защиту информации от несанкционированного чтения и ошибок, возникающих в канале связи. При этом ФКВД решает задачу обнаружения ошибок, а их исправление достигается повторной передачей искаженного помехой кодового слова. Вместе с тем при определенных обстоятельствах относительная скорость передачи информации в системах с решающей обратной может оказаться чрезмерно малой. Для ее повышения (а также в системах реального масштаба времени) целесообразно использовать коды с исправлением ошибок. Кроме того, как сказано в [7], комбинирование процедур обнаружения и исправления ошибок является зачастую более эффективной, чем либо только исправление ошибок, либо только обнаружение ошибок с повторной передачей. Поэтому актуальной задачей является задача совмещения процедур криптографического преобразования информации, а также обнаружения и исправления ошибок.

Целью данной работы является разработка метода факториального кодирования информации, который реализует функцию защиты информации от несанкционированного доступа, а также функцию помехоустойчивого кодирования, сочетающего обнаружение и исправление ошибок, возникающих в канале связи.

1 ПОСТАНОВКА ЗАДАЧИ

Пусть информация от источника поступает на вход кодера блоками из k бит. Тогда мощность множества информационных слов составляет 2^k. Обозначим через $A(x)$ представленное в двоичном виде информационное слово (вектор). ФКВД реализует биективное преобразование множества информационных слов $A(x)$ в разрешенное множество из 2^k перестановок $R_{FCDR}(x)$ порядка M $\left(M! \geq 2^k\right)$.

Задачей синтеза метода факториального кодирования информации, сочетающего защиту информации от несанкционированного чтения, а также обнаружение и исправление ошибок заключается в определении и анализе структуры множества из 2^k векторов $R_{FCDR}(x)$, позволяющей выделить для каждого из них область возможных значений $\hat{R}_{FCDR}(x)$ на входе приемника, расстояние до которых в заданной метрике не превышает заданного значения, а также область значений $\hat{\hat{R}}_{FCDR}(x)$, находящихся на одинаковом расстоянии до двух или более векторов $R_{FCDR}(x)$ из 2^k возможных.

2 ОБЗОР ЛИТЕРАТУРЫ

Согласно [4], перестановка $R_{FCDR}(x)$ представляет собой последовательность закодированных равномерным двоичным кодом чисел $\{0;1;\ldots;M-1\}$, очередность следования которых определяется информационной последовательностью и алгоритмом кодирования. Если порядок формирования перестановки по информационному слову источника держится в секрете, ФКВД, помимо обнаружения ошибок в канале связи, обеспечивает защиту данных от несанкционированного чтения. Кроме того, такой код является самосинхронизирующимся и не требует разделителя кодовых слов.

Как показано в [4], приемник содержит блок проверки корректности принятой из канала кодовой комбинации и декодер ФКВД. Проверка корректности сводится к проверке того факта, что в принятой кодовой комбинации каждый символ множества $\{0;1;\ldots;M-1\}$ применяется ровно по одному разу. В случае, если принятая последовательность является некорректной, она не допускается к декодированию, а на передающую станцию по обратному каналу связи передается запрос повторной передачи блока.

Корректная последовательность подлежит декодированию – обратному преобразованию $f_{FCDR}^{-1}: R_{FCDR}(x) \to A(x)$. Согласно [4], поскольку $M! > 2^k$ при $k > 1$, множество перестановок на входе декодера состоит из двух подмножеств – разрешенного и запрещенного. К разрешенному подмножеству относятся 2^k перестановок (в простейшем случае их синдромы S_F соответствуют целым числам $\left[0; 2^k - 1\right]$ числовой оси), а к запрещенному – подмножество из $\left(M! - 2^k\right)$ остальных перестановок (в простейшем случае их синдромы S_F соответствуют целым числам $\left[2^k; M! - 1\right]$ числовой оси). Прием любой перестановки из неразрешенной части множества также инициирует команду переспроса.

В работе [5] для ФКВД введен показатель избыточности (по мощности) α:

$$\alpha = M! / 2^k . \qquad (1)$$

В [5] также показано, что при $k>1$ справедливо $M!>2^k$ и, соответственно, $\alpha>1$, что приводит к избыточности кода. При этом введение дополнительных проверочных бит перед преобразованием информационного вектора в перестановку позволяет повысить обнаруживающую способность ФКВД. С другой стороны, избыточность ФКВД обеспечивает возможность увеличения расстояния между перестановками – носителями информации и создает предпосылки для создания факториального кода с исправлением ошибок. Такой код будем называть факториальным кодом с восстановлением данных и исправлением ошибок – ФКВДио (FCDRec – FCDR with error correction).

3 МАТЕРИАЛЫ И МЕТОДЫ

Введем следующие определения.

Определение 1. Сигнальными векторами называются представленные в двоичном виде перестановки разрешенного множества.

Множество сигнальных векторов образует сигнально-кодовую конструкцию (СКК).

Определение 2. Сигнальными точками называются точки на числовой оси $[0;M!-1]$, которые соответствуют сигнальным векторам кода.

Множество сигнальных точек кода образует его сигнальное созвездие.

Рассмотрим два способа формирования СКК для ФКВДио:

1) СКК, основанная на минимальном расстоянии Эвклида между сигнальными точками. Такие СКК будем называть СКК первого типа и обозначать через СКК-1;

2) СКК, основанная на минимальном расстоянии Хэмминга между сигнальными векторами. Такие СКК будем называть СКК второго типа и обозначать через СКК-2.

Рассмотрим ФКВДио с СКК-1.

Минимальное расстояние между сигнальными точками на оси $[0;M!-1]$

$$D_{\min}\le\left[(M!-1)/(2^k-1)\right]. \qquad (2)$$

В простейшем случае 2^k сигнальных точек располагаются на числовой оси $[0;2^k-1]$ с шагом $D_{\min}=1$. Такой код не предназначен для исправления ошибок. Он может быть применен для обнаружения ошибок, причем только тех, которые приводят к преобразованию перестановки в «не перестановку» или в перестановку из запрещенного множества.

Напомним, что для ФКВД $k\le[\log_2 M!]$. Выполним оценку $D_{\min}$ при $k=[\log_2 M!]$, для которого достигается максимальная скорость кода. Поскольку $\log_2 M!-1<[\log_2 M!]\le\log_2 M!$, имеет место $M!/2<2^k\le M!$. Тогда $1\le(M!-1)/(2^k-1)<2+2/(M!-2)$. Поэтому при $k=[\log_2 M!]$ минимальное расстояние между сигнальными точками $D_{\min}\le 2$. Такой ФКВД не способен исправлять все ошибки, приводящие даже к минимальному смещению сигнальных векторов по числовой оси, и поэтому его целесообразно применять для обнаружения ошибок. При этом, как и для $D_{\min}=1$, обнаруживаются только те ошибки, которые приводят к преобразованию переданной перестановки в «не перестановку» или в перестановку из запрещенного множества.

Исправление ошибок возможно при $D_{\min}\ge 3$. Для увеличения $D_{\min}$ необходимо увеличивать показатель α. Очевидно, что $\alpha=M!/2^k$ монотонно возрастает по M и убывает по k. Поэтому увеличение может быть достигнуто как увеличением M, так и уменьшением k. При этом, как показано в [5], уменьшение длины информационного вектора на Δk бит при фиксированном M приводит к увеличению показателя α в $2^{\Delta k}$ раз.

Графически расположение сигнальных точек на числовой оси представлено на рис. 1. При этом расстояние от нуля до сигнальной точки i будем обозначать через D_i, а между сигнальными точками i и j – через $D_{i,j}=D_j-D_i$.

Положение сигнальных точек на числовой оси определяется СКК. В простейшем случае сигнальные точки располагаются равномерно с шагом $D_{\min}$, при этом $D_{i,i+1}=D_{\min}$ для $i\in[0;2^k-2]$. В более общем случае $D_{i,i+1}\ne\text{const}$, а $D_{i,j}\ge D_{\min}$, $i,j\in[0;2^k-1]$, $i\ne j$.

При передаче сигнального вектора действующая в канале связи помеха может сместить сигнальную точку передатчика в любую другую точку отрезка $[0;M!-1]$, которая может быть как сигнальной, так и не сигнальной, а принятая перестановка может относиться как к разрешенному, так и к запрещенному множеству.

Приемник принимает решение о переданном сигнальном векторе на основании критерия максимального правдоподобия путем нахождения сигнальной точки, ближайшей (в метрике Эвклида) к точке, соответствующей принятому вектору. Для этого декодер вычисляет расстояния от соответствующей принятому вектору точке числовой оси до соседних сигнальных точек. При равенстве этих расстояний формируется сигнал переспроса.

Таким образом, если помеха сместила сформированный передатчиком i-ый вектор не более чем на $-\left[(D_{i-1,i}-1)/2\right]$ и $+\left[(D_{i,i+1}-1)/2\right]$ точек, эта ошибка исправляется, а принятый вектор корректируется приемником в перестановку, соответствующую i-ой сигнальной точке. Если смещение равняется $-\left[D_{i-1,i}/2\right]$ (или $+\left[D_{i,i+1}/2\right]$) и при этом $D_{i-1,i}/2\in\mathbb{Z}$ $\left(D_{i,i+1}/2\in\mathbb{Z}\right)$, ошибка обнаруживается кодом и исправляется пере-

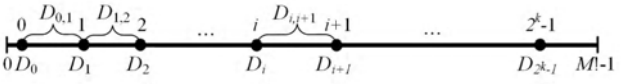

Рисунок 1 – Расположение сигнальных точек на числовой оси

спросом. Если же смещение превышает $-\left[D_{i-1,i}/2\right]$ (или $+\left[D_{i,i+1}/2\right]$), такие ошибки код исправить не может. В этом случае, если расстояния от соответствующей принятому вектору точки до соседних сигнальных точек одинаковы, ошибка обнаруживается, в противном случае возникает ошибка декодирования и, как следствие, не обнаруженная кодом ошибка.

Если принятый вектор соответствует точке из диапазона $\left[D_0-\left[\left(D_{\min}-1\right)/2\right];D_0-1\right]$, приемник корректирует ее в нулевую сигнальную точку, если же точке из диапазона $\left[D_{2^k-1}+1;D_{2^k-1}+\left[\left(D_{\min}-1\right)/2\right]\right]$ – в $\left(2^k-1\right)$ сигнальную точку, остальные точки диапазонов $\left[0;D_0-1\right]$ или $\left[D_{2^k-1}+1;M!-1\right]$ являются запрещенными.

Таким образом, все ошибки, приводящие к смещению сигнальной точки на расстояние $D\le\left[\left(D_{\min}-1\right)/2\right]$, исправляются кодом.

Положим $D_{i,i+1}=D_{\min}$ для $\forall i\in\left[0;2^k-2\right]$, $D_0=\left[\left(D_{\min}-1\right)/2\right]$, а $M!-1-D_{2^k-1}\ge\left[\left(D_{\min}-1\right)/2\right]$. В этом случае имеет место оценка

$$\left(2^k-1\right)D_{\min}+2\left[\left(D_{\min}-1\right)/2\right]+1\le M!. \qquad (3)$$

При заданных k и M $D_{\min}\le\max\left(D\right):\left(2^k-1\right)D+2\left[\left(D-1\right)/2\right]+1\le M!$.

Например, если $k=40$, а $M=16$, то $D_{\min}\le 19$. Поэтому выбор параметров k и M однозначно определяют максимальную исправляющую способность кода. Выражение (3) также может служить для выбора k или M при других известных параметрах. Например, если $k=16$, $D_{\min}=3$, то $M\ge 9$; если $M=8$, $D_{\min}=6$, то $k\le 12$. Кроме того, выражение (3) показывает, что все точки, лежащие правее пороговой точки $\left(2^k-1\right)D_{\min}+2\left[\left(D_{\min}-1\right)/2\right]+1$, относятся к запрещенной части числового множества. Поэтому все принятые кодовые комбинации после проверки корректности проходят сравнение с пороговым значением. Если соответствующая кодовой комбинации точка расположена выше пороговой точки, производится переспрос блока данных, в противном случае выполняется поиск ближайшей сигнальной точки и отождествление с ней принятой кодовой комбинации.

Структурная схема приемника ФКВДио представлена на рис. 2, где введены следующие обозначения: БПК – блок проверки корректности принятой комбинации; БИИ – блок извлечения информации из перестановки; БОМ – блок оценки принадлежности принятой перестановки к разрешенному множеству; БО – блок отождествления принятой перестановки с ближайшим разрешенным вектором данных.

Определим вероятностные характеристики ФКВДио с СКК-1.

Примем, что канал связи – симметричный двоичный постоянный с переходной вероятностью p_0, а битовые ошибки возникают в нем независимо. Тогда вероятность не обнаруженной ФКВД или ФКВДио ошибки

$$P_{ud}\left(FCDR\left(ec\right),p_0\right)=\sum_{i=0}^{2^k-1}\left(P_w\left(i\right)\cdot\sum_{t=1}^{r}f_{per}^{ud}\left(i,t\right)p_0^t q_0^{r-t}\right). \qquad (4)$$

Доля ошибок, приводящих к ошибочному декодированию: $\left(2^k-1\right)/M!$ для ФКВД и $\left(2^k-1\right)\left(2\left[\left(D_{\min}-1\right)/2\right]+1\right)/M!$ для ФКВДио. Поскольку множество ошибок, приводящих к ошибочному декодированию ФКВДио, содержит множество ошибок, приводящих к ошибочному декодированию ФКВД, $P_{ud}\left(FCDRec,p_0\right)>P_{ud}\left(FCDR,p_0\right)$ при $D_{\min}\ge 3$.

Учтем, что для простейшей системы с РОС динамическая составляющая потери скорости вследствие переспросов $\nu_2=Q+P_{ud}$ [8]. В случае использования ФКВДио

$$Q+P_{EC}+P_{det}+P_{ud}=1. \qquad (5)$$

Тогда динамическая составляющая потери скорости для ФКВДио:

$$\nu_2=1-P_{det}=Q+P_{EC}+P_{ud}. \qquad (6)$$

Вероятность исправления ошибок для ФКВДио:

$$P_{EC}\left(FCDRec,p_0\right)=\sum_{i=0}^{2^k-1}\left(P_w\left(i\right)\cdot\sum_{t=1}^{r}f_{per}^{EC}\left(i,t\right)p_0^t q_0^{r-t}\right). \qquad (7)$$

Поскольку $\nu_2=Q+P_{ud}$ для ФКВД меньше значения ν_2 по (6) для ФКВДио, при одинаковых параметрах и $D_{\min}\ge 3$ ФКВДио обеспечивает большую относительную скорость передачи по сравнению с ФКВД, однако проигрывает в помехоустойчивости.

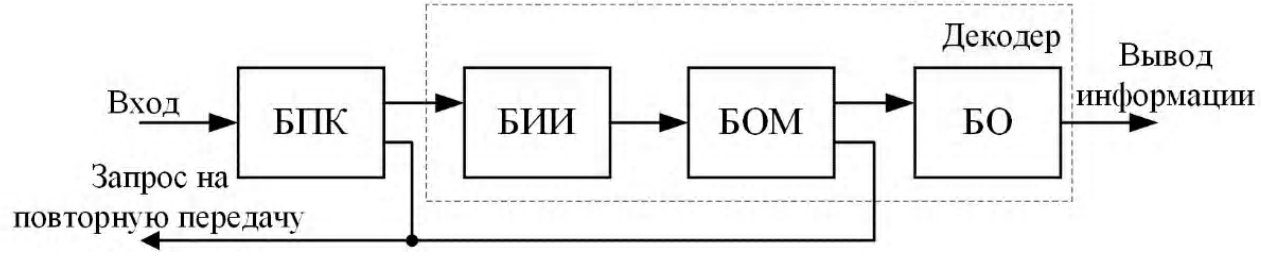

Рисунок 2 – Структурная схема приемника ФКВДио

Определим энергетический выигрыш ΔP при применении ФКВДио для некогерентного приемника, характеризующегося вероятностью битовой ошибки $p = 0,5 \cdot e^{-0,5h^2}$ [9], где h^2 – соотношение сигнал/шум. В этом случае

$$\Delta P = 10\lg\left(\ln h_{eq}^2 / \ln h_0^2\right) = 10\lg\left(\ln\left(2p_{0eq}\right)/\ln\left(2p_0\right)\right), \quad (8)$$

где эквивалентная вероятность битовой ошибки p_{0eq} [8] равна

$$p_{0eq} \approx P_{ud} / \left(k\left(1 - P_{det}\right)\right). \quad (9)$$

Учтем, что из (5) $1 - P_{det} = Q + P_{EC} + P_{ud}$. Тогда выражение (9) принимает вид:

$$p_{0eq} \approx P_{ud} / \left(k\left(Q + P_{EC} + P_{ud}\right)\right). \quad (10)$$

Остаточная вероятность ошибочного приема [8] для ФКВДио равна

$$P_{res} = P_{ud} / \left(1 - P_{det}\right) = P_{ud} / \left(Q + P_{EC} + P_{ud}\right). \quad (11)$$

Рассмотрим ФКВДио с СКК-2.

Определенное для СКК-1 расстояние Эвклида $D_{i,j}$ между сигнальными точками *i* и *j* в общем случае не равняется расстоянию Хэмминга между кодовыми словами, соответствующими этим сигнальным точкам. Вместе с тем из теории корректирующих кодов [7] известно, что для исправления ошибки в двоичных разрядах кратности *t* минимальное расстояние Хэмминга между кодовыми словами $d_{\min} \geq 2t + 1$.

Расстояние Хэмминга между сигнальными векторами *i* и *j* будем обозначать через $d_{i,j}$. СКК-2 для ФКВДио предусматривает выполнение условия $d_{i,j} \geq d_{\min}$, $i, j \in \left[0; 2^k - 1\right]$, $i \neq j$.

Определение связи между *M*, *k* и $d_{\min}$ является актуальной задачей, однако выходит за рамки данной работы. В простейшем случае для ФКВД сигнальные вектора соответствуют сигнальным точкам с шагом $D_{i,i+1} = D_{\min} = 1$ и $D_0 = 1$. Тогда $d_{\min} = 2$, а ФКВД только обнаруживает ошибки, приводящие к преобразованию переданной перестановки в «не перестановку» или в перестановку из запрещенного множества. Очевидно, что для обеспечения возможности исправления ошибок необходимо увеличивать $d_{\min}$. Для этого необходимо увеличивать показатель α. При этом ошибки исправляются при $d_{\min} \geq 3$.

При передаче сигнального вектора по каналу связи на него воздействует помеха. Модифицированный помехой вектор поступает на вход приемника ФКВДио с СКК-2, структура которого показана на рис. 3. Приемник содержит блок исправления и обнаружения ошибок БИОО и блок извлечения информации из перестановки БИИ.

БИОО реализует следующие функции: определяет расстояния Хэмминга r_i между принятым вектором и всеми сигнальными векторами, $i \in \left[0; 2^k - 1\right]$; находит минимальное расстояние $r_{\min} = \min\left\{r_i\right\}$; если существует единственное $i \in \left[0; 2^k - 1\right]$: $r_i = r_{\min}$, принятая комбинация отождествляется с *i*-ым сигнальным вектором; если существует как минимум два значения $i, j \in \left[0; 2^k - 1\right]$: $r_i = r_j = r_{\min}$, формируется сигнал переспроса. Таким образом, правила декодирования основываются на критерии максимального правдоподобия.

В БИИ производится преобразование перестановки в *k*-битную последовательность.

Учтем, что $d_{i,j} \vdots 2$ и, следовательно, $d_{\min} \vdots 2$. Поэтому при передаче *i*-го сигнального вектора ФКВДио с СКК-2 справедливы следующие утверждения:

1) ошибка с весом $t \leq \left[\left(d_{\min} - 1\right)/2\right] = \left(d_{\min} - 2\right)/2 = d_{\min}/2 - 1$ исправляется, а принятый вектор корректируется приемником в переданный сигнальный вектор;

2) ошибка с весом $t = d_{\min}/2$ может быть как исправлена (если $r_{\min}$ соответствует расстоянию только до одного *i*-го сигнального вектора), так и обнаружена и исправлена переспросом (если $r_{\min}$ соответствует расстоянию до двух и более сигнальных векторов);

3) если $t > d_{\min}/2$, ошибка либо исправляется (если $r_{\min}$ соответствует расстоянию только до одного *i*-го сигнального вектора), либо обнаруживается (если соответствует расстоянию до двух и более сигнальных векторов), либо не обнаруживается (если соответствует расстоянию только до одного сигнального вектора, отличного от *i*-го).

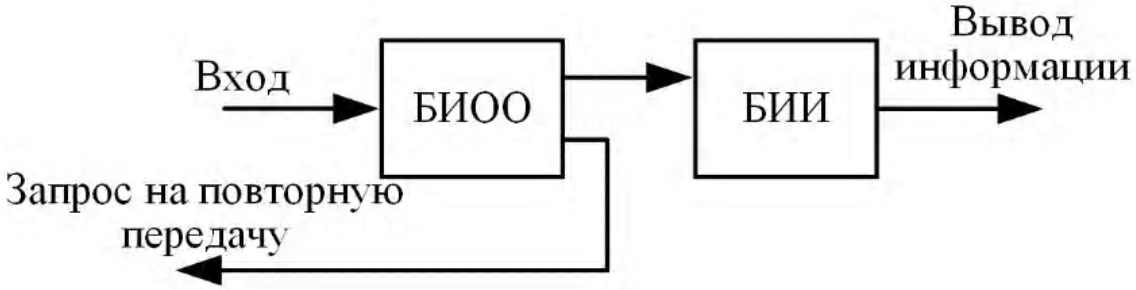

Рисунок 3 – Структурная схема приемника ФКВДио с СКК-2

Таким образом, ФКВДио с СКК-2 позволяет комбинировать исправление наиболее частых сочетаний ошибок и обнаружение с последующей повторной передачей для более редких сочетаний ошибок. Вероятностные характеристики определяются по тем же формулам, что и ФКВДио с СКК-1: (4), (6), (7), (8), (11).

Актуальным, однако выходящим за рамки данной работы, является вопрос о максимальном количестве $N_{sv}\left(d_{\min}, M\right)$ сигнальных векторов, обеспечивающих заданное $d_{\min}$ при известном M (данный вопрос тесно связан с теорией решеток и задачей наилучших упаковкой шаров в пространствах различных размерностей [10]).

4 ЭКСПЕРИМЕНТЫ

Примем $k=3$, а $M=4$. В соответствии с (3) для СКК-1 $D_{\min}\le 3$. Тогда сигнальными точками для ФКВДио с СКК-1 являются точки 1, 4, 7, 10, 13, 16, 19, 22. СКК-1 для базовой перестановки $\pi(0)=\{0;1;2;3\}$ представлена в табл. 1.

Ошибка не обнаруживается кодом, если кодовое слово, соответствующее *i*-ой сигнальной точке СКК-1, будет преобразовано помехой в комбинацию, соответствующую любой точке числовой оси, не принадлежащей диапазону $\left[D_i-1; D_i+1\right]$.

Примем, что все слова применяются источником с одинаковой вероятностью $P_w(i)=P_w=1/2^k$. Для $k=3$, $M=4$: $P_w=1/8$, $l_r=2$, $r=8$. Учтем, что $f_{per}^{ud}(i,t)=0$ при $t<2$. Тогда $P_{ud}\left(FCDRec, p_0\right)=1/8\sum_{i=0}^{7}\sum_{t=1}^{4} f_{per}^{ud}\left(i,2t\right)p_0^{2t}q_0^{8-2t}$. Значения $f_{per}^{ud}\left(i,2t\right)$ приведены в табл. 2.

С учетом четности ошибок, преобразующих перестановку в перестановку, для СКК-1

$$P_{EC}\left(FCDRec, p_0\right)=\sum_{i=0}^{2^k-1}\left(P_w(i)\cdot\sum_{t=1}^{[r/2]} f_{per}^{EC}\left(i,2t\right)p_0^{2t}q_0^{r-2t}\right).$$

Значения $f_{per}^{EC}\left(i,2t\right)$ приведены в табл. 3.

Значения $f_{per}^{ud}\left(i,2t\right)$ для ФКВД с СКК-1 приведены в табл. 4.

В табл. 1 представлена СКК-2 с $d_{\min}=4$. Экспериментально установлено, что ФКВДио с такой СКК исправляет только любые ошибки с $t=1$, а ошибка не обнаруживается тогда и только тогда, когда кодовое слово, соответствующее *i*-ому сигнальному вектору, преобразовывается помехой в комбинацию, для которой $r_j\le 1$ для $j\in\left[0;2^k-1\right]$, $j\ne i$. Поэтому $f_{per}^{EC}(i,t)=8$ при $t=1$ и $f_{per}^{EC}(i,t)=0$ при $t\ne 1$.

Значения $f_{per}^{ud}(i,t)$ для СКК-2 не зависят от сигнальной точки *i* и равны: $f_{per}^{ud}(i,3)=24$, $f_{per}^{ud}(i,4)=6$, $f_{per}^{ud}(i,5)=24$, $f_{per}^{ud}(i,6)=0$, $f_{per}^{ud}(i,7)=8$, $f_{per}^{ud}(i,8)=1$, $f_{per}^{ud}(i,t)=0$ при $t\le 2$.

Для обнаруживающего ошибки ФКВД с СКК-2 значения $f_{per}^{ud}(i,t)$ не зависят от сигнальной точки *i* и равны: $f_{per}^{ud}(i,4)=6$, $f_{per}^{ud}(i,8)=1$, $f_{per}^{ud}(i,t)=0$ при других *t*.

5 РЕЗУЛЬТАТЫ

На рис. 4 показаны графики зависимостей вероятностей необнаруженной ошибки от вероятности битовой ошибки p_0 для рассмотренных кодов: ФКВДио с СКК-1 (FCDRec-1) и СКК-2 (FCDRec-2), а также ФКВД с СКК-1 (FCDR-1) и СКК-2 (FCDR-2).

На рис. 5 для этих кодов показаны графики зависимостей величины $1-\nu_2$ от p_0.

Таблица 2 – Значения $f_{per}^{ud}\left(i,2t\right)$ для ФКВДио с СКК-1

t	Сигнальная точка							
	0	1	2	3	4	5	6	7
1	3	4	3	3	3	3	4	3
2	13	12	13	13	13	13	12	13
3	4	4	4	4	4	4	4	4
4	1	1	1	1	1	1	1	1

Таблица 3 – Значения $f_{per}^{EC}\left(i,2t\right)$ для ФКВДио с СКК-1

t	Сигнальная точка							
	0	1	2	3	4	5	6	7
1	1	0	1	1	1	1	0	1
2	1	2	1	1	1	1	2	1

Таблица 4 – Значения $f_{per}^{ud}\left(i,2t\right)$ для ФКВД с СКК-1

t	Сигнальная точка							
	0	1	2	3	4	5	6	7
1	2	2	1	1	1	1	2	2
2	2	2	4	4	4	4	2	2
3	2	2	1	1	1	1	2	2
4	1	1	1	1	1	1	1	1

Таблица 1 – СКК-1 и СКК-2 для ФКВДио при $k=3$, $M=4$

СКК-1		СКК-2	
Сигнальные точки	Сигнальные вектора	Сигнальные вектора	Сигнальные точки
1	00 01 11 10	00 01 10 11	0
4	00 11 01 10	01 00 11 10	7
7	01 00 11 10	10 11 00 01	16
10	01 11 00 10	11 10 01 00	23
13	10 00 11 01	11 01 10 00	21
16	10 11 00 01	01 11 00 10	10
19	11 00 10 01	10 00 11 01	13
22	11 10 00 01	00 10 01 11	2

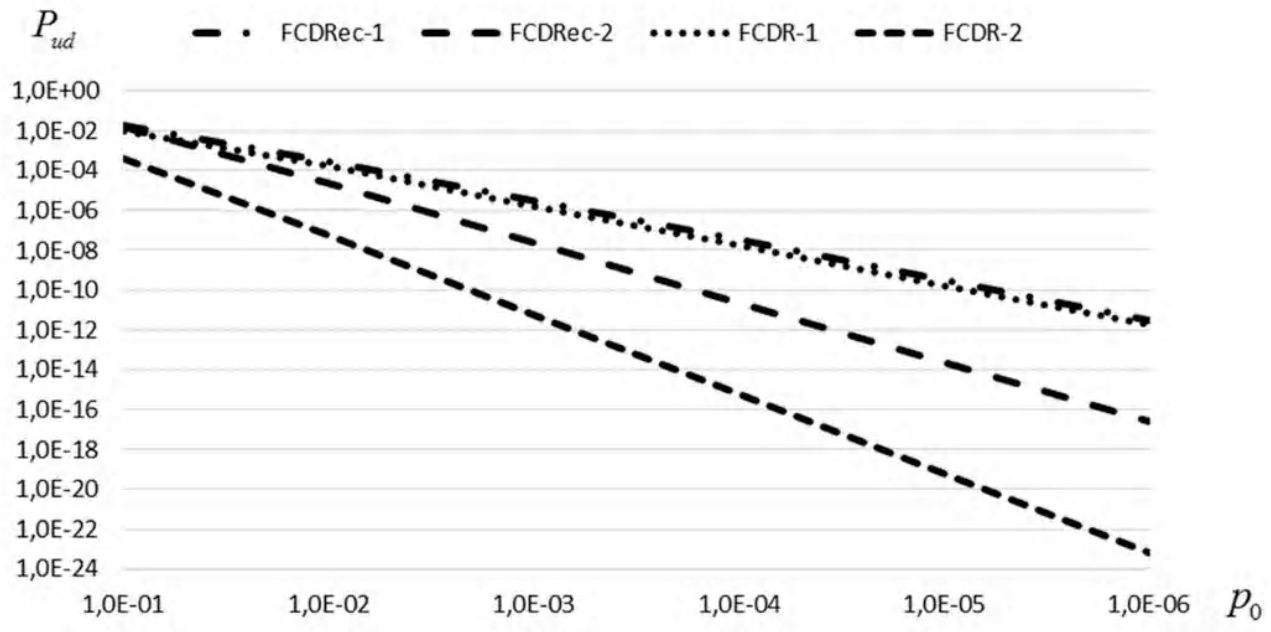

Рисунок 4 – Графики зависимостей вероятностей необнаруженной ошибки от p_0

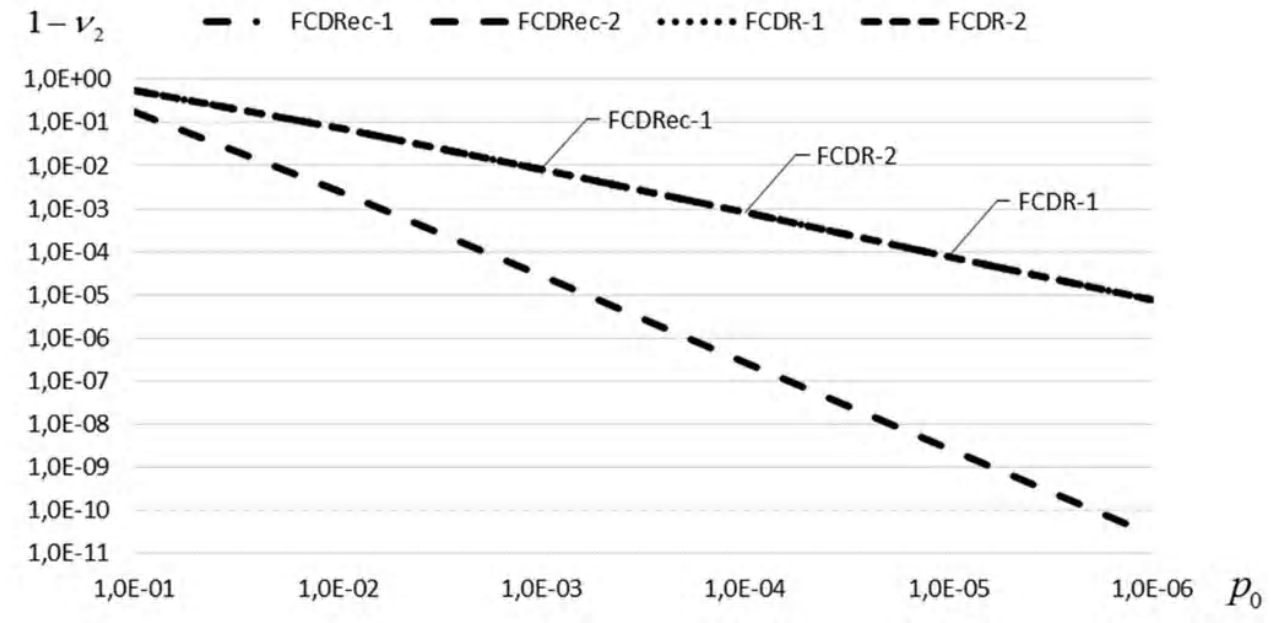

Рисунок 5 – Графики зависимостей величины $1-\nu_2$ от p_0

6 ОБСУЖДЕНИЕ

Из представленных графиков следует, что наименьшую достоверность передачи из рассмотренных кодов обеспечивает ФКВДио с СКК-1, для которого вероятность необнаруженной ошибки практически в два раза больше по сравнению с ФКВД с СКК-1. При этом динамическая составляющая потери скорости для ФКВДио и ФКВД с СКК-1 различаются незначительно (менее 3% при $p_0 = 0{,}1$). Поэтому в данном сравнении ФКВД с СКК-1 является более предпочтительным. Вместе с тем из этого пока не следует вывод в общем случае о меньшей эффективности ФКВДио по сравнению с ФКВД для СКК-1.

Наименьшую вероятность необнаруженной ошибки и наибольший энергетический выигрыш имеет ФКВД с СКК-2. Отношение $P_{ud}\left(FCDR-2, p_0\right)/P_{ud}\left(FCDR-1, p_0\right)$ равно $2{,}4\cdot 10^{1}$ при $p_0 = 0{,}1$ (разница в энергетическом выигрыше $\Delta P = 2{,}42$ дБ) и $2{,}9\cdot 10^{5}$ при $p_0 = 0{,}001$ ($\Delta P = 2{,}84$ дБ), указывая на большую эффективность СКК-2 для ФКВД.

Использование СКК-2 для ФКВДио увеличивает по сравнению с ФКВД вероятность необнаруженной ошибки: $P_{ud}\left(FCDRec-2, p_0\right)/P_{ud}\left(FCDR-2, p_0\right)$ равно $3{,}7\cdot 10^{1}$

при $p_0 = 0,1$ ($\Delta P = 2,23$ дБ) и $4 \cdot 10^3$ при $p_0 = 0,001$ ($\Delta P = 1,65$ дБ). Вместе с тем $\nu_2\left(FCDR-2, p_0\right) \approx \nu_2\left(FCDR\left(ec\right)-1, p_0\right)$, в то время, как $\nu_2\left(FCDRec-2, p_0\right)$ может значительно превосходить $\nu_2\left(FCDR-2, p_0\right)$: их разность при $p_0 = 0,1$ равна $0,828-0,431 \approx 0,4$ (более 92%) и увеличивается с увеличением p_0. Применение СКК-2 вместо СКК-1 для ФКВДио позволяет увеличить ν_2 до 82,9% при $p_0 = 0,1$, при этом P_{ud} уменьшается в 1,23 раза.

Приведенный анализ указывает, что для рассмотренных кодов ФКВД(ио) с СКК-1 и СКК-2 большей эффективностью обладают ФКВД(ио) с СКК-2. Вместе с тем из этого пока не следует вывод в общем случае о меньшей эффективности СКК-1 по сравнению с СКК-2.

ВЫВОДЫ

В процессе проведенного исследования показана возможность факториального кодирования информации, совмещающего функции исправления и обнаружения ошибок, возникающих в канале связи при передаче сообщения. Такое совмещение позволяет повысить динамическую составляющую потери скорости и, как следствие, относительную скорость передачи, по сравнению с обнаруживающим ошибки факториальным кодированием за счет снижения помехоустойчивости кода.

Установлено также, что показатели помехоустойчивости факториального кодирования с восстановлением данных, а также с восстановлением данных и исправлением ошибок не являются инвариантными по отношению к выбору сигнально-кодовой конструкции, если в качестве сигнальных векторов используется некоторое собственное подмножество множества векторов всех возможных перестановок порядка M.

СПИСОК ЛИТЕРАТУРЫ

1. Фауре Э. В. Контроль целостности информации на основе факториальной системы счисления / Э. В. Фауре, В. В. Швыдкий, А. И. Щерба // Journal of Qafqaz University. Mathematics and computer science. – 2016. – № 2. Т. 4. – (В печати).
2. Фауре Э.В. Метод формирования имитовставки на основе перестановок / Э. В. Фауре, В. В. Швыдкий, В. А. Щерба // Захист інформації. – 2014. – №4, Т. 16. – С. 334–340. DOI: 10.18372/2410-7840.16.7620.
3. Фауре Э.В. Комбинированное факториальное кодирование и его свойства / Э. В. Фауре, В. В. Швыдкий, В. А. Щерба // Радіоелектроніка, інформатика, управління. – 2016. – №3. – С. 80–86. DOI: 10.15588/1607-3274-2016-3-10.
4. Фауре Э. В. Факториальное кодирование с восстановлением данных / Э. В. Фауре // Вісник Черкаського державного технологічного університету. – 2016. – № 2. – С. 33–39.
5. Фауре Э. В. Метод повышения эффективности факториального кодирования с восстановлением данных / Э. В. Фауре // Вісник Черкаського державного технологічного університету. – 2016. – №4. – (В печати).
6. Фауре Э. В. Факториальное кодирование с несколькими контрольными суммами / Э. В. Фауре // Вісник Житомирського державного технологічного університету. – 2016. – № 3. – С. 104–113.
7. Питерсон У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон ; пер. с англ. под ред. Р. Л. Добрушина, С. И. Самойленко] – М. : Мир, 1976. – 590 с. – (Редакция литературы по новой технике).
8. Финк Л. М. Теория передачи дискретных сообщений / Л. М. Финк. – Изд. 2-е. – М. : Советское радио, 1970. – 728 с.
9. Теплов Н. Л. Помехоустойчивость систем передачи дискретной информации / Н. Л. Теплов. – М. : Связь, 1964. – 360 с.
10. Конвей Дж. Упаковки шаров, решетки и группы : в 2 т. / Дж. Конвей, Н. Слоэн ; при участии Э. Баннаи и др.; [перевод с англ. С. Н. Лицына и др.] – М. : Мир, 1990. – 2 т.

Статья поступила в редакцию 09.02.2017.
После доработки 25.03.2017.

Фауре Е. В.
Канд. техн. наук, доцент, докторант, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету, Черкаси, Україна

ФАКТОРІАЛЬНЕ КОДУВАННЯ З ВИПРАВЛЕННЯМ ПОМИЛОК

Актуальність. Факторіальне кодування даних дозволяє поєднувати операції крипто- й імітозахисту, а також завадостійкого кодування, що призводить до зменшення внесеної передавачем надлишковості, підвищення швидкодії та збільшення ефективної пропускної здатності. Разом з тим описані методи факторіального кодування не дозволяють виправляти помилки, що обмежує область їх використання.

Метою роботи є розробка методу факторіального кодування з відновленням даних за перестановкою, що забезпечує комплексне вирішення задач криптографічного захисту та завадостійкого кодування і дозволяє поєднати функції виправлення та виявлення помилок каналу зв'язку.

Метод. Основна ідея запропонованого методу кодування полягає в збільшенні відстані між дозволеними кодовими словами, які являють собою перестановки, обчислені за всіма інформаційними бітами блоку даних і представлені в двійковому вигляді. Досліджено методи збільшення відстані на основі метрик Евкліда і Хеммінга. Для кожного з цих методів визначено основні властивості факторіального коду з виправленням помилок, у тому числі виконано оцінку достовірності передавання при незалежності і біноміальному розподілі помилок у каналі зв'язку, розроблено структурні схеми приймача. Правила декодування, реалізовані в приймачі, ґрунтуються на критерії максимальної правдоподібності і передбачають як пряме виправлення помилок, так і їх виявлення з наступним виправленням шляхом перезапиту пошкодженого блоку.

Результати. Реалізовано факторіальні коди з виправленням помилок, які використовують метрики Евкліда і Хеммінга. Для цих кодів виконано порівняльний аналіз ймовірності невиявленої помилки, залишкової ймовірності помилкового прийому, енергетичного виграшу та відносної швидкості передавання. Показано, що характеристики коду не є інваріантними щодо множини дозволених кодових слів, а з розглянутих кодів більш ефективними є коди, які використовують метрику Хеммінга.

Висновки. Отримав подальший розвиток метод факторіального кодування з відновленням даних за перестановкою, який за рахунок поєднання функцій виправлення та виявлення помилок дозволяє підвищити динамічну складову втрати швидкості і, як наслідок, відносну швидкість передавання, в порівнянні з виявляючим помилки факторіальним кодуванням за рахунок зниження його завадостійкості. Проведені експерименти підтвердили ефективність факторіальних кодів з виправленням помилок.

Ключові слова: надлишковість, факторіальний код, перестановка, завадостійке кодування, виправлення помилок, виявлення помилок, достовірність передавання, відносна швидкість передавання.

Faure E. V.

PhD, Associate Professor, Post-Doctoral Associate, Associate Professor of Department of Information Security and Computer Engineering, Cherkasy State Technological University, Cherkasy, Ukraine

FACTORIAL CODING WITH ERROR CORRECTION

Context. Factorial data coding allows combining operations of cryptographic protection, intentional alteration of data, and error-correcting coding which leads to the decrease of redundancy introduced by transmitter and to the increase of data rate and effective throughput. At the same time, the described methods of factorial coding do not correct errors, which limits their use.

Objective of this work is to develop a method of factorial coding with data recovery that provides a comprehensive solution of cryptographic protection and error control coding and allows combining the functions of communication channel errors detecting and correcting.

Method. The basic idea of the proposed coding method is to increase the distance between the allowed code words that represent permutations calculated for all information bits of a data block and represented in a binary form. The methods of distance increasing based on Euclidean and Hamming metrics are investigated. The basic properties of factorial code with error correction are defined for each of these methods. The estimate of probability characteristics is done on the condition of independence of communication channel errors and their binomial distribution. The receiver structures are developed. Decoding rules implemented in receiver are based on the maximum likelihood criteria and provide both forward error correction and error detection with further correction by retransmission of damaged data block.

Results. The factorial error-correcting codes using Euclidean and Hamming metrics are implemented. The comparative analysis of the probability of an undetected error, the residual probability of erroneous reception, energy gain, and the relative transmission rate is done for these codes. It is shown that code characteristics are not invariant to the set of allowed code words, and the codes that use Hamming metric are the most efficient codes between the presented codes.

Conclusions. The method of factorial coding data recovery by permutation has been further developed. Due to the combination of error correction and detection functions, it can increase the rate loss dynamic component and, consequently, the relative transmission rate, compared to error-detecting factorial coding by reducing its noise immunity. The experiments confirmed the effectiveness of the factorial error-correcting codes.

Keywords: redundancy, factorial code, permutation, error control coding, error correction, error detection, reliability of data transmission, relative transmission rate.

REFERENCES

1. Faure E'. V., Shvydkij V. V., Shherba A. I. Kontrol' celostnosti informacii na osnove faktorial'noj sistemy schisleniya, *Journal of Qafqaz University. Mathematics and computer science*, 2016, No. 2, Vol. 4. (V pechati).
2. Faure E'. V., Shvydkij V. V., Shherba V. A. Metod formirovaniya imitovstavki na osnove perestanovok, *Zaxist informacii*, 2014, No. 4, Vol. 16, pp. 334–340. DOI: 10.18372/2410-7840.16.7620.
3. Faure E'.V., Shvydkij V. V., Shherba V. A. Kombinirovannoe faktorial'noe kodirovanie i ego svojstva, *Radio Electronics, Computer Science, Control*, 2016, No. 3, pp. 80–86. DOI: 10.15588/1607-3274-2016-3-10.
4. Faure E'.V. Faktorial'noe kodirovanie s vosstanovleniem dannyx, *Visnyk Cherkas'kogo derzhavnogo tehnologichnogo universytetu*, 2016, No. 2, pp. 33–39.
5. Faure E'.V. Metod povysheniya e'ffektivnosti faktorial'nogo kodirovaniya s vosstanovleniem dannyx, *Visnyk Cherkas'kogo derzhavnogo tehnologichnogo universytetu*, 2016, No. 4. (V pechati).
6. Faure E'.V. Faktorial'noe kodirovanie s neskol'kimi kontrol'nymi summami, *Visnyk Zhytomyrs'kogo derzhavnogo tehnologichnogo universytetu*, 2016, No. 3, pp. 104–113.
7. Piterson U., Ue'ldon E'.; [per. s angl. pod red. R. L. Dobrushina, S. I. Samojlenko] Kody, ispravlyayushhie oshibki. Moscow, Mir, 1976, 590 p. (Redakciya literatury po novoj texnike).
8. Fink L. M. Teoriya peredachi diskretnyx soobshhenij. [Izd. 2-e, pererab. i dopoln.]. Moscow, Sovetskoe radio, 1970, 728 p.
9. Teplov N. L. Pomexoustojchivost' sistem peredachi diskretnoj informacii. Moscow, Svyaz', 1964, 360 p.
10. Konvej Dzh., Sloe'n N. ; pri uchastii E'. Bannai i dr.; [perevod s angl. S. N. Licyna i dr.] Upakovki sharov, reshetki i gruppy : v 2 t. Moscow, Mir, 1990, 2 t.