УДК 004.056

Э.В. Фауре, к.т.н., доц.
Черкасский государственный технологический университет

ФАКТОРИАЛЬНОЕ КОДИРОВАНИЕ С НЕСКОЛЬКИМИ КОНТРОЛЬНЫМИ СУММАМИ

Предложены и подробно рассмотрены методы факториального кодирования с несколькими контрольными суммами, которые направлены на сокращение времени формирования кодового слова и объем используемой при этом памяти за счет параллельной обработки поступающих на вход кодера и декодера данных при комплексном решении задач контроля целостности информации и ее криптографической защиты. Метод систематического факториального кодирования с несколькими контрольными суммами использует в качестве проверочной части кодового слова конкатенацию нескольких проверочных частей, вычисленных по отдельным частям информационного блока. Несистематическое кодирование с несколькими контрольными суммами предусматривает замену информационной последовательности на конкатенацию нескольких перестановок, вычисленных по различным блокам, на которые разбивается информационная последовательность символов. Для предложенных методов кодирования изучены зависимости оценок вероятности необнаруженной ошибки и энергетического выигрыша от длины информационного вектора на входе кодера. Произведено сравнение показателей обнаруживающей способности для факториальных кодов с несколькими контрольными суммами и других помехоустойчивых кодов.

Ключевые слова: *факториальный код; перестановка; контроль целостности информации; криптозащита; помехоустойчивое кодирование; достоверность передачи; стойкость.*

Постановка проблемы. Конфиденциальность и контроль целостности информации являются неотъемлемой частью функционирования телекоммуникационных систем общего и специального назначения. Методы кодирования, которые обеспечивают комплексное решение задач криптозащиты, имитозащиты и защиты данных от ошибок, обусловленных действием помех в канале связи, позволяют уменьшить вводимую избыточность и снизить требования к производительности устройств преобразования информации, а разработка таких методов является актуальным направлением исследований.

Анализ последних исследований и публикаций. Приведенные в работах [1–5] результаты исследований показывают эффективность факториальных методов кодирования для обеспечения контроля целостности информации, совмещающего в себе функции имитозащиты и помехоустойчивого кодирования.

В работе [6] предложен метод факториального кодирования с восстановлением данных по перестановке (ФКВД), реализующий в себе функции обнаружения ошибок в канале связи и криптографической защиты информации. В работе [7] представлен метод повышения эффективности ФКВД за счет введения дополнительных проверочных бит – ФКВДд.

Отметим, что все известные факториальны коды [1–7] предусматривают формирование контрольной суммы (перестановки) в соответствии с поступающим на вход кодера k-битным информационным вектором $A(x)$ (в данной работе будем использовать широко принятый [8 с. 601; 9, с. 232; 10. с. 361] подход к рассмотрению векторов над полем F_2 в виде элементов алгебры многочленов с коэффициентами из F_2). При этом:

– при последовательной обработке символов информационного вектора $A(x)$ количество операций и, соответственно, время формирования контрольной суммы (перестановки) увеличиваются при увеличении k;

– при использовании таблицы замен вектора $A(x)$ на перестановку (например, для ФКВД(д)) количество записей в ней равняется 2^k и также увеличивается при увеличении k.

Таким образом, при увеличении размера поступающего на вход кодера блока данных время формирования перестановки, а также объем необходимой памяти возрастают и при некотором значении k могут превышать допустимые пределы.

Целью данной работы является разработка и оценка эффективности методов факториального кодирования данных, позволяющих сократить время формирования кодового слова и объем используемой при этом памяти за счет параллельной обработки поступающих на вход кодера и декодера данных.

Изложение основного материала. Рассмотрим метод факториального кодирования данных с прореживанием, позволяющий уменьшить количество бит информационного вектора $A(x)$, обрабатываемых кодером в процессе формирования кодового слова.

1. Факториальное кодирование с прореживанием

Определение 1. Факториальным кодом с прореживанием (ФКП) называется систематический код, использующий в качестве проверочной части кодового слова перестановку чисел порядка M, которая вычисляется по части поступающих на вход кодера информационных символов.

Примечание. Процедура выборки k_{FCD} бит из k информационных бит $(k_{FCD} < k)$ является процедурой прореживания или децимации. Проверочная часть ФКП (FCD – Factorial Code with Decimation) формируется по прореженной последовательности из k_{FCD} бит в соответствии с принципами полного факториального кодирования (ПФК) [2]. При равномерном двоичном кодировании символов перестановки длина проверочной части $r_{FCD} = M \cdot (\text{entier}(\log_2 M)+1)$ бит. Длина кодового слова $n_{FCD} = k + r_{FCD}$, скорость кода $\nu_{FCD} = k/(k + r_{FCD})$.

Оценка достоверности передачи. Все характеристики методов кодирования будем определять для простейшей системы передачи данных с решающей обратной связью, где прямой канал – двоичный симметричный с переходной вероятностью p_0 $(q_0 = 1 - p_0)$, обратный канал – идеальный. Поскольку контрольная сумма охватывает проверкой только k_{FCD} из k информационных бит, не обнаруженная ФКП ошибка может возникнуть вследствие:

1) ошибки в остальных $(k - k_{FCD})$ битах информационной части;

2) необнаруженной ошибки при декодировании контрольной суммы ПФК, вычисленной по k_{FCD} информационным битам.

Вероятность не обнаруженной ФКП ошибки вычисляется следующим образом:

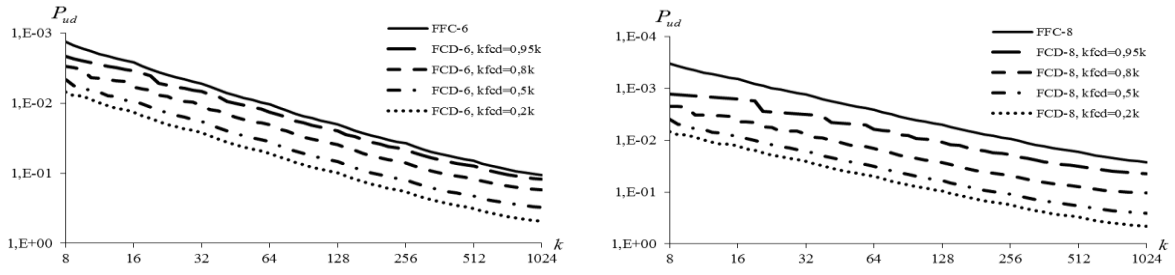
$$P_{ud}(FCD, p_0) = P_{ud}(FFC, p_0) + p_{dec}, \quad (1)$$

где вероятность не обнаруженной ПФК (FFC) ошибки $P_{ud}(FFC, p_0)$ определяется по (2) из [2]:

$$P_{ud}(FFC, p_0) = p_r^{\wedge} \cdot p_r, \quad (2)$$

при этом $p_r^{\wedge}$ и p_r оцениваются по формулам (1) и (7) (или (11) и (12)) из [2], а значение k в этих формулах заменяется на k_{FCD}; $p_{dec} = \left(1 - q_0^{k-k_{FCD}}\right) \cdot q_0^{k_{FCD}+r_{FCD}}$ – вероятность ошибки децимации: ошибки в $(k - k_{FCD})$ битах информационной части, не использующихся при формировании контрольной суммы, при условии, что остальные $(k_{FCD} + r_{FCD})$ бит помехой не поражены.

На рисунке 1 представлены графики зависимостей оценок вероятностей необнаруженной ошибки (1) от длины информационной части кодового слова в результате применения ФКП при $p_0 = 10^{-3}$ для различных соотношений k_{FCD}/k и величины M.



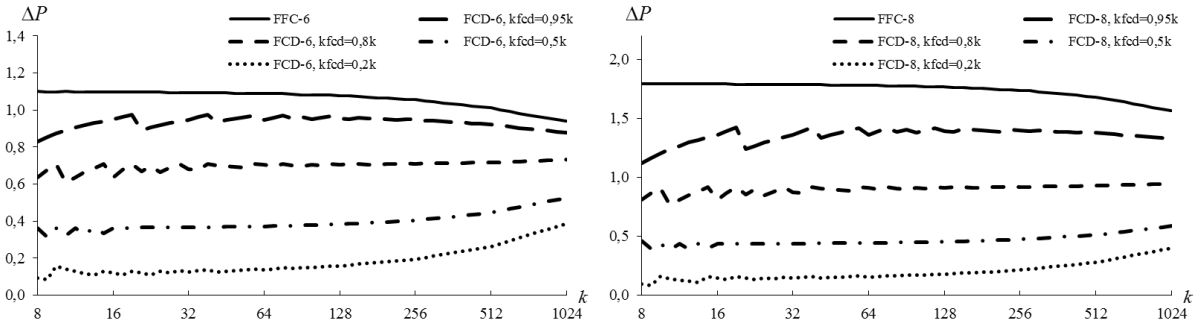
а) *б)*

Рис. 1. Графики зависимостей оценок вероятностей необнаруженной ошибки ФКП от длины информационной части при $p_0 = 10^{-3}$ для различных значений k_{FCD}/k и $M = 3$ (а); $M = 4$ (б)

Энергетический выигрыш в результате применения факториального кодирования будем оценивать для оптимального некогерентного приемника двоичных сигналов с ЧМн, характеризующийся вероятностью битовой ошибки $p = 0.5 \cdot e^{-0.5h^2}$ [11, с. 45], где h^2 – соотношение сигнал/шум (отношение энергии сигнала, приходящейся на 1 бит принимаемого сообщения, к спектральной плотности мощности шума).

Пример. Оценим энергетический выигрыш ФКП при $p_0 = 10^{-3}$, $k = 1376$, $k_{FCD} = 500$, $M = 8$ и $r_{FCD} = 24$. Тогда $\nu_{FCD} = 1376/1400 = 0.983$, $P_{ud}(FCD, p_0) \le 0.346$, а $\Delta P \ge 0.56$ дБ.

На рис. 2 представлены графики оценок энергетического выигрыша от длины информационной части кодового слова в результате применения ФКП при $p_0 = 10^{-3}$ для различных соотношений k_{FCD}/k и величины M.



а) *б)*

Рис. 2. Графики зависимостей оценок энергетического выигрыша ФКП от длины информационной части при $p_0 = 10^{-3}$ для различных значений k_{FCD}/k и $M = 3$ (а); $M = 4$ (б)

Рисунки 1 и 2 указывают на очевидный проигрыш ФКП по сравнению с ПФК, который увеличивается при уменьшении соотношения k_{FCD}/k.

Свойства факториального кодирования с прореживанием:

– информационная часть кодового слова передается в канал связи в исходном виде, поэтому ФКП не обеспечивает защиту информации от несанкционированного чтения;

– поскольку ФКП охватывает проверкой только часть информационных символов, он не может служить в качестве полноценного средства КЦИ;

– обнаруживающая способность ФКП уступает обнаруживающей способности ПФК и CRC-кода;

– ФКП обладает свойством самосинхронизации.

Отметим, что достоверность передачи ФКП можно увеличить (за счет уменьшения скорости кода), если для информационной последовательности вычислить N $(N \ge 2)$ контрольных сумм-перестановок по принципам ФКП, охватив проверкой все информационные биты. В этом случае принципы ФКП являются базовыми для следующего вида факториального кодирования – с несколькими контрольными суммами.

2. Факториальное кодирование с несколькими контрольными суммами. Рассмотрим два типа факториального кодирования с несколькими контрольными суммами (ФКНКС) – систематическое и несистематическое.

2.1. Систематическое факториальное кодирование с несколькими контрольными суммами

Определение 2. Систематическим факториальным кодом с несколькими контрольными суммами (ФКНКСс) называется код, использующий в качестве проверочной части кодового слова конкатенацию нескольких проверочных частей ФКП.

Примем, что i-ая проверочная часть ФКП $(1 \le i \le N)$ является перестановкой порядка $M(i)$ и вычисляется по $k_{FCD}(i)$ информационным битам. При этом $\sum_{i=1}^{N} k_{FCD}(i) = k$, а каждый информационный бит участвует в формировании только одной контрольной суммы.

При равномерном двоичном кодировании символов перестановок длина i-ой проверочной части $r_{FCD}(i) = M(i)\cdot\left(\text{entier}\left(\log_2 M(i)\right)+1\right)$ бит. Тогда полная длина кодового слова ФКНКСс (FCSCs – Factorial Code with Several Checksums (systematic)) $n_{FCSCs} = k + \sum_{i=1}^{N} r_{FED}(i)$, а скорость кода $\nu_{FCSCs} = k \Big/ \left(k + \sum_{i=1}^{N} r_{FCD}(i) \right)$.

Практически реализовать ФКНКСс при $k_{FCD}(i) = k_{FCD} = const$ можно следующим образом.

Укрупним символы источника таким образом, чтобы каждый укрупненный символ образовывался группой из l_k бит и соответствовал элементу поля $F_2^{l_k}$ (числу L-адической системы счисления, где $L = 2^{l_k}$ (четверичной, восьмеричной, шестнадцатеричной и т.п.)). Примем, что k кратно l_k, тогда информационная часть будет содержать $k_{FCD} = k/l_k$ укрупненных символов. Первая контрольная сумма-перестановка формируется по двоичной последовательности, образованной первыми битами укрупненных информационных символов, вторая – вторыми битами, третья – третьими и т.д. Полученные l_k контрольных сумм объединяются путем конкатенации в единую проверочную часть и дополняют информационную последовательность при передаче по каналу связи.

Заметим, что ФКНКС позволяет уменьшить корреляцию битовых ошибок в принятом блоке данных, например, при их группировании.

Оценка достоверности передачи. Поскольку кодовое слово ФКНКСс представляет собой объединение N кодовых слов ПФК, не обнаруженная им ошибка возникает, когда хотя бы в одном из N кодовых слов ПФК ошибка не обнаружена, а остальные – ошибкой не поражены.

Вероятность не обнаруженной ФКНКСс ошибки равняется разности между вероятностями события, при котором в N кодовых словах ПФК нет обнаруженных ошибок, и события, при котором все N кодовых слов ПФК приняты без ошибок:

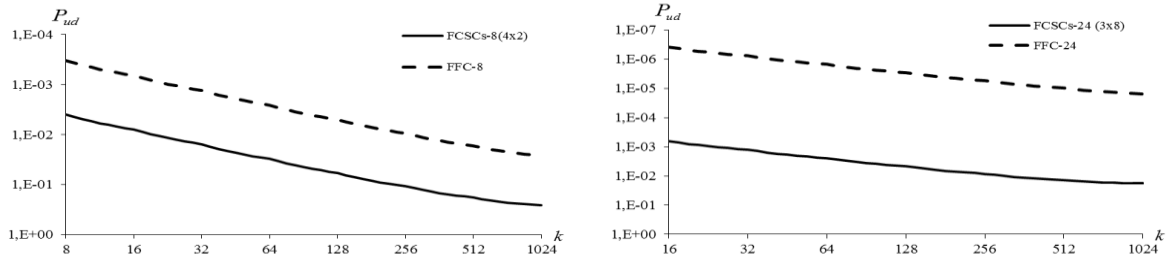
$$P_{ud}\left(FCSCs, p_0\right) = \prod_{i=1}^{N}\left[Q(i) + P_{ud}\left(FFC(i), p_0\right)\right] - \prod_{i=1}^{N} Q(i), \qquad (3)$$

где $Q(i) = q_0^{n_{FCD}(i)}$ – вероятность приема без ошибок $n_{FED}(i)$ бит блока данных, соответствующих i-му кодовому слову ПФК, $n_{FCD}(i) = k_{FCD}(i) + r_{FCD}(i)$; $P_{ud}\left(FFC(i), p_0\right)$ – вероятность появления необнаруженной ошибки в i-м кодовом слове ПФК, которая вычисляется по формуле (2), при этом при оценке $p_r^{\wedge}$ и p_r значение k заменяется на $k_{FCD}(i)$, а M – на $M(i)$.

Пример. Оценим энергетический выигрыш ФКНКСс для некогерентного приема при $p_0 = 10^{-3}$, $k = 768$, $N = 3$, $k_{FCD}(i) = 256$, $M(i) = 4$ для $\forall i \in [1; N]$. Тогда $l_r(i) = \text{entier}\left(\log_2 M(i)\right)+1 = 2$, $\forall i \in [1; N]$, $r_{FCSCs} = \sum_{i=1}^{N} l_r(i)\cdot M(i) = 24$, а $\nu_{FCSCs} = 768/792 = 0.97$.

Вероятность не обнаруженной ФКНКСс ошибки $P_{ud}\left(FCSCs, p_0\right) \le 1.67\cdot 10^{-2}$, а $\Delta P \ge 1.74$ дБ.

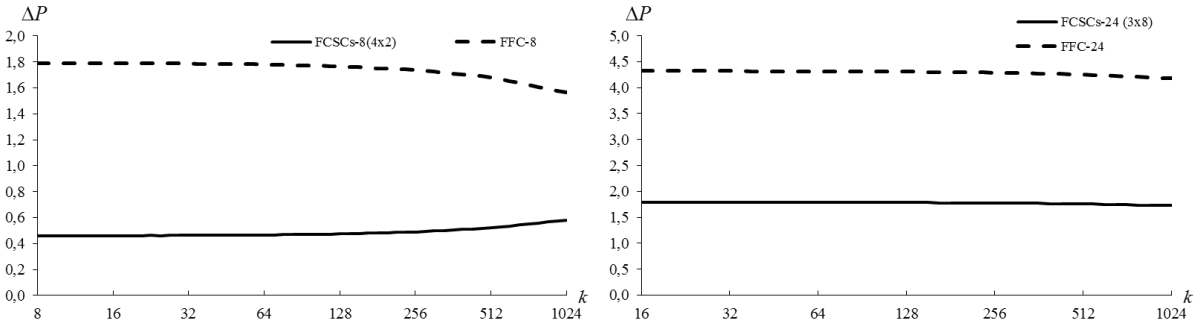
На рисунке 3 представлены графики зависимостей (3) оценок вероятностей необнаруженной ошибки от длины информационной части кодового слова в результате применения ФКНКСс и ПФК при $p_0 = 10^{-3}$ для различных значений N и M.



а) *б)*

Рис. 3. Графики зависимостей оценок вероятностей необнаруженной ошибки ФКНКСс и ПФК от длины информационной части при $p_0 = 10^{-3}$ для $N = 4$, $M = 2$ (а); $N = 3$, $M = 4$ (б)

На рисунке 4 показаны графики зависимостей оценок энергетического выигрыша от длины информационной части кодового слова в результате применения ФКНКСс и ПФК при $p_0 = 10^{-3}$ для различных значений N и M.



а) *б)*

Рис. 4. Графики зависимостей оценок энергетического выигрыша ФКНКСс и ПФК от длины информационной части при $p_0 = 10^{-3}$ *для* $N = 4$ *и* $M = 2$ *(а);* $N = 3$ *и* $M = 8$ *(б)*

Сравнение зависимостей $\Delta P_{FCSCs}(k)$ и $\Delta P_{FFC}(k)$ при одинаковых скоростях кодов указывает на меньшую обнаруживающую способность ФКНКСс по сравнению с ПФК.

Свойства ФКНКСс:

– информационная часть кодового слова передается в канал связи в исходном виде, поэтому данный код не обеспечивает защиту информации от несанкционированного чтения;

– процедура формирования проверочной части кодового слова обеспечивает возможность ее использования в качестве имитовставки и совмещение функций имитозащиты и защиты от ошибок канала связи;

– обнаруживающая способность ФКНКСс уступает обнаруживающей способности ПФК и CRC-кода;

– ФКНКСс обладает свойством самосинхронизации.

2.2. Несистематическое факториальное кодирование с несколькими контрольными суммами

Определение 3. Несистематическим ФКНКС (ФКНКСн) называется код, предусматривающий замену информационной последовательности на конкатенацию N кодовых слов ФКВД, вычисленных по N различным блокам, на которые разбивается информационная последовательность символов.

Кодовое слово ФКНКСн (FCSCn – Factorial Code with Several Checksums (nonsystematic)), в отличие от ФКНКСс, состоит только из контрольных сумм-перестановок. При этом перестановки вычисляются в соответствии с принципами ФКВД, а $M(i)! \geq 2^{k_{FCD}(i)}$.

При равномерном двоичном кодировании символов перестановок $r_{FCD}(i) = M(i) \cdot \left(\text{entier}\left(\log_2 M(i)\right) + 1\right)$, длина кодового слова $n_{FCSCn} = \sum_{i=1}^{N} r_{FCD}(i)$, а скорость кода

$$\nu_{FCSCn} = k \Big/ \sum_{i=1}^{N} r_{FCD}(i). \qquad (4)$$

Оценка достоверности передачи. Поскольку кодовое слово ФКНКСн представляет собой конкатенацию N кодовых слов ФКВД, не обнаруженная им ошибка возникает, когда хотя бы в одном из N кодовых слов ФКВД ошибка не обнаружена, а остальные – ошибкой не поражены.

Вероятность не обнаруженной ФКНКСн ошибки равняется разности между вероятностями события, при котором в N кодовых словах ФКВД нет обнаруженных ошибок, и события, при котором все N кодовых слов ФКВД приняты без ошибок:

$$P_{ud}(FCSCn, p_0) = \prod_{i=1}^{N} \left[Q(i) + P_{ud}\left(FCDR(i), p_0\right) \right] - \prod_{i=1}^{N} Q(i), \qquad (5)$$

где $Q(i) = q_0^{r_{FCD}(i)}$ – вероятность приема без ошибок $r_{FCD}(i)$ бит блока данных, соответствующих i-му кодовому слову ФКВД; $P_{ud}\left(FCDR(i), p_0\right)$ – вероятность необнаруженной ошибки в i-м кодовом слове ФКВД (FCDR), которая оценивается по (2) из [6] или (4) из [7], при этом значение r заменяется на $r_{FCD}(i)$.

Пример. Оценим энергетический выигрыш ФКП для некогерентного приема при $p_0 = 10^{-3}$, $k = 768$, $N = 4$, $k_{FCD}(i) = 192$, $M(i) = 47$ для $\forall i \in [1; N]$. Тогда $r_{FCD}(i) = M(i) \cdot \left(\text{entier}\left(\log_2 M(i)\right) + 1\right) = 282$, $\forall i \in [1; N]$, а $n_{FCSCn} = \sum_{i=1}^{N} r_{FCD}(i) = 1128$, $v_{FCSCn} = k \Big/ \sum_{i=1}^{N} r_{FCD}(i) = 0.68$. Вероятность не обнаруженной ФКНКСс ошибки $P_{ud}\left(FCSCn, p_0\right) \le 1.84 \cdot 10^{-4}$, при этом энергетический выигрыш $\Delta P \ge 3.35$ дБ.

На рисунке 5 показаны графики зависимостей (5) оценок вероятностей необнаруженной ошибки ФКНКСн от размера блока данных на входе кодера при $p_0 = 10^{-3}$ для различных значений N и способов формирования блоков ФКВД (ФКВД или ФКВДд).

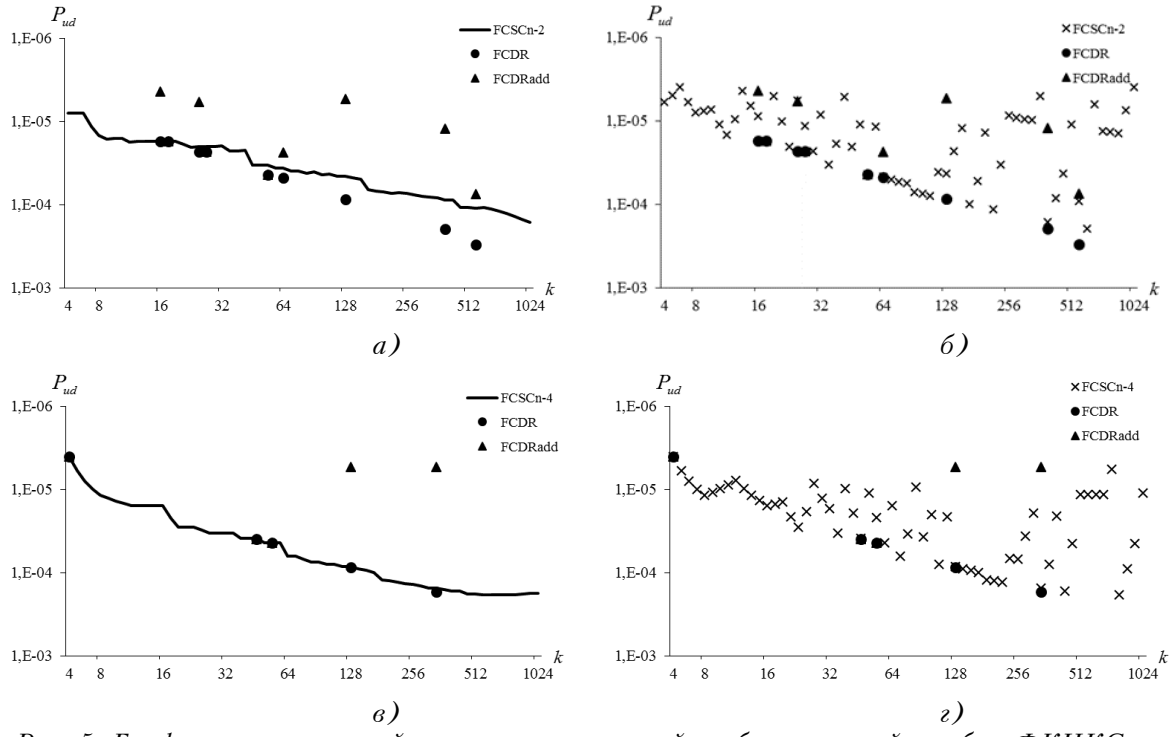


Рис. 5. Графики зависимостей оценок вероятностей необнаруженной ошибки ФКНКСн от размера блока данных на входе кодера при $p_0 = 10^{-3}$ для $N = 2$ блоков ФКВД (а); $N = 2$ блоков ФКВДд (б); $N = 4$ блоков ФКВД (в); $N = 4$ блоков ФКВДд (г)

На рисунке 6 представлены графики зависимостей энергетического выигрыша ФКНКСн от размера блока данных на входе кодера при $p_0 = 10^{-3}$ для различных значений N и способов формирования блоков ФКВД (ФКВД или ФКВДд).

Дополнительно на графиках рисунков 5 и 6 отображены оценки вероятностей необнаруженной ошибки и энергетического выигрыша, достигаемые в результате применения ФКВД и ФКВДд (FCDRadd) при идентичных ФКНКСн размере блока данных на входе кодера и скорости кода.

Из анализа представленных графиков следует, что обнаруживающая способность ФКНКСн не уступает обнаруживающей способности ФКВД при одинаковом размере блока данных на входе кодера и одинаковой скорости кода. Данное обстоятельство позволяет уменьшить

требования к реализующим ФКВД вычислительным средствам за счет использования блока меньшей длины и конкатенации нескольких кодовых слов ФКВД в кодовое слово ФКНКСн, сохраняя при этом обнаруживающую способность кода и его скорость. Вместе с тем в большинстве случаев обнаруживающая способность ФКНКСн уступает обнаруживающей способности ФКВДд.

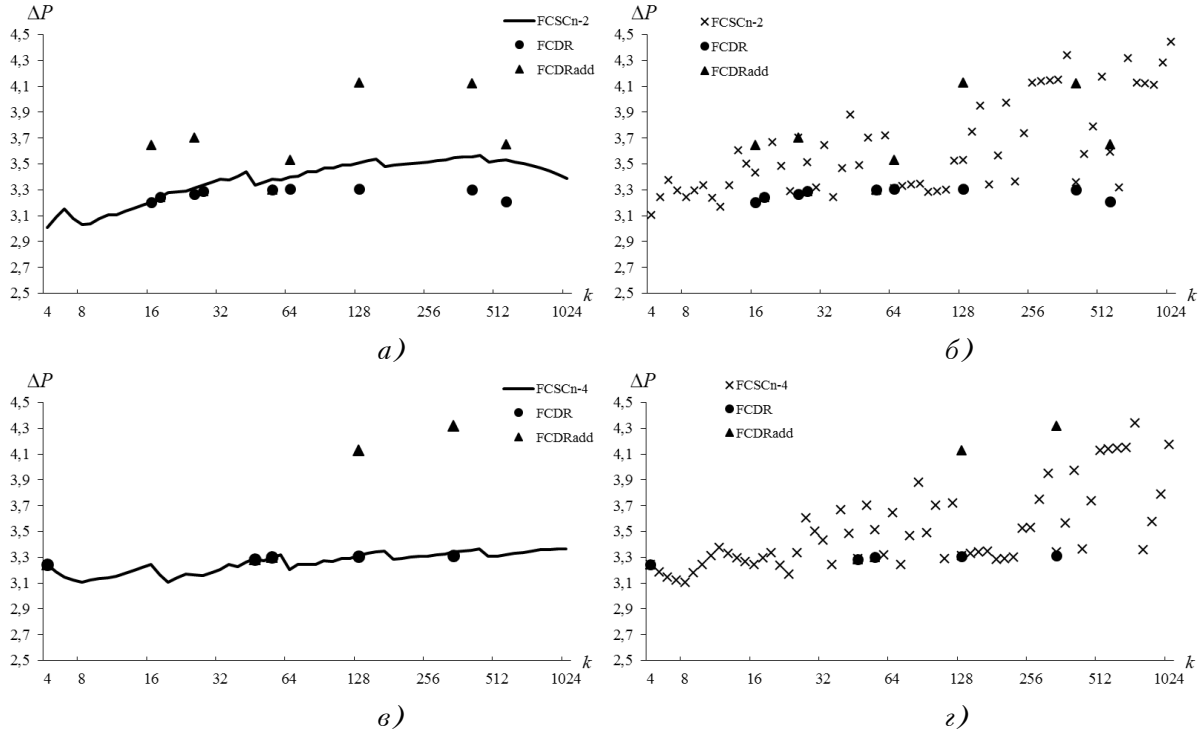


Рис. 6. Графики зависимостей оценок энергетического выигрыша ФКНКСн от размера блока данных на входе кодера при $p_0 = 10^{-3}$ для $N = 2$ блоков ФКВД (а); $N = 2$ блоков ФКВДд (б); $N = 4$ блоков ФКВД (в); $N = 4$ блоков ФКВДд (г)

Графики зависимостей (4) скорости ФКНКСн от размера блока данных на входе кодера для различных N показаны на рисунке 7.

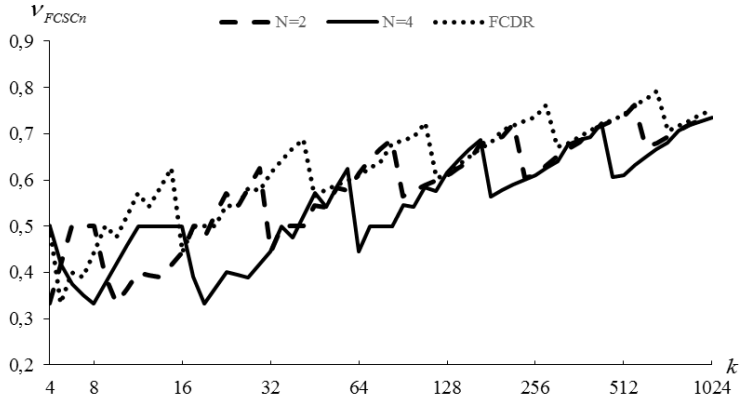


Рис. 7. График зависимости скорости ФКНКСн от размера блока данных на входе кодера при различных N

Из графика на рисунке 7 следует, что увеличение количества N кодовых слов ФКВД в кодовом слове ФКНКСн, в целом, уменьшает скорость кода. Поэтому скорость ФКНКСн уступает скорости ФКВД, хотя при некоторых размерах блока данных на входе кодера k их скорости приблизительно равны (см., например, скорости при $k \in [352; 448]$). Диапазоны

значений k, при которых скорости ФКНКСн и ФКВД практически совпадают, уменьшаются при увеличении N.

Поскольку кодовое слово ФКНКСн состоит из кодовых слов ФКВД, он обладает свойствами, характерными для ФКВД:

– ФКНКСн обеспечивает защиту от несанкционированного чтения;

– ФКНКСн обеспечивает защиту от ошибок в канале связи и не обеспечивает имитозащиту;

– обнаруживающая способность ФКНКСс сравнима с обнаруживающей способностью ФКВД, однако в большинстве случаев ей уступает;

– скорость ФКНКСн, в целом, уступает скорости ФКВД;

– ФКНКСн обладает свойством самосинхронизации;

– при использовании ФКНКСн не возникают коллизии.

3. Оценка крипто- и имитостойкости кодов. Выполним количественную оценку стойкости разработанных кодов от несанкционированного чтения и/или навязывания ложных данных при атаке только на передаваемые данные и взломе методом «грубой силы» путем перебора множества значений ключевого пространства.

При использовании ФКП криптографическая защита данных не обеспечивается. Вместе с тем обеспечивается имитозащита с вероятностью взлома системы КЦИ при однократной попытке подбора ключа $P_{ПС}(FCD) \le \left(C_k^{k_{FCD}}\right)^{-1} \cdot (M!)^{-2}$. Вероятность подбора имитовставки для одного блока данных при однократной попытке $P_{MAC}(FCD) = (M!)^{-1}$. Вместе с тем навязывание ложных данных возможно при изменении бит информационной части, не участвующих в формировании проверочной части. Вероятность этого события $P_{dec}(FCD) = C_{k-k_{FCD}}^{k_{mod}} \Big/ C_k^{k_{mod}}$, где k_{mod} – количество модифицируемых криптоаналитиком бит информационной части.

При использовании ФКНКСс, как и при ФКП, криптографическая защита данных не обеспечивается. Вероятность взлома системы КЦИ на основе ФКНКСс при однократной попытке подбора ключа $P_{ПС}(FCSCs) \le \left(\prod_{i=1}^{N} C_{k-\sum_{j=1}^{i-1} k_{FCD}(j)}^{k_{FCD}(i)} \cdot \left(M(i)!\right)^2 \right)^{-1}$. Вероятность подбора имитовставки для одного блока данных при однократной попытке $P_{MAC}(FCSCs) = \prod_{i=1}^{N} \left(M(i)!\right)^{-1}$.

При использовании ФКНКСн, как и при ФКВД, обеспечивается криптографическая защита данных и не обеспечивается их имитозащита. Вероятность взлома такой системы защиты от несанкционированного чтения методом грубой силы при однократной попытке подбора ключа $P_{UR}(FCSCn) \le \left(\prod_{i=1}^{N} C_{k-\sum_{j=1}^{i-1} k_{FCD}(j)}^{k_{FCD}(i)} \cdot \left(M(i)!\right)^2 \right)^{-1}$.

4. Классификация методов факториального кодирования. В заключение выполним сравнительную оценку всех известных факториальных кодов и их классификацию. Результаты анализа приведем в таблице 1.

Таблица 1

Свойства помехоустойчивых кодов

Код	Систематический	Помехоустойчивый	Криптостойкий	Имитостойкий	Самосинхронизирующийся
ПФК	+	+	-	+	+
КФК	+	+	-	+	-
ФКВД	-	+	+	-	+
ФКП	+	+	-	+	+
ФКНКСс	+	+	-	+	+
ФКНКСн	-	+	+	-	+
CRC	+	+	-	-	-

Представленная классификация и оценка свойств разработанных методов факториального кодирования позволяют определить сферы применения каждого из них.

Выводы. В работе представлены методы факториального кодирования, которые позволяют сократить время формирования кодового слова и объем используемой при этом памяти за счет формирования нескольких контрольных сумм и параллельной обработки поступающих на вход кодека данных. С другой стороны, предложенные методы кодирования позволяют уменьшить требования к вычислительным ресурсам кодека при вычислении перестановок, входящих в состав кодового слова. Вместе с тем, факториальные коды с несколькими контрольными суммами в большинстве случаев уступают в обнаруживающей способности другим факториальным кодам при идентичных длине кодового слова и скорости кода.

Список использованной литературы:

1. *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 [Електронний ресурс]. – Режим доступу : http://jrnl.nau.edu.ua/index.php/ZI/article/view/334/8755.
2. *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.
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 [Електронний ресурс]. – Режим доступу : http://www.csit.narod.ru/ric/riu_2016_3.pdf, doi:10.15588/1607-3274-2016-3-10.
4. Пат. 107655 Україна, МПК G06F 21/64 (2013.01), H04L 1/16 (2006.01). Спосіб контролю цілісності інформації / *В.М. Рудницький, Е.В. Фауре, В.В. Швидкий, А.І. Щерба* ; заявник та патентовласник ЧДТУ. – № a201505937 ; заявл. 16.06.2015; опубл. 24.06.2016. – Бюл. № 12.
5. Пат. 107657 Україна, МПК H03M 13/09 (2006.01), H04K 1/06 (2006.01), G09C 1/06 (2006.01). Спосіб комбінованого кодування інформації / *В.М. Рудницький, Е.В. Фауре, В.В. Швидкий, А.І. Щерба* ; заявник та патентовласник ЧДТУ. – № a201508148 ; заявл. 17.08.2015; опубл. 24.06.2016. – Бюл. № 12.
6. *Фауре Э.В.* Факториальное кодирование с восстановлением данных / *Э.В. Фауре* // Вісник Черкаського дер. технол. ун-ту. – 2016. – № 2. – С. 33–39.
7. *Фауре Э.В.* Метод повышения эффективности факториального кодирования с восстановлением данных / *Э.В. Фауре* // Вісник Черкаського держ. технол. ун-ту. – 2016. – № 3.
8. *Лидл Р.* Конечные поля: В 2 т. / *Р.Лидл, Г.Нидеррайтер* ; пер. с англ. под ред. *Нечаева В.И.* – Т. 2. – М. : Мир, 1988. – 822 с.
9. *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.
10. *Прокис Д.* Цифровая связь / *Дж.Прокис* ; пер. с англ. под ред. *Д.Д. Кловского*. – М. : Радио и связь, 2000. – 800 с.
11. *Теплов Н.Л.* Помехоустойчивость систем передачи дискретной информации / *Н.Л. Теплов*. – М. : Связь, 1964. – 360 с.

References:

1. Faure, E.V., Shvydkyi, V.V. and Shcherba, V.A. (2014), “Metod formirovaniya imitovstavki na osnove perestanovok”, *Zahyst informacii*, Vol. 16, No. 4, pp. 334–340, available at: http://jrnl.nau.edu.ua/index.php/ZI/article/view/334/8755
2. Faure, E.V., Shvydkyi, V.V. and Shcherba, A.I. (2016), “Kontrol tselostnosti informatsii na osnove faktorialnoi sistemy schisleniya”, *Journal of Qafqaz University. Mathematics and computer science*.

3. Faure, E.V., Shvydkyi, V.V. and Shcherba, V.A. (2016), "Kombinirovannoe faktorialnoe kodirovanie i ego svoistva", *Radioelektronika, informatyka, upravlinnja*, No. 3, pp. 80–86, available at: www.csit.narod.ru/ric/riu_2016_3.pdf, doi:10.15588/1607-3274-2016-3-10
4. Rudnytskyi, V.M., Faure, E.V., Shvydkyi, V.V. and Shcherba, A.I. (2016), *Sposib kontrolju cilisnosti informacii*, Patent UA, No. 107655.
5. Rudnytskyi, V.M., Faure, E.V., Shvydkyi, V.V. and Shcherba, A.I. (2016), *Sposib kombinovanogo koduvannja informacii*, Patent UA, No. 107657.
6. Faure, E.V. (2016), "Faktorialnoe kodirovanie s vosstanovleniem dannykh", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universytetu*, No. 2, pp. 33–39.
7. Faure, E.V. (2016), "Metod povysheniya effektivnosti faktorialnogo kodirovaniya s vosstanovleniem dannykh", *Visnyk Cherkaskogo derzhavnogo tehnologichnogo universytetu*, No. 3.
8. Lidl, R. and Niederreiter, H. (1988), *Konechnye polya* [Introduction to finite fields and their applications], translated by Petrov, V.I. and Zhukov, A.E., in Nechaev, V.I. (Ed.), Vol. 2, Mir, Moscow, 822 p.
9. Peterson, W.W. and Weldon-jr., E.J. (1976), *Kody, ispravlyayushchie oshibki* [Error-correcting codes], 2nd ed., translated by Fillippova, L.E., Boyarinov, I.M. and Dynkin, V.N., in Dobrushin, R.L. and Samoylenko, S.I. (Eds.), Mir, Moscow, 590 p.
10. Proakis, J.G. (2000), *Tsifrovaya svyaz* [Digital communications], translated by Klovskiy, D.D. and Nikolaev, B.I., in Klovskiy, D.D. (Ed.), Radio i sviaz, Moscow, 800 p.
11. Teplov, N.L. (1964), *Pomekhoustoychivost sistem peredachi diskretnoy informatsii*, Sviaz, Moscow, 360 p.

ФАУРЕ Еміль Віталійович – кандидат технічних наук, доцент, докторант, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету.

Наукові інтереси:

– дослідження моделей, методів і засобів формування псевдовипадкових послідовностей чисел;

– дослідження і розробка методів і засобів криптографічного перетворення інформації;

– дослідження кодових і некодових методів підвищення достовірності переданих даних.

Тел.: (097) 913–20–66.

E-mail: faureemil@gmail.com.

Стаття надійшла до редакції 02.09.2016.