УДК 621.391

В.Н. Рудницкий, И.В. Миронец, В.В. Веретельник

Черкасский государственный технологический университет, Черкассы

ОПЕРАЦИИ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ В ДВОИЧНО-ЧЕТВЕРИЧНОЙ СИСТЕМЕ СЧИСЛЕНИЯ

Данная статья посвящена разработке системы контроля ошибок в процессе криптографического перекодирования информации на основании двухразрядных логических функций. Так как синтезированные 2r-системы счисления с постоянным числом единиц являются арифметическими, причем обладают одномерным весовым рядом, а также имеют большую вероятность обнаружения ошибок при значительной простоте устройства контроля информации, следовательно, их можно считать перспективными для применения в специализированных вычислительных системах и системах управления.

Ключевые слова: *криптографическое перекодирования, системы счисления, обнаружения ошибок, устройство контроля информации.*

Введение

Постановка проблемы. Задача обеспечения надежного функционирования сложных вычислительных систем приобретает в настоящее время первостепенное значение. Это объясняется увеличением парка вычислительных машин, расширением сферы их применения и важностью решаемых с их помощью задач. Кроме того, расширяются области применения ЭВМ, в которых техническое обслуживание затруднено либо совсем исключено, и поэтому обеспечение их правильного функционирования при наличии неисправностей является главным и обязательным требованием [1].

Развитие средств вычислительной техники сопровождается ростом производительности вычислительных машин, усложнением их конструкции и расширением области применения. Это обуславливает постоянный интерес к проблеме повышения надежности работы. Решение данной задачи практически всегда предполагает введение избыточности. Среди многообразия форм введения избыточности все больший вес приобретают методы помехоустойчивого кодирования, позволяющие обнаруживать ошибки при передаче, хранении и обработке информации [2].

Традиционно «неудобными» для помехоустойчивого кодирования оставались узлы управления ЭВМ, обладающие нерегулярной структурой. Для обнаружения и исправления ошибок в исполнительных устройствах были созданы специальные коды, которые принято называть арифметическими, потому что они предназначены для обнаружения ошибок при выполнении арифметических операций.

Однако эти коды создавались в большей степени интуитивно. Поэтому большой интерес вызывает анализ методов синтеза кодов, корректирующих ошибки, и разработка методов синтеза арифметических кодов [3].

Анализ публикаций и исследований. В настоящее время в связи со значительным ростом объемов информации и скоростями ее переработки, а также высокими требованиями к достоверности результатов работы и качеству управления, поддержание высокой надежности может быть достигнуто только полной автоматизацией процесса контроля информации. Более того, подвижный характер специализированных вычислительных систем, их удаленность от стационарных баз технического обслуживания и ремонта делают недоступными другие виды повышения надежности, кроме введения избыточности [4, 5]. Еще в большей мере это относится к необслуживаемой аппаратуре, которая обязана непрерывно функционировать в течение многих лет. Поэтому наиболее рациональным и практически единственным путем повышения надежности является введение избыточности, позволяющей своевременно обнаруживать возникающие ошибки и обеспечивать их дальнейшее устранение.

Проблема обеспечения высокой надежности является одной из центральных, о чем свидетельствует значительная вводимая избыточность. Однако вводимая избыточность вступает в противоречие с быстродействием и сложностью, что, в конечном счете, сказывается на самой надежности. Методология разработанного научного направления состоит из введения избыточности на этапе синтеза первичной системы счисления, при этом исключается реальное выражение контрольных компонент. Применение такой избыточности имеет менее негативные последствия [6, 7]. В качестве избыточных систем счисления А.П. Стахов выбрал и обобщил известные ранее коды Фибоначчи и золотой пропорции [8]. Предложенные Е.И. Брюховичем так называемые позиционные счисления практическое применение имеют только к многозначным структурам, и поэтому на данном этапе развития технологии распространения не получили [9].

Органичным продолжением и обобщением работ А.П. Стахова можно считать работы А.В. Ткаченко, посвященные теории синтеза структурных кодов [10]. Разработаны принципы и методы кодирования, декодирования и выполнения арифметических операций в структурных кодах. Однако полученные системы счисления не обладают гарантированным обнаружением ошибок.

Целью данной работы является разработка системы контроля ошибок в процессе криптографического перекодирования информации на основе двухразрядных логических функций.

Основной материал

На практике вводимая информационная избыточность преследует цели повышения надежности, помехозащищенности и отказоустойчивости функционально автономных устройств. Вместе с тем был бы идеальным случай представить всю информацию одним избыточным кодом, обеспечивающим единство процессов обнаружения и исправления ошибок на всех этапах переработки информации. Эффективность любого применяемого кода определяется, прежде всего, соответствием его реальной модели ошибок. Внутриаппаратные тракты характеризуются асимметрией ошибок. Коды с постоянным числом единиц обнаруживают все асимметричные ошибки с учетом редко возникающих пакетов ассиметричных ошибок [11].

Любое число X может быть представлено в виде

$$X = \pm\sum_{i=0}^{n-1} x_i \times 2^1, \qquad x \in [0;1]. \tag{1}$$

Такое представление называется однородной двоичной позиционной системой счисления (безизбыточной) с естественным следованием весов. На основе данной системы счисления методом перебора можно синтезировать коды с постоянным числом единиц [12]. Для этого алгоритм перебора определим как последовательность выборки кодовых слов из безизбыточного кода, а в качестве ограничения на выборку – постоянное число единиц. Данное ограничение на основе выражения (1) может быть определено

$$a = \sum_{i=0}^{n-1} x_i = \text{const}. \tag{2}$$

Применив метод перебора с ограничением (2), получим коды с постоянным числом единиц в явном виде для разных a.

Рассмотрим представление числа X в кодах с постоянным числом единиц для любого a.

Любое число X может быть представлено кодом с постоянным числом единиц следующим образом:

$$X = \pm\sum_{j=0}^{a-1}\sum_{i=0}^{n-1} X_i^{j+1} \cdot C_{i-j}^{j+1}, \quad x \in [0;1], \quad a < n. \tag{3}$$

Выражение (3) дает основание полагать, что все коды с постоянным количеством единиц являются весозначными, следовательно, они являются системами счисления, над которыми можно выполнять арифметические операции.

Единственной системой счисления с постоянным числом единиц, которой может быть отдано предпочтение, является система счисления при a=1. Однако ее применение в явном виде не представляется возможным из-за большой избыточности.

Любое число X в данных системах счисления может быть представлено в виде слов

$$X = \pm\left(x_{n-1}, x_{n-2}, ..., x_1, x_0\right),$$

где

$$X = \pm\sum_{i=0}^{n-1} x_i r^i, \qquad 0 \le x \le r-1. \tag{4}$$

Представление данного числа в виде двоичных слов будем называть двоично-*r*-ичной позиционной системой счисления (*2r*).

Любое целое число X может быть представлено *2r* кодом в следующем виде:

$$X = \pm\sum_{j=0}^{n-1}\sum_{i=0}^{r-1} x_{r\cdot i+j} i r^i, \qquad x \in [0;1]. \tag{5}$$

Выражение (5) позволяет сделать вывод, что любой *2r* код с постоянным числом единиц при a=1 является весозначным с одномерным весовым рядом.

Следовательно, данные коды можно рассматривать как системы счисления.

В ряде работ [13, 14] показано, что применительно к средствам вычислительной техники наиболее эффективно использовать системы счисления при r=4, так как она обеспечивает наибольшую вероятность безотказной работы аппаратных средств. Данная система счисления получила название двоично-четверичной системы счисления с постоянным числом единиц.

Любое целое число X может быть представлено в двоично-четверичной системе счисления:

$$X = \pm\sum_{j=0}^{n-1}\sum_{i=0}^{3} x_{4i+j} \cdot i \cdot 4^i, \quad x \in [0;1]. \tag{6}$$

Коды цифр в двоично-четверичной системе счисления представлены в табл. 1.

Синтезированные системы счисления с постоянным числом единиц являются частным случаем кодов с постоянным числом единиц, поэтому они предназначены для обнаружения ошибок в каналах передачи, хранения и обнаружения информации.

Так как весовой ряд *2r* системы счисления можно условно разбить на блоки по r-разрядов в каждом блоке, и представленное любое число может иметь только одну единицу в каждом блоке разрядов, следовательно, устройство обнаружения ошибок будет иметь общий вид:

$$F = \overline{F_1} \vee \overline{F_2} \vee ... \vee \overline{F_k} \vee ... \vee \overline{F_n}, \quad k \in [1; n], \qquad (7)$$

где

$$\overline{F_k} = C_1\overline{C_2}\overline{C_3}...\overline{C_r} \vee \overline{C_1}C_2\overline{C_3}...\overline{C_r} \vee ... \vee \overline{C_1}\overline{C_2},$$

C_i – i -й вход устройства контроля $i \in [1; r]$.

Таблица 1

Коды цифр в двоично-четверичной системе

Значение разряда								**Число**
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	
0	0	0	1	0	0	0	1	**0**
0	0	0	1	0	0	1	0	**1**
0	0	0	1	0	1	0	0	**2**
0	0	0	1	1	0	0	0	**3**
0	0	1	0	0	0	0	1	**4**
0	0	1	0	0	0	1	0	**5**
0	0	1	0	0	1	0	0	**6**
0	0	1	0	1	0	0	0	**7**
0	1	0	0	0	0	0	1	**8**
0	1	0	0	0	0	1	0	**9**
0	1	0	0	0	1	0	0	**10**
0	1	0	0	1	0	0	0	**11**
1	0	0	0	0	0	0	1	**12**
1	0	0	0	0	0	1	0	**13**
1	0	0	0	0	1	0	0	**14**
1	0	0	0	1	0	0	0	**15**
12	**8**	**4**	**0**	**3**	**2**	**1**	**0**	

Так как синтезированные *2r* системы счисления с постоянным числом единиц являются арифметическими, причем обладают одномерным весовым рядом, а также имеют большую вероятность обнаружения ошибок при значительной простоте устройства контроля информации, следовательно, их можно считать перспективными для применения в специализированных вычислительных системах и системах управления.

На основании разработанной двоично-четверичной системы счисления, для 24 исследованных логических функций кодирования-декодирования в двоичной системе [15, 16] были получены соответствующие функции кодирования и декодирования:

– если функция кодирования-декодирования в двоичной системе совпадает (слева), то и в разработанной двоично-четверичной системе тоже совпадает (справа):

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \vec{F}_1^{2/4} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix};$$

$$\vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} \to \vec{F}_2^{2/4} = \begin{pmatrix} x_1 \\ x_3 \\ x_2 \\ x_4 \end{pmatrix};$$

$$\vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_3^{2/4} = \begin{pmatrix} x_3 \\ x_4 \\ x_1 \\ x_2 \end{pmatrix};$$

$$\vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_4^{2/4} = \begin{pmatrix} x_2 \\ x_1 \\ x_4 \\ x_3 \end{pmatrix};$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix} \to \vec{F}_5^{2/4} = \begin{pmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \end{pmatrix};$$

$$\vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_6^{2/4} = \begin{pmatrix} x_4 \\ x_2 \\ x_3 \\ x_1 \end{pmatrix};$$

$$\vec{F}_9 = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix} \to \vec{F}_9^{2/4} = \begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_4 \end{pmatrix};$$

$$\vec{F}_{14} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{pmatrix} \to \vec{F}_{14}^{2/4} = \begin{pmatrix} x_1 \\ x_4 \\ x_3 \\ x_2 \end{pmatrix};$$

$$\vec{F}_{17} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix} \to \vec{F}_{17}^{2/4} = \begin{pmatrix} x_2 \\ x_1 \\ x_3 \\ x_4 \end{pmatrix};$$

$$\vec{F}_{21} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix} \to \vec{F}_{21}^{2/4} = \begin{pmatrix} x_1 \\ x_2 \\ x_4 \\ x_3 \end{pmatrix}.$$

– если функция кодирования-декодирования в двоичной системе не совпадает (слева, причем 1 после точки в индексе функции обозначает функцию кодирования, 2 – функцию декодирования), то и в разработанной двоично-четверичной системе тоже не совпадает (справа):

$$\vec{F}_{7.1} = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix} \to \vec{F}_{7.1}^{2/4} = \begin{pmatrix} x_3 \\ x_1 \\ x_4 \\ x_2 \end{pmatrix};$$

$$\vec{F}_{7.2} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix} \to \vec{F}_{7.2}^{2/4} = \begin{pmatrix} x_2 \\ x_4 \\ x_1 \\ x_3 \end{pmatrix};$$

$$\vec{F}_{8.1}=\begin{pmatrix}x_2\oplus 1\\ x_1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{8.1}=\begin{pmatrix}x_2\\ x_4\\ x_1\\ x_3\end{pmatrix};$$

$$\vec{F}_{8.2}=\begin{pmatrix}x_2\\ x_1\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{8.2}=\begin{pmatrix}x_3\\ x_1\\ x_4\\ x_2\end{pmatrix};$$

$$\vec{F}_{10.1}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\rightarrow \vec{F}^{2/4}_{10.1}=\begin{pmatrix}x_3\\ x_1\\ x_2\\ x_4\end{pmatrix};$$

$$\vec{F}_{10.2}=\begin{pmatrix}x_1\oplus x_2\\ x_1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{10.2}\begin{pmatrix}x_2\\ x_3\\ x_1\\ x_4\end{pmatrix};$$

$$\vec{F}_{11.1}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{11.1}=\begin{pmatrix}x_4\\ x_1\\ x_2\\ x_3\end{pmatrix};$$

$$\vec{F}_{11.2}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{11.2}=\begin{pmatrix}x_2\\ x_3\\ x_4\\ x_1\end{pmatrix};$$

$$\vec{F}_{12.1}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{12.1}=\begin{pmatrix}x_4\\ x_2\\ x_1\\ x_3\end{pmatrix};$$

$$\vec{F}_{12.2}=\begin{pmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{12.2}=\begin{pmatrix}x_3\\ x_2\\ x_4\\ x_1\end{pmatrix};$$

$$\vec{F}_{13.1}=\begin{pmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{13.1}=\begin{pmatrix}x_2\\ x_3\\ x_4\\ x_1\end{pmatrix};$$

$$\vec{F}_{13.2}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{13.2}=\begin{pmatrix}x_4\\ x_1\\ x_2\\ x_3\end{pmatrix};$$

$$\vec{F}_{15.1}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{15.1}=\begin{pmatrix}x_1\\ x_3\\ x_4\\ x_2\end{pmatrix};$$

$$\vec{F}_{15.2}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{15.2}=\begin{pmatrix}x_1\\ x_4\\ x_2\\ x_3\end{pmatrix};$$

$$\vec{F}_{16.1}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\rightarrow \vec{F}^{2/4}_{16.1}=\begin{pmatrix}x_2\\ x_4\\ x_3\\ x_1\end{pmatrix};$$

$$\vec{F}_{16.2}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{16.2}=\begin{pmatrix}x_4\\ x_1\\ x_3\\ x_2\end{pmatrix};$$

$$\vec{F}_{18.1}=\begin{pmatrix}x_1\oplus x_2\\ x_1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{18.1}=\begin{pmatrix}x_2\\ x_3\\ x_1\\ x_4\end{pmatrix};$$

$$\vec{F}_{18.2}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\rightarrow \vec{F}^{2/4}_{18.2}=\begin{pmatrix}x_3\\ x_1\\ x_2\\ x_4\end{pmatrix};$$

$$\vec{F}_{19.1}=\begin{pmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{19.1}=\begin{pmatrix}x_4\\ x_3\\ x_1\\ x_2\end{pmatrix};$$

$$\vec{F}_{19.2}=\begin{pmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{pmatrix}\rightarrow \vec{F}^{2/4}_{19.2}=\begin{pmatrix}x_3\\ x_4\\ x_2\\ x_1\end{pmatrix};$$

$$\vec{F}_{20.1}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{20.1}=\begin{pmatrix}x_4\\ x_1\\ x_3\\ x_2\end{pmatrix};$$

$$\vec{F}_{20.2}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\rightarrow \vec{F}^{2/4}_{20.2}=\begin{pmatrix}x_2\\ x_4\\ x_3\\ x_1\end{pmatrix};$$

$$\vec{F}_{22.1}=\begin{pmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{pmatrix}\rightarrow \vec{F}^{2/4}_{22.1}=\begin{pmatrix}x_3\\ x_4\\ x_2\\ x_1\end{pmatrix};$$

$$\vec{F}_{22.2}=\begin{pmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\rightarrow \vec{F}^{2/4}_{22.2}=\begin{pmatrix}x_4\\ x_3\\ x_1\\ x_2\end{pmatrix};$$

$$\vec{F}_{23.1} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{pmatrix} \rightarrow \vec{F}_{23.1}^{2/4} = \begin{pmatrix} x_3 \\ x_2 \\ x_4 \\ x_1 \end{pmatrix};$$

$$\vec{F}_{23.2} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix} \rightarrow \vec{F}_{23.2}^{2/4} = \begin{pmatrix} x_4 \\ x_2 \\ x_1 \\ x_3 \end{pmatrix};$$

$$\vec{F}_{24.1} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{pmatrix} \rightarrow \vec{F}_{24.1}^{2/4} = \begin{pmatrix} x_1 \\ x_4 \\ x_2 \\ x_3 \end{pmatrix};$$

$$\vec{F}_{24.2} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix} \rightarrow \vec{F}_{24.2}^{2/4} = \begin{pmatrix} x_1 \\ x_3 \\ x_4 \\ x_2 \end{pmatrix}.$$

Анализируя полученные функции кодирования-декодирования в двоично-четверичной системе счисления, можем сделать вывод, что все кодирование сводится к перестановке разрядов.

Выводы

Приведенные результаты свидетельствуют, что для всех двухразрядных операций криптографического преобразования информации получены операции кодирования-декодирования в двоично-четверичной системе счисления.

Синтезированные аналоги операций кодирования-декодирования для двоично-четверичной системы счисления представляют собой перестановку четырех разрядов. Данный результат подтверждает гипотезу о том, что группа двухразрядных операций криптографического преобразования являет собой алгебраическую группу G_4 -перестановок. Причем, предложенные математические модели операций кодирования и декодирования могут быть использованы для повышения достоверности передачи конфиденциальной информации по каналам связи.

Список литературы

1. Согомонян Б.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы / Б.С. Согомонян, Е.В. Слабаков. – М.: Радио и связь, 1989. – 208 с.

2. Дадаев Ю.Г. Теория арифметических кодов / Ю.Г. Дадаев. – М.: Радио и связь, 1981.

3. Рудницкий В.Н. Исследование методов синтеза структурных кодов / В.Н. Рудницкий, Н.Н. Пантелеева // Электроника и связь. – 2003. – №18. – С. 62-64.

4. Жильцов Е.И. Диагностирование приборов информационно-управляющих систем / Е.И. Жильцов, И.И. Васильев, В.А. Монастырецкий // Измерительная техника. – 1993. – №5. – С. 23-24.

5. Крючков А.В. Повышение надежности цифровых измерительных приборов / А.В. Крючков, В.Н. Рудницкий, А.В. Скобеев // Тез. докл. НТК. – Краснодар: КГМУ, 1997. – С. 83.

6. Научно-исследовательская работа по х/д N285: отчет N 14 / МО СССР. Руководитель работы В.И. Ключко. – Краснодар, 1986. – С. 137.

7. Кузьмин И.В. Аппаратный контроль электронных цифровых вычислительных машин / И.В. Кузьмин, Р.Г. Бурназян, А.А. Ковергин. – М.: Энергия, 1974. – 74 с.

8. Стахов А.П. Коды золотой пропорции / А.П. Стахов. – М.: Радио и связь, 1984. – 152 с.

9. Брюхович Е.И. Экстремальная эффективность аппаратного контроля ЭВМ и принципиальные возможности ее достижения на основе естественной избыточности позиционных счислений / Е.И. Брюхович // УСиМ. – 1979. – № 6. – С. 83-86.

10. Ткаченко А.С. Теория синтеза структурных кодов и отказоустойчивых систем на их основе / А.С. Ткаченко. – МО России, 1993.

11. Злотник Б.М. Помехоустойчивые коды в системах связи / Б.М. Злотник. – М.: Радио и связь, 1989.

12. Киносита К. Логическое проектирование СБИС - U. / К. Киносита, К. Асада, О. Карацу. – М.: Мир, 1988.

13. Рудницький В.М. Синтез елементів пристроїв криптографічного захисту інформації в системах числення з постійною кількістю одиниць / В.М. Рудницький // Вісник ЧДТУ: Наукові праці ЧДТУ. – 2004. – № 3. – С. 96-100.

14. Рудницкий В.Н. Обобщенные результаты исследования структурных кодов с ограниченной серией символов / В.Н. Рудницкий, Н.Н. Пантелеева, О.В. Нечипоренко // Вістник КДПУ. – Кременчуг: КДПУ, 2003. – № 2 (19). – С. 38-40.

15. Бабенко В.Г. Метод підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій: Дис. ... канд. техн. наук: 05.13.21 / Бабенко Віра Григорівна. – Черкаси, 2009. – 166 с.

16. Миронець І.В. Метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів: Дис. ... канд. техн. наук: 05.13.05 / Миронець Ірина Валеріївна. – Черкаси, 2011. – 157 с.

Поступила в редколлегию 7.03.2012

Рецензент: д-р техн. наук, проф. И.В. Шостак, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ОПЕРАЦІЇ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ В ДВІЙКОВО-ЧЕТВІРКОВІЙ СИСТЕМІ ЧИСЛЕННЯ

В.М. Рудницький, І.В. Миронець, В.В. Веретельник

Дана стаття присвячена розробці системи контролю помилок в процесі криптографічного перекодування інформації на основі дворозрядних логічних функцій. Оскільки, синтезовані 2r-системи числення з постійним числом одиниць є арифметичними, причому мають одновимірний ваговий ряд, а також мають велику ймовірність виявлення помилок при значній простоті пристрою контролю інформації, тому їх можна вважати перспективними для застосування в спеціалізованих обчислювальних системах і системах управління.

Ключові слова: *криптографічне перекодування, системи числення, виявлення помилок, пристрій контролю інформації.*

THE OPERATIONS OF CRYPTOGRAPHIC TRANSFORMATION OF INFORMATION AT BINARY-QUATERNARY NUMBER SYSTEM

V.N. Rudnitsky, I.V. Mironets, V.V. Veretelnik

This article focuses on the development of control system of errors in cryptographic transcoding of information on the basis of double-bit logic functions. Since the synthesized 2r-number system with a constant number of units are arithmetic, and have a number of one-dimensional weight and are more likely to detect errors in a large simplicity of the information control device, so they can be considered promising for use in specialized computer systems and control systems.

Keywords*: cryptographic transcoding, number systems, error detection, the information control device.*