УДК 621.391

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

Черкасский государственный технологический университет, Черкассы

МЕТОД КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ ИНФОРМАЦИИ С ВВЕДЕНИЕМ ИНФОРМАЦИОННОЙ ИЗБЫТОЧНОСТИ НА ОСНОВЕ ДВУХРАЗРЯДНЫХ ЛОГИЧЕСКИХ ФУНКЦИЙ

Данная статья посвящена разработке метода криптографического кодирования информации с введением информационной избыточности на основе двухразрядных логических функций. Традиционно задачи передачи конфиденциальной информации в избыточных системах решаются двумя путями: введение информационной избыточности с последующим криптографическим преобразованием или криптографическое преобразование с последующим введением информационной избыточности, тогда для уменьшения сложности программно-аппаратной части системы, а также уменьшения времени получения информации целесообразным есть совмещение процесса введения избыточности с криптографическим преобразованием.

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

Введение

Постановка проблемы. Развитие современной технологии характеризуется внедрением вычислительной техники и электроники во все сферы человеческой деятельности.

Увеличение сложности и важности выполняемых задач привело к совершенствованию основных показателей цифровых устройств вычислительной техники, производительности, надежности, устойчивости к сбоям и т.п.

В основе современной электронной вычислительной техники лежат числа и системы счисления, которые эти числа порождают. От эффективности последних зависят параметры вычислительных систем и устройств, в первую очередь показатели быстродействия и надежности.

В процессе хранения данных и передачи информации в компьютерных системах и сетях неизбежно возникают ошибки. Контроль целостности данных и исправление ошибок – важная задача на многих уровнях работы с информацией.

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 цифровых устройств.

Решение данной задачи предполагает введение избыточности, а среди многообразия форм ввода избыточности все большее внимание приобретают методы помехоустойчивого кодирования, что позволяет контролировать ошибки при передаче, хранении и обработке информации [1].

Анализ публикаций и исследований. В компьютерных системах и сетях возможны три стратегии борьбы с ошибками:

– выявления ошибок в блоках данных и автоматический запрос повторной передачи поврежденных блоков;

– выявления ошибок в блоках данных и отбрасывание поврежденных блоков – такой подход иногда применяется в системах потокового мультимедиа, где важна задержка передачи и нет времени на повторную передачу;

– исправления ошибок (прямая коррекции) применяемое на физическом уровне.

Коды, контролирующие ошибки, используются для обнаружения ошибок, возникающих при передаче информации под влиянием помех, а также при ее хранении. Для этого при передаче в полезные данные добавляют специальным образом структурированную избыточную информацию (контрольное число), а при чтении этих данных ее используют для того, чтобы выявить ошибку. Естественно, что число ошибок, которое можно исправить, ограничено и зависит от конкретного применяемого кода.

В действительности, коды обнаружения ошибок принадлежат к тем же классам кодов, что и коды, корректирующие ошибки. Фактически, любой код, корректирующий ошибки, может быть также использован для контроля ошибок.

Для обнаружения и исправления ошибок в цифровых исполнительных устройствах были созданы специальные коды, которые принято называть арифметическими, потому что они предназначены для контроля ошибок при выполнении арифметических операций. Однако эти коды создавались в большей степени интуитивно, поэтому ученых очень заинтересовал анализ методов синтеза кодов, контролирующих ошибки, и, непосредственно, сама разработка методов синтеза арифметических кодов [2].

В настоящее время отсутствуют систематизированные данные о влиянии позиционных избыточ-

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

ных систем счисления на сложность реализации арифметических операций, построенных на основе моделей систем счисления разрядности больше трех. Данная информация необходима для целенаправленного проведения исследований по двум направлениям [3]:

– повышение надежности арифметических устройств вычислительной техники за счет уменьшения их сложности на основе введения избыточности;

– повышение быстродействия арифметических устройств на основе введения избыточности.

Целью данной работы является разработка метода криптографического кодирования информации с введением информационной избыточности на основе двухразрядных логических функций.

Основной материал

Задача анализа форм представления информации заключается в выборе форм представления обеспечивающих минимальную сложность арифметических устройств, при заданном быстродействии. Формы представления информации, требующие наименьшей аппаратной сложности устройства, обеспечат наиболее простые алгоритмы его функционирования.

Проведем исследование результатов моделирования арифметических устройств для определения кодов цифр, наиболее перспективных для дальнейшего исследования и синтеза систем счисления с оптимальной информационной избыточностью.

На основе проведения вычислительного эксперимента были получены модели позиционных избыточных системах счисления.

Выбор системы счисления для применения - важный практический вопрос, поскольку от его решения зависят такие характеристики как быстродействие, сложность, надежность, отказоустойчивость и т.д. [4]

В ряде работ [5, 6] показано, что устройства взаимного преобразования кодов, для кодированных систем счисления будут наименее сложными при кодировании группой разрядов количества цифр соответствующих степени числа 2.

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

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

При исследовании систем счисления и разработке избыточных арифметических устройств значительно проще использовать не представление числа в системе счисления, а модель системы счисления. Двоично-четверичная система счисления с постоянным числом единиц заданная выражением (1) определяется моделью $M_{1,2,4,8}^{3,2,1,0}$, явный вид которой представлен в табл. 1.

На практике в информационных базах данных информация представлена безизбыточным кодом, но обеспечение достоверности передачи информации требует введения избыточности.

Таблица 1

Идентификация модели двоично-четверичной системы счисления с постоянным числом единиц

Код числа				**Код цифры**	**Кодируемое число**	**Обозначение модели**
0	0	0	1	**1**	**0**	$M_{1,2,4,8}^{3,2,1,0}$
0	0	1	0	**2**	**1**	
0	1	0	0	**4**	**2**	
1	0	0	0	**8**	**3**	
3	**2**	**1**	**0**	Весовой коэффициент разряда модели		

Традиционно задачи передачи конфиденциальной информации в избыточных системах решаются двумя путями:

1) введение информационной избыточности с последующим криптографическим преобразованием;

2) криптографическое преобразование с последующим введением информационной избыточности.

Для уменьшения сложности программно-аппаратной части системы, а также уменьшения времени получения информации было бы целесообразно совместить процесс введения избыточности с криптографическим преобразованием.

Поскольку синтезированные 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 [7, 8] были получены соответствующие функции кодирования и декодирования с введением избыточности (причем верхний индекс функции обозначает принадлежность к двоично-четверичной системе счисления, а в нижнем индексе – 1 после точки обозначает функцию кодирования, 2 – функцию декодирования).

Таким образом, функции кодирования имеют следующий вид:

$$\vec{F}_1=\begin{pmatrix}x_1\\x_2\end{pmatrix}\to\vec{F}_1^{2/4}=\begin{pmatrix}x_1\cdot x_2\\x_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_9=\begin{pmatrix}x_1\oplus x_2\\x_2\end{pmatrix}\to\vec{F}_9^{2/4}=\begin{pmatrix}\overline{x}_1\cdot x_2\\x_1\cdot\overline{x}_2\\x_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_{17}=\begin{pmatrix}x_1\\x_1\oplus x_2\end{pmatrix}\to\vec{F}_{17}^{2/4}=\begin{pmatrix}x_1\cdot\overline{x}_2\\x_1\cdot x_2\\\overline{x}_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\end{pmatrix};$$

$$\vec{F}_2=\begin{pmatrix}x_2\\x_1\end{pmatrix}\to\vec{F}_2^{2/4}=\begin{pmatrix}x_1\cdot x_2\\\overline{x}_1\cdot x_2\\x_1\cdot\overline{x}_2\\\overline{x}_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_{10.1}=\begin{pmatrix}x_2\\x_1\oplus x_2\end{pmatrix}\to F_{10}^{2/4}=\begin{pmatrix}\overline{x}_1\cdot x_2\\x_1\cdot x_2\\x_1\cdot\overline{x}_2\\\overline{x}_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_{18.1}=\begin{pmatrix}x_1\oplus x_2\\x_1\end{pmatrix}\to\vec{F}_{18}^{2/4}=\begin{pmatrix}x_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\\x_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\end{pmatrix};$$

$$\vec{F}_3=\begin{pmatrix}x_1\oplus 1\\x_2\end{pmatrix}\to\vec{F}_3^{2/4}=\begin{pmatrix}\overline{x}_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\\x_1\cdot x_2\\x_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_{11.1}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{pmatrix}\to\vec{F}_{11}^{2/4}=\begin{pmatrix}\overline{x}_1\cdot\overline{x}_2\\x_1\cdot x_2\\x_1\cdot\overline{x}_2\\\overline{x}_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_{19.1}=\begin{pmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{pmatrix}\to\vec{F}_{19}^{2/4}=\begin{pmatrix}\overline{x}_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\\x_1\cdot x_2\\x_1\cdot\overline{x}_2\end{pmatrix};$$

$$\vec{F}_4=\begin{pmatrix}x_1\\x_2\oplus 1\end{pmatrix}\to\vec{F}_4^{2/4}=\begin{pmatrix}x_1\cdot\overline{x}_2\\x_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\end{pmatrix};\qquad \vec{F}_{12.1}=\begin{pmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{pmatrix}\to\vec{F}_{12}^{2/4}=\begin{pmatrix}\overline{x}_1\cdot\overline{x}_2\\x_1\cdot\overline{x}_2\\x_1\cdot x_2\\\overline{x}_1\cdot x_2\end{pmatrix};\qquad \vec{F}_{20.1}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{pmatrix}\to\vec{F}_{20}^{2/4}=\begin{pmatrix}\overline{x}_1\cdot\overline{x}_2\\x_1\cdot x_2\\\overline{x}_1\cdot x_2\\x_1\cdot\overline{x}_2\end{pmatrix};$$

$$\vec{F}_5=\begin{pmatrix}x_1\oplus 1\\x_2\oplus 1\end{pmatrix}\to\vec{F}_5^{2/4}=\begin{pmatrix}\overline{x}_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\\x_1\cdot\overline{x}_2\\x_1\cdot x_2\end{pmatrix};\qquad \vec{F}_{13.1}=\begin{pmatrix}x_1\oplus x_2\\x_2\oplus 1\end{pmatrix}\to\vec{F}_{13}^{2/4}=\begin{pmatrix}x_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\\x_1\cdot x_2\end{pmatrix};\qquad \vec{F}_{21}=\begin{pmatrix}x_1\\x_1\oplus x_2\oplus 1\end{pmatrix}\to\vec{F}_{21}^{2/4}=\begin{pmatrix}x_1\cdot x_2\\x_1\cdot\overline{x}_2\\\overline{x}_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\end{pmatrix};$$

$$\vec{F}_6=\begin{pmatrix}x_2\oplus 1\\x_1\oplus 1\end{pmatrix}\to\vec{F}_6^{2/4}=\begin{pmatrix}\overline{x}_1\cdot\overline{x}_2\\x_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\\x_1\cdot x_2\end{pmatrix};\qquad \vec{F}_{14}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_2\end{pmatrix}\to\vec{F}_{14}^{2/4}=\begin{pmatrix}x_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\\x_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_{22.1}\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1\oplus 1\\x_1\oplus x_2\end{pmatrix}\to\vec{F}_{22}^{2/4}=\begin{pmatrix}\overline{x}_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\\x_1\cdot\overline{x}_2\\x_1\cdot x_2\end{pmatrix};$$

$$\vec{F}_{7.1}=\begin{pmatrix}x_2\\x_1\oplus 1\end{pmatrix}\to\vec{F}_7^{2/4}=\begin{pmatrix}\overline{x}_1\cdot x_2\\x_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\\x_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_{15.1}=\begin{pmatrix}x_2\\x_1\oplus x_2\oplus 1\end{pmatrix}\to\vec{F}_{15}^{2/4}=\begin{pmatrix}x_1\cdot x_2\\\overline{x}_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\\x_1\cdot\overline{\overline{x}}_2\end{pmatrix};\qquad \vec{F}_{23.1}=\begin{pmatrix}x_1\oplus x_2\\x_1\oplus 1\end{pmatrix}\to\vec{F}_{23}^{2/4}=\begin{pmatrix}\overline{x}_1\cdot x_2\\x_1\cdot\overline{x}_2\\\overline{x}_1\cdot\overline{x}_2\\x_1\cdot x_2\end{pmatrix};$$

$$\vec{F}_{8.1}=\begin{pmatrix}x_2\oplus 1\\x_1\end{pmatrix}\to\vec{F}_8^{2/4}=\begin{pmatrix}\overline{x}_1\cdot x_2\\\overline{x}_1\cdot\overline{x}_2\\x_1\cdot x_2\\x_1\cdot\overline{x}_2\end{pmatrix};\qquad \vec{F}_{16.1}=\begin{pmatrix}x_2\oplus 1\\x_1\oplus x_2\end{pmatrix}\to\vec{F}_{16}^{2/4}=\begin{pmatrix}x_1\cdot\overline{x}_2\\\overline{x}_1\cdot\overline{x}_2\\\overline{x}_1\cdot x_2\\x_1\cdot x_2\end{pmatrix};\qquad \vec{F}_{24.1}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_1\end{pmatrix}\to\vec{F}_{24}^{2/4}=\begin{pmatrix}x_1\cdot x_2\\\overline{x}_1\cdot x_2\\x_1\cdot\overline{x}_2\\\overline{x}_1\cdot\overline{x}_2\end{pmatrix}.$$

А функции декодирования, относительно, имеют вид:

$$\vec{F}_1=\begin{pmatrix}x_1\\x_2\end{pmatrix}\to\vec{F}_1^{2/4}=\begin{pmatrix}x_1\vee x_2\\x_1\vee x_3\end{pmatrix};\qquad \vec{F}_6=\begin{pmatrix}x_2\oplus 1\\x_1\oplus 1\end{pmatrix}\to\vec{F}_6^{2/4}=\begin{pmatrix}x_2\vee x_4\\x_3\vee x_4\end{pmatrix};\qquad \vec{F}_{11.2}=\begin{pmatrix}x_1\oplus x_2\\x_2\oplus 1\end{pmatrix}\to\vec{F}_{11}^{2/4}=\begin{pmatrix}x_2\vee x_3\\x_2\vee x_4\end{pmatrix};$$

$$\vec{F}_2=\begin{pmatrix}x_2\\x_1\end{pmatrix}\to\vec{F}_2^{2/4}=\begin{pmatrix}x_1\vee x_3\\x_1\vee x_2\end{pmatrix};\qquad \vec{F}_{7.2}=\begin{pmatrix}x_2\oplus 1\\x_1\end{pmatrix}\to\vec{F}_7^{2/4}=\begin{pmatrix}x_2\vee x_4\\x_1\vee x_2\end{pmatrix};\qquad \vec{F}_{12.2}=\begin{pmatrix}x_1\oplus x_2\\x_1\oplus 1\end{pmatrix}\to\vec{F}_{12}^{2/4}=\begin{pmatrix}x_2\vee x_3\\x_3\vee x_4\end{pmatrix};$$

$$\vec{F}_3=\begin{pmatrix}x_1\oplus 1\\x_2\end{pmatrix}\to\vec{F}_3^{2/4}=\begin{pmatrix}x_3\vee x_4\\x_1\vee x_3\end{pmatrix};\qquad \vec{F}_{8.2}=\begin{pmatrix}x_2\\x_1\oplus 1\end{pmatrix}\to\vec{F}_8^{2/4}=\begin{pmatrix}x_3\vee x_4\\x_1\vee x_3\end{pmatrix};\qquad \vec{F}_{13.2}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{pmatrix}\to\vec{F}_{13}^{2/4}=\begin{pmatrix}x_1\vee x_4\\x_2\vee x_4\end{pmatrix};$$

$$\vec{F}_4=\begin{pmatrix}x_1\\x_2\oplus 1\end{pmatrix}\to\vec{F}_4^{2/4}=\begin{pmatrix}x_1\vee x_2\\x_2\vee x_4\end{pmatrix};\qquad \vec{F}_9=\begin{pmatrix}x_1\oplus x_2\\x_2\end{pmatrix}\to\vec{F}_9^{2/4}=\begin{pmatrix}x_2\vee x_3\\x_1\vee x_3\end{pmatrix};\qquad \vec{F}_{14}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_2\end{pmatrix}\to\vec{F}_{14}^{2/4}=\begin{pmatrix}x_1\vee x_4\\x_1\vee x_3\end{pmatrix};$$

$$\vec{F}_5=\begin{pmatrix}x_1\oplus 1\\x_2\oplus 1\end{pmatrix}\to\vec{F}_5^{2/4}=\begin{pmatrix}x_3\vee x_4\\x_2\vee x_4\end{pmatrix};\qquad \vec{F}_{10.2}=\begin{pmatrix}x_1\oplus x_2\\x_1\end{pmatrix}\to\vec{F}_{10}^{2/4}=\begin{pmatrix}x_2\vee x_3\\x_1\vee x_2\end{pmatrix};\qquad \vec{F}_{15.2}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\x_1\end{pmatrix}\to\vec{F}_{15}^{2/4}=\begin{pmatrix}x_1\vee x_4\\x_1\vee x_2\end{pmatrix};$$

$$\vec{F}_{16.2}=\begin{pmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{pmatrix}\to\vec{F}_{16}^{2/4}=\begin{pmatrix}x_1\vee x_4\\ x_3\vee x_4\end{pmatrix};\quad \vec{F}_{19.2}=\begin{pmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to\vec{F}_{19}^{2/4}=\begin{pmatrix}x_3\vee x_4\\ x_2\vee x_3\end{pmatrix};\quad \vec{F}_{22.2}=\begin{pmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to\vec{F}_{22}^{2/4}=\begin{pmatrix}x_3\vee x_4\\ x_1\vee x_4\end{pmatrix};$$

$$\vec{F}_{17}=\begin{pmatrix}x_1\\ x_1\oplus x_2\end{pmatrix}\to\vec{F}_{17}^{2/4}=\begin{pmatrix}x_1\vee x_2\\ x_2\vee x_3\end{pmatrix};\quad \vec{F}_{20.2}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{pmatrix}\to\vec{F}_{20}^{2/4}=\begin{pmatrix}x_2\vee x_4\\ x_2\vee x_3\end{pmatrix};\quad \vec{F}_{23.2}=\begin{pmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to\vec{F}_{23}^{2/4}=\begin{pmatrix}x_2\vee x_4\\ x_1\vee x_4\end{pmatrix};$$

$$\vec{F}_{18.2}=\begin{pmatrix}x_2\\ x_1\oplus x_2\end{pmatrix}\to\vec{F}_{18}^{2/4}=\begin{pmatrix}x_1\vee x_3\\ x_2\vee x_3\end{pmatrix};\quad \vec{F}_{21}=\begin{pmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to\vec{F}_{21}^{2/4}=\begin{pmatrix}x_1\vee x_2\\ x_1\vee x_4\end{pmatrix};\quad \vec{F}_{24.2}=\begin{pmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{pmatrix}\to\vec{F}_{24}^{2/4}=\begin{pmatrix}x_1\vee x_3\\ x_1\vee x_4\end{pmatrix}.$$

Представленные функции кодирования и декодирования можно рассматривать как математические модели арифметических устройств кодирования и декодирования информации.

Выводы

Таким образом, полученные в работе математические модели устройств кодирования и декодирования информации обеспечивают совмещение операций кодирования в двоично-четверичную систему счисления с постоянным числом единиц с одновременным криптографическим преобразованием.

Также они обеспечивают криптографическое декодирование информации с декодированием результатов с двоично-четверичной системы счисления в двоичную систему, при этом сложность реализации арифметических устройств кодирования и декодирования информации не более двух входов логических элементов на один выход и скорость совмещенных преобразований соизмерима со скоростью переключения одного логического элемента.

Список литературы

1. Дадаев Ю.Г. Теория арифметических кодов / Ю.Г. Дадаев. – М.: Радио и связь, 1981. – 256 с.

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

3. Бабенко В.Г Моделирование позиционных избыточных систем счисления / В.Г. Бабенко, С.Ю. Кучеренко, В.М. Зажома // Системи управління, навігації та зв'язку : зб. наук. праць. – Вип. 4 (16). – К. : ДП «Центр. наук.-досл. ін-т навігації і управління» Мінпромполітики, 2010. – С. 51-54.

4. Стахов А.П. Алгоритмическая теория измерений / А.П. Стахов. – М.: Знание/ Новое в жизни, науке, технике. Сер. математика, кибернетика, 1979. – 64 с.

5. 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.

6. Рудницкий В.Н. Анализ форм представления информации / В.Н. Рудницкий, О.В. Нечипоренко // Электроника и связь. – К.: КПИ. – 2003. – № 19. – С. 150-152.

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

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

Поступила в редколлегию 18.07.2012

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

МЕТОД КРИПТОГРАФІЧНОГО КОДУВАННЯ ІНФОРМАЦІЇ З ВВЕДЕННЯМ ІНФОРМАЦІЙНОЇ НАДЛИШКОВОСТІ НА ОСНОВІ ДВОХРОЗРЯДНИХ ЛОГІЧНИХ ФУНКЦІЙ

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

Дана стаття присвячена розробці методу криптографічного кодування інформації з введенням інформаційної надлишковості на основі двохрозрядних логічних функцій. Традиційно задачі передачі конфіденційної інформації в надлишкових системах вирішуються двома шляхами: введенням інформаційної надлишковості з послідуючим криптографічним перетворенням або криптографічне перетворення з послідуючим введенням інформаційної надлишковості, тоді для зменшення складності програмно-апаратної частини системи, а також зменшення часу отримання інформації доцільним є суміщення процесу введення надлишковості з криптографічним перетворенням.

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

METHOD OF DATA ENCODING CRYPTOGRAPHIC WITH THE INTRODUCTION OF INFORMATION REDUNDANCY BASED ON TWO-DIGIT LOGICAL FUNCTION

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

This article focuses on the development of cryptographic methods of coding information with the introduction of information redundancy on the basis of double-bit logic functions. Traditionally, the problem of transmission of confidential information in the redundant system is solved in two ways: the introduction of information redundancy, followed by a cryptographic transformation, or a cryptographic transformation followed by information redundancy, then to reduce the complexity of software and hardware systems as well as reducing the time information is useful to combine the process of introducing redundancy with cryptographic transformation.

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