УДК 681.04

В.А.КРАСНОБАЕВ, д-р техн. наук

МЕТОД И АЛГОРИТМЫ КОРРЕКЦИИ ОШИБОК В СИСТЕМАХ ЦИФРОВОЙ ОБРАБОТКИ ИНФОРМАЦИИ

Известно [1-5], что использование непозиционной системы счисления в системе остаточных классов (СОК) позволяет улучшить такие характеристики систем цифровой обработки информации (СЦОИ), как пользовательская производительность, надежность и отказоустойчивость при решении определенного класса задач (для определенного типа операций). Как правило, в известных работах [6-7] рассматриваются коды в СОК со взаимно попарно простыми основаниями (модулями). Однако, если ставится задача минимизации времени коррекции ошибок, то в этом случае целесообразно рассмотреть коды в СОК со взаимно непростыми основаниями.

В предлагаемой статье рассматривается метод и алгоритмы коррекции ошибок в СЦОИ посредством применения кодов в СОК со взаимно непростыми модулями.

В СОК произвольный операнд A представляется в виде набора остатков $\{a_i\}$ от последовательного деления его на совокупность $\{m_i\}$ натуральных чисел, т.е. число A представится как $A = [A(\mathrm{mod}\ m_1), A(\mathrm{mod}\ m_2),\ldots, A(\mathrm{mod}\ m_n)]$ или $A = (a_1, a_2,\ldots, a_n)$, где $a_i \equiv A(\mathrm{mod}\ m_i)$. Диапазон представимых чисел представится в виде (0, M], где $M = [\ m_1, m_2,\ldots m_n\ ]$ – НОК оснований СОК.

Для последующего доказательства теорем, на основании которых базируется метод коррекции ошибок, рассмотрим следующую лемму [8].

Лемма. Для любого целого числа A, заданного в СОК с основаниями $\{m_i\}$, $i=\overline{1,n}$ и для любой пары оснований m_i, m_j ($i,j=\overline{1,n}$; $i \neq j$) должно выполнятся следующее условие:
$(a_i - a_j) \mathrm{mod}\ d_{ij} = 0$, где $d_{ij} = (m_i, m_j)$ – НОД оснований m_i и m_j.

Используя результаты леммы сформулируем и докажем следующую теорему, которая определяет необходимые условия обнаружения ошибок в СОК.

Теорема 1. Для обнаружения ошибки в остатке по произвольному основанию m_i числа A, заданного в СОК совокупностью оснований $\{m_i\}$, $i=\overline{1,n}$, необходимо, чтобы произвольное основание m_i имело хотя бы один, отличный от единицы, общий делитель с каждым из остальных оснований m_j ($j=\overline{1,n}$; $j \neq i$).

<u>Доказательство.</u> Обозначим НОД оснований m_i и m_j как $d_{ij} = (m_i, m_j)$ для $i,j=\overline{1,n}$ и $j \neq i$. Пусть ошибка произошла по модулю m_i, т.е. $\tilde{a}_i = (a_i + \Delta a_i)\ \mathrm{mod}\ m_i$.

Вначале покажем, что выражение ($\tilde{a}_i - \Delta a_i$) mod d_{ij} (1) эквивалентно выражению Δa_j (mod d_{ij}). Действительно, в соответствии с результатами вышеприведенной леммы имеем $(a_i + a_j)$ mod $d_{ij} \equiv 0$. Запишем выражение $\tilde{a}_i = (a_i + \Delta a_i)$ mod m_i в следующем виде:

$$a_i + \Delta a_i = m \cdot m + \tilde{a}_i, \tag{2}$$

где m – целое число. Из выражения (2) определим значение искаженного остатка $\tilde{a}_i = a_i + \Delta a_i - m \cdot m_i$ и, подставив его в выражение (1), получим:

$$(\tilde{a}_i - a_j) \bmod d_{ij} = [(a_i + \Delta a_i - m \cdot m_i) - a_j] \bmod d_{ij} =$$
$$= [(a_i - a_j) + (-m \cdot m_i + \Delta a_i)] \bmod d_{ij} = \qquad (3)$$
$$= [(a_i - a_j) + (-m \cdot k \cdot d_{ij} + \Delta a_i)] \bmod d_{ij},$$

где: $m_i = k \cdot d_{ij}$ (по условию леммы); k – натуральное число.

Рассматривая каждое из слагаемых выражений (3), получим: $(a_i - a_j) \bmod d_{ij} \equiv 0$ (согласно лемме) и также $(m \cdot k \cdot d_{ij}) \bmod d_{ij} \equiv 0$. В этом случае

$$\Delta a \equiv (\tilde{a}_i - a_j) \bmod d_{ij}. \qquad (4)$$

Анализируя формулу (4) очевидно, что при отсутствии для модулей m_i и m_j общих делителей больше единицы выполняется условие $\Delta a_i \pmod{d_{ij}} \equiv 0$. Таким образом необходимым условием обнаружения ошибки по одному из оснований является выполнение условия

$$d_{ij} = (m_i, m_j) \neq 1. \qquad (5)$$

Необходимое условие (5) теоремы 1 является и достаточным, если величина $\Delta a_i \equiv (\tilde{a}_i - a) \bmod d_{ij}$ не кратна одновременно двум делителям $d_{i-1,i}$ и $d_{i,i+1}$, т.е.

$$\text{НОД } d_{\Delta a_i}^{(i-1)} = (d_{i-1,i}, \Delta a_i) = 1 \text{ и НОД } d_{\Delta a_i}^{(i+1)} = (d_{i,i+1}, \Delta a_i) = 1. \qquad (6)$$

Для исправления ошибок в СОК воспользуемся доказательством следующей теоремы [9].

Теорема 2. Для исправления ошибки в остатке по произвольному основанию m_i $(i = \overline{1,n})$ числа А, заданного в СОК основаниями $\{m_i\}$, необходимо выполнение следующего условия:

$$(d_{ik} - 1) \cdot (d_{ij} - 1) \geq \delta(\Delta a_i), \qquad (7)$$

где $\delta(\Delta a_i) = m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik}, d_{ij}]})$.

При этом :

$K_{d_{ik}}$ - число возможных делителей значения ошибки Δa_i по основанию m_i, кратных значению d_{ik};

$K_{d_{ij}}$ - число возможных делителей значения ошибки Δa_i по основанию m_i, кратных значению d_{ij};

$K_{[d_{ik}, d_{ij}]}$ - число возможных делителей ошибки Δa_i по основанию m_i, кратных значению НОК чисел d_{ik}, d_{ij}.

Условие (7) теоремы 2 является и достаточным, если различным возможным значениям $\delta(\Delta a_i)$ ошибок соответствуют различные пары величин a_{ik}, a_{ij}.

На основании вышеприведенных теорем построим алгоритмы обнаружения и исправления однократных (по одному из оснований СОК) ошибок.

Алгоритмы обнаружения ошибок

Алгоритм 1. Пусть необходимо проверить факт наличия либо отсутствия ошибок в операнде $A = (a_1, a_2, \ldots, a_n)$.

1.Определим следующую совокупность значений:

$$
\begin{cases}
a_{12} = (a_1 - a_2)\bmod d_{12}, \\
a_{13} = (a_1 - a_3)\bmod d_{13}, \\
\quad . \quad . \quad . \\
a_{1n} = (a_1 - a_n)\bmod d_{1n}.
\end{cases} \tag{8}
$$

Если вся совокупность (8) значений $a_{1i} = 0$ $(i = \overline{1,n}; i \neq 1)$ равна нулю, то далее вычисляется и проверяется совокупность значений $a_{2i} = (a_2 - a_1)\bmod d_{2i} (i \neq 2)$ и т.д.

2.При получении всех возможных значений a_{ij} $(j \neq j)$ составляем матрицу G вида

$$
G = \begin{vmatrix}
a_{12} & a_{13} & \dots & a_{1n} \\
a_{21} & a_{23} & \dots & a_{2n} \\
\vdots & & & \vdots \\
a_{n1} & a_{n2} & \dots & a_{nn}
\end{vmatrix}.
$$

При составлении матрицы G нет необходимости указывать истинное числовое значение элементов a_{ij}, а достаточно представить элементы матрицы в виде единицы или нуля, т.е.

$$
a_{ij} = \begin{cases} 0, \text{при}\, a_{ij} = 0, \\ 1, \text{при}\, a_{ij} \neq 0. \end{cases}
$$

3.Если определитель $|G| = 0$, то A считается неискаженным, а если $|G| \neq 0$ - число A искажено.

Если воспользоваться соотношением

$$
a_i - a_j \equiv [d_{ij} - (a_j - a_i)]\bmod d_{ij},
$$

то для определения правильности или неправильности операнда A достаточно определить лишь следующую совокупность чисел:

$$
a_{12}, a_{23}, a_{34}, \dots, a_{n-1n}, a_{n1}.
$$

Исходя из вышеизложенного очевидно, что посредством предлагаемого метода кодирования информации в СОК исключительно просто реализуется процесс обнаружения ошибок. При этом время обнаружения ошибок, сравнительно с обнаружением ошибок в позиционной двоичной системе счисления, достаточно мало и постоянно для любого числа оснований СОК [10].

Алгоритм 2. Приведем некоторые соображения, позволяющие упростить вышеприведенный алгоритм обнаружения ошибок.

Покажем, что

$$
[(a_1 + \overline{a_j}) + (\overline{a_1} + a_j)] \equiv 0 \pmod{d_{1j}},
$$

где: $\overline{a_j} = m_j - a_j$; $\overline{a_1} = m_1 - a_1$.

Пусть в операнде $A = (a_1, a_2, ..., a_j, ..., a_n)$ искажен остаток a_j по основанию m_j, т.е. $\tilde{a}_j = (a_j + \Delta a_j) \bmod m_j$. Запишем систему следующих равенств:

$$\begin{cases} K_1 = a_i - \tilde{a}_j = a_i + (m_j - \tilde{a}_j) = a_i + m_j - a_j - \Delta a_j; \\ K_2 = \tilde{a}_j - a_i = a_j + \Delta a_j - a_i = a_j - a_i + \Delta a_j. \end{cases}$$

Сложив эти два равенства, получим:

$$K_1 + K_2 = m_j \text{ или } K_1 + K_2 \equiv 0 \pmod{m_j}.$$

Таким образом очевидно, что

$$a_1 + \overline{a}_j = d_{1j} - (\overline{a}_1 + a_j),$$

т.е. для определения факта наличия или отсутствия ошибок нет необходимости вычисления точного значения величины $(a_1 + \overline{a}_j) \bmod d_{1j}$, а достаточно знать факт равенства или неравенства этого значения нулю. Это в свою очередь позволит в техническом устройстве для обнаружения ошибок в СОК [11] вместо (n – 1) сумматоров по модулям m_j ($j = \overline{2, n}$), которые определяют совокупность значений $\overline{a}_j = m_j - a_j$, использовать всего один сумматор по модулю m_1, определяющий значение $\overline{a}_1 = m_1 - a_1$.

Алгоритм обнаружения и исправления ошибок

1. Определим все возможные значения вида $a_{i,i+1} = (a_1 - a_{i+1}) \bmod d_{i,i+1}$:

$$\begin{cases} a_{12} = (a_1 - a_2) \bmod d_{12}, \\ a_{23} = (a_2 - a_3) \bmod d_{23}, \\ \quad \cdots \\ a_{n-1,n} = (a_{n-1} - a_n) \bmod d_{n-1,n}, \\ a_{n1} = (a_n - a_1) \bmod d_{n1}. \end{cases} \tag{9}$$

2. Если вся совокупность (9) значений принимает нулевое значение, то ошибка отсутствует либо она кратна одному из делителей $d_{i-1,i}, d_{i,i+1}$, что противоречит условию ограничения класса возможных корректируемых ошибок. Таким образом считается, что ошибка отсутствует.

3. Если одновременно выполняются условия $a_{i-1,i} \neq 0$ и $a_{i,i+1} \neq 0$, а все остальные значения в совокупности (9) принимают значения ноль, то считается, что ошибка имеется в остатке по модулю m_i, т.е.

$$\tilde{a}_i = (a_i + \Delta a_i) \bmod m_i \, (0 < \Delta a_i \le m_{i-1}).$$

4. В соответствии с известным алгоритмом производится коррекция ошибок по i–му основанию СОК.

В соответствии с данным алгоритмом разработано устройство для его реализации [12]. Кратко рассмотрим алгоритм его функционирования (см. рис. 1).

Пусть задана СОК основаниями $m_1 = 4$, $m_2 = 6$, $m_3 = 12$. Возможная совокупность кодовых слов представлена в табл. 1 (т.е. НОК значений 4,6 и 12 равно M = [4, 6, 12] = 12). Определим следующее значение НОД: $d_{12} = (4, 6) = 2$; $d_{23} = (6, 12) = 6$; $d_{31} = (4, 12) = = 4$; $\delta(\Delta a_1) = 2$ (табл. 2); $\delta(\Delta a_2) = 3$ (табл. 3); $\delta(\Delta a_3) = 8$ (табл. 4).

Пусть искажено правильное число A = (11, 001, 0111) по основанию m_2, т.е. на вход устройства (см. рис. 1) подается операнд вида $\tilde{A}$ = (11, 100, 0111). Необходимо определить правильность числа $\tilde{A}$ и при необходимости провести его коррекцию.

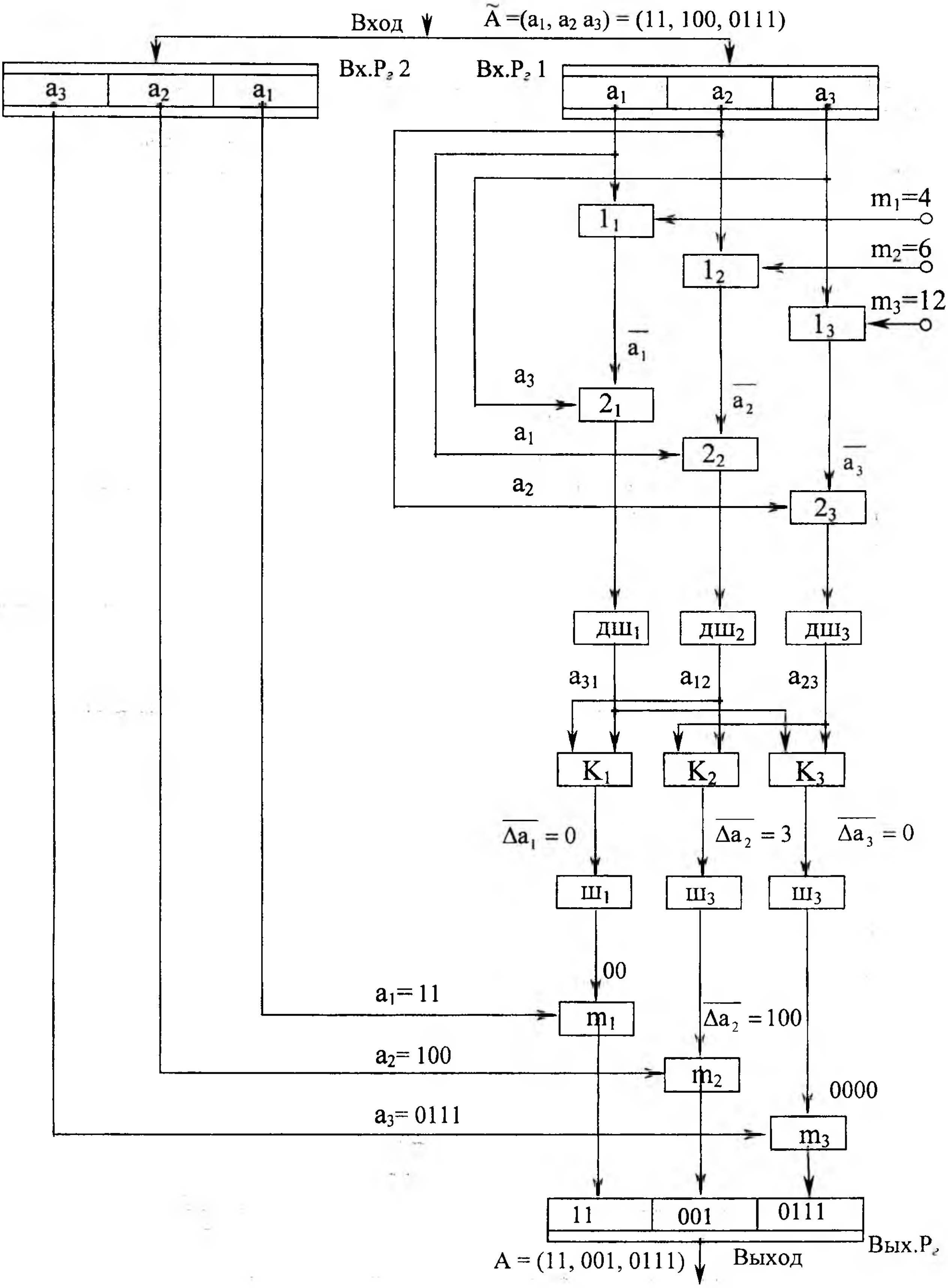
Операнд $\tilde{A}$ записывается в первый $P_г1$ и второй $P_г2$ входные регистры. На выходах соответствующих сумматоров $1_1 \div 1_3$ по модулям $m_1 \div m_3$ получим инвертированные значения соответствующих остатков $\bar{a}_i = m_i - a_i (i = \overline{1,3})$. На выходах сумматоров $2_1 \div 2_3$ получим такие значения: $2_1 - (a_3 + \bar{a}_1)\bmod d_{31} = 0000$; $2_2 - (a_1 + \bar{a}_2)\bmod d_{12} = 001$; $2_3 - (a_2 + \bar{a}_3)\bmod d_{23} = 0011$, которые через соответствующие дешифраторы $ДШ_1$ – $ДШ_3$ в унитарном коде поступают на соответствующие входы коммутаторов $K_1 \div K_3$, которые реализуют значения $\delta(\Delta a_i)$ соответствующих таблиц.

Таблица 1

А в ПСС	Кодовые числа		
	А в СОК		
	m_1	m_2	m_3
0000	00	000	0000
0001	01	001	0001
0010	10	010	0010
0011	11	011	0011
0100	00	100	0100
0101	01	101	0101
0110	10	000	0110
0111	11	001	0111
1000	00	010	1000
1001	01	011	1001
1010	10	100	1010
1011	11	101	1011

Таблица 2

a_{31}	$a_{12} = 1$
1	$\Delta\bar{a}_1 = 1$
2	—
3	$\Delta\bar{a}_1 = 3$



Вход
$\tilde{A}$ =(a1, a2 a3) = (11, 100, 0111)
Вх.Р 2
Вх.Р 1
a3 a2 a1
a1 a2 a3
m1=4
m2=6
m3=12
1 1
1 2
1 3
a3
a1
a2
2 1
2 2
2 3
дш1
дш2
дш3
a31
a12
a23
K1
K2
K3
Δa1 = 0
Δa2 = 3
Δa3 = 0
ш1
ш3
ш3
00
a1= 11
m1
Δa2 = 100
a2= 100
m2
0000
a3= 0111
m3
11
001
0111
Вых.Р
A = (11, 001, 0111)
Выход

Рис.1

Таблица 3

a_{23}	$a_{12} = 1$
1	$\Delta\bar{a}_2 = 5$
2	—
3	$\Delta\bar{a}_2 = 3$
4	—
5	$\Delta\bar{a}_2 = 1$

Таблица 4

a_{31}	a_{23}				
	1	2	3	4	5
1	$\Delta\bar{a}_3 = 7$	—	$\Delta\bar{a}_3 = 3$	—	$\Delta\bar{a}_3 = 11$
2	—	$\Delta\bar{a}_3 = 2$	—	$\Delta\bar{a}_3 = 10$	—
3	$\Delta\bar{a}_3 = 1$	—	$\Delta\bar{a}_3 = 9$	—	$\Delta\bar{a}_3 = 5$

(табл. 2 - табл. 4) значений ошибок. В этом случае только на выходе второго (табл. 3) коммутатора K_2 имеется ненулевое значение (это факт наличия ошибки в операнде $\tilde{A}$), которое поступает через шифратор $Ш_2$ (который преобразует его в двоичный код) на первый вход сумматора по модулю m_2. На второй вход этого сумматора с выхода второго регистра Вх. $P_2 2$ поступает значение искаженного остатка $\tilde{a}_2 = 100$. С выхода сумматора по модулю m_2 в выходной регистр (Вых. $P_2 2$) поступит значение исправленного остатка

$$(\tilde{a}_2 + \overline{\Delta a_2}) \bmod m_2 = (a_2 + \Delta a_2) + (m_2 - \Delta a_2) = a_2 (\bmod m_2) = 001.$$

В этом случае в выходном регистре устройства содержится исправленный операнд $A = (11, 001, 0111)$.

Таким образом, в статье предложен метод коррекции ошибок, основанный на использовании непозиционных кодовых структур в СОК. В соответствии с рассмотренным методом разработаны алгоритмы обнаружения и исправления ошибок в СЦОИ, на основании которых разработаны патентоспособные технические устройства. Использование этих устройств в СЦОИ показали высокую эффективность применения непозиционного кодирование информации в СОК.

Список литературы: 1. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. М.: Сов. радио, 1968. 440 с. 2. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов: Пер. с англ. М.: Мир, 1989. 448 с. 3. *Кравченко В.Ф., Крот А.М.* Методы и микроэлектронные средства цифровой фильтрации сигналов и изображений на основе теоретико – числовых преобразований // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1997. №6. С. 3-31. 4. *Червяков Н.И., Тынчеров К.Т., Велигоша А.В.* Высокоскоростная цифровая обработка сигналов с использованием непозиционной арифметики // Радиотехника. 1997. №10. С. 23-27. 5. *Лавриненко Д.И.* Применение быстрого преобразования Фурье в криптографических преобразователях // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2000. Вып. 114. с. 75-79. 6. *Краснобаев В.А.* Основы создания вычислителей на основе остаточных классов // Системи обробки інформації. Харків:НАНУ, ПАНМ, ХВУ. 2001. Вип. 1(11). с. 3-7. 7. *Краснобаев В.А.* Методы реализации модульных операций в системах цифровой обработки информации // Радиотехника: Всеукр. межвед. сб. 2001. Вып. 119. с. 130-134. 8. *Торгашев В.А.* Система остаточных классов и надежность ЦВМ. М.: Сов. радио, 1973. 118 с. 9. *Краснобаев В.А.* Техническая реализация метода коррекции ошибок в системе остаточных классов // АСУ и приборы автоматики. 1987. Вып. 81. С. 97 – 101. 10. А.с. 964645 СССР. Устройство для обнаружения одиночных ошибок кода в системе остаточных классов / *В.А. Краснобаев, А.И. Бецков, Е.И. Бороденко и др.* // Бюл. изобрет. 1982. №37. С. 184. 11. А. с. 1013957 СССР. Устройство для обнаружения ошибок в системе остаточных классов / *В.А. Краснобаев, И.Б. Давыдов* // Бюл. изобрет. 1983. №15. С. 210. 12. А. с. 1166117 СССР. Устройство для контроля информации в системе остаточных классов / *В.А. Краснобаев* // Бюл. изобрет. 1985. №25. С. 124.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 25.04.2002