УДК 681.3

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ НУЛЕВИЗАЦИИ В МОДУЛЯРНЫХ ПОЛИНОМИАЛЬНЫХ КОДАХ

Мартиросян А.Г., Калмыков М.И.

ФГБОУ ВПО «Северо-кавказский федеральный университет», Ставрополь, e-mail: kia762@yandex.ru

Применение кодов полиномиальной системы классов вычетов (ПСКВ) позволяет не только повысить скорость вычислений, но и обеспечить процедуры поиска и коррекции ошибок. В работе показано, что использование двух контрольных основания позволяет исправлять все однократные ошибки в модулярных кодовых конструкциях. С целью сокращения временных затрат на выполнение процедур поиска и коррекции ошибок в статье предлагается провести усовершенствование алгоритма нулевизации. Переход к параллельному алгоритму вычисления позиционной характеристики следа позволяет не только повысить скорость вычислений, но и сокращает аппаратурные затраты. Проведен сравнительный анализ реализаций последовательного и усовершенствованного алгоритма нулевизации.

Ключевые слова: корректирующие коды, полиномиальная система классов вычетов, позиционные характеристики кода, нулевизация кода, след полинома

ADVANCED ALGORITHMS NULEVIZATSII IN MODULAR POLYNOMIAL CODES

Martirosyan A.G., Kalmykov M.I.

North-caucasian federal university, Stavropol, e-mail: kia762@yandex.ru

Application code polynomial system of residue classes (PSKV) not only improves the speed of computation , but also to ensure the search procedure and error correction. It is shown that the use of two control base allows you to fix all single error in code in modular designs. With a view to reducing the time to perform the search and correction of errors in the article proposed that the improvement algorithm nulevizatsii . Transition to parallel_ reduce computing positional characteristics should not only improves the speed of computation , but also reduces the hardware cost . A comparative analysis of serial implementations and advanced algorithm nulevizatsii.

Keywords: Error-Correcting Codes, polynomial system of residue classes, positional characteristics code nulevizatsiya code trace polynomial

Структура современных спецпроцессоров (СП) цифровой обработки сигналов (ЦОС) очень насыщена и сложна. Применение параллельных алгоритмов ортогональных преобразований сигналов определяется требованием реального масштаба проводимых вычислений. При этом такие вычислительные устройства должны обладать свойством устойчивости к отказам, возникающим в процессе функционирования. Применение корректирующих кодов полиномиальной системы классов вычетов (ПСКВ) позволяет осуществлять поиск и коррекцию ошибок в реальном масштабе времени.

Основная часть. В современных условиях сохранение работоспособного состояния параллельных спецпроцессоров ЦОС во многом определяется быстротой и точностью определения местоположения и глубины ошибки, которая возникает из-за отказа оборудования. При этом предпочтение отдается информационной, а не технологической надежности системы, которая может быть достигнута путем специального кодирования, обеспечивающего обнаружение ошибок, возникающих в результате сбоев и отказов элементов системы, и их исправление [2-7].

В основу большинства алгоритмов и методов поиска и коррекции ошибок в модулярных кодах положена процедура вычисления позиционной характеристики. По способу построения процедур поиска и локализации ошибки в модулярных кодах существующие методы можно разделить на две основные группы. К первой относятся методы и алгоритмы контроля и коррекции ошибок кода ПСКВ, базирующиеся на вычисление позиционных характеристик во временной области [2-7, 9, 10]. Что касается процедур второй группы, то они реализуются в частотной области [1, 8]. Рассмотрим методы обнаружения и коррекции ошибок, работающие во временной области, а так же их реализацию в базисе нейросетевой логики.

Реализация данного подхода предполагает использование некоторого функционального отношения, однозначно отражающего множество значений модульных характеристик во множество рассматриваемых ошибок E. При этом необходимо, чтобы математическая модель, отражающая данное отношение, при реализации обеспечивала бы параллельно-конвейерную организацию вычислений.

В работе [4] доказана теорема о возможности использования непозиционных полиномиальных кодов в процедурах обнаружения и коррекции ошибок. С этой целью в модулярную комбинацию вводится дополнительное контрольное основание $p_{k+1}(z)$, где k – количество рабочих оснований. При этом степень избыточного основания не должна быть меньше наибольшей степени рабочего основания. $\deg p_{k+1}(z) \ge \deg p_k(z)$. Однако проводимые исследования показали, что наличие одного избыточного основания, даже удовлетворяющего предельной теореме, является недостаточным, так как корректирующие способности такого кода не позволяют исправить однократные ошибки по всем основаниям ПСКВ [2].

Для решения данной проблемы необходимо осуществить логическое упрочнение контрольного основания. С этой целью вводится дополнительное контрольное основание $p_{k+2}(z)$, удовлетворяющее условию $\deg p_{k+2}(z) \ge \deg p_{k+1}(z)$. Однако упрочение контрольного основания требует значительного расширения диапазона обрабатываемых данных. В этом случае рабочий диапазон полиномиальной системы классов вычетов будет определяться

$$P_{раб}(z) = \prod_{i=1}^{k} p_i(z), \qquad (1)$$

а полный диапазон системы задается выражением

$$P_{пол}(z) = \prod_{i=1}^{k+2} p_i(z) = P_{раб}(z)\, p_{k+1}(z)\, p_{k+2}(z). \qquad (2)$$

А чтобы точность представления не претерпела заметного уменьшения, надо увеличивать диапазон представления величин, и тогда их истинные (без введенной погрешности) значения будут в пределах заданного рабочего диапазона.

Альтернативным путем решения данной проблемы является метод определения правильности $A(z) = (\alpha_1(z), \ldots \alpha_2(z), \ldots, \alpha_{k+1}(z), \ldots, \alpha_{k+r}(z))$ на основе нулевизации, заключающейся в переходе от исходного полинома к полиному

$$(0, 0, \ldots, \gamma_{k+1}(z), \ldots, \gamma_{k+r}(z)),$$

при помощи преобразований, при которых не имеет место ни один выход за пределы рабочего диапазона системы.

Алгоритм процедуры нулевизации заключается в последовательном вычитании из исходного полинома, представленного в модулярном коде, некоторых минимальных полиномов – констант нулевизации таких, что полином $A(z)$ последовательно преобразуется в полином вида

$$(0, \alpha_2^1(z), \alpha_3^1(z), \ldots, \alpha_k^1(z), \alpha_{k+1}^1(z), \ldots, \alpha_{k+r}^1(z)),$$

затем в полином

$$(0, 0, \alpha_3^2(z), \ldots, \alpha_k^2(z), \alpha_{k+1}^2(z), \ldots, \alpha_{k+r}^2(z)),$$

и так далее. Продолжая данный процесс в течение k итераций, получается

$$(0, 0, \ldots, \gamma_{k+1}(z), \ldots, \gamma_{k+r}(z)).$$

Применение метода нулевизации позволяет последовательно получать наименьший полином, кратный сначала $p_1(z)$, затем полином – кратный произведению $p_1(z)p_2(z)$, и в конечном итоге – кратный рабочему

$$P_{раб}(z) = \mathop{\Pi}_{i=1}^{k} p_i(z).$$

Основным недостатком метода нулевизации [6, 9] является последовательный характер вычислительного процесса, что не позволяет реализовать его на основе двухслойной нейронной сети. Это обусловлено, прежде всего тем, что константы нулевизации представляют собой наименьшие возможные числа

$$\begin{aligned} &M_1(z) = (\alpha_1^1(z), \alpha_2^1(z), \ldots, \alpha_k^1(z), \alpha_{k+1}^1(z), \ldots, \alpha_{k+r}^1(z));\\ &M_2(z) = (0, \alpha_2^2(z), \ldots, \alpha_k^2(z), \alpha_{k+1}^2(z), \ldots, \alpha_{k+r}^2(z));\\ &\vdots\\ &M_k(z) = (0, 0, \ldots, \alpha_k^k(z), \alpha_{k+1}^k(z), \ldots, \alpha_{k+r}^k(z)). \end{aligned} \qquad (3)$$

где $\alpha_j^i(z) = 1, z, z+1, \ldots, z^{osdp_i(z)-1} + \ldots + z + 1;\ i = 1, 2, \ldots, k+r;\ j = 1, \ldots, k$.

Решить данную проблему можно за счет отказа от констант нулевизации $M_i(z)$ и перехода к использованию псевдоортогональных полиномов. Если положить условие, что $A(z) \in P_{раб}(z)$, то

$$A(z) = (\alpha_1(z), \alpha_2(z), ..., \alpha_k(z)).$$

Тогда, согласно китайской теореме об остатках, полином *A(z)* можно представить

$$A(z) = (\alpha_1, (z), 0, 0, ..., 0) + (0, \alpha_2(z), 0, ..., 0) + ...(0, 0, 0, ..., \alpha_k(z)). \quad (4)$$

Каждое слагаемое выражения (4) представляет собой

$$(0,0,...0, \alpha_i(z),0,...,0) = \alpha_i(z)B_i^*(z) \bmod P_{раб}(z), \quad (5)$$

где $B_i^*(z)$ – ортогональный базис, безизбыточной системы оснований.

Проведя расширение системы оснований $p_1(z), p_2(z), ..., p_k(z)$ на *r* контрольных $p_{k+1}(z), p_{k+2}(z), ..., p_{k+r}(z)$, представим

$$\alpha_i(z)B_i^*(z) \bmod P_{раб}(z)$$

в виде

$$\begin{cases} \alpha_1(z)B_1^*(z) \bmod P_{раб}(z) = (\alpha_1(z),0,0,...,0,\ \gamma_{k+1}^1(z),\ \gamma_{k+2}^1(z),...,\ \gamma_{k+1}^1(z)); \\ \alpha_2(z)B_2^*(z) \bmod P_{раб}(z) = (0,\ \alpha_2(z),0,...,0,\ \gamma_{k+1}^2(z), \gamma_{k+2}^2(z),..., \gamma_{k+1}^2(z)); \\ \vdots \\ \alpha_k(z)B_k^*(z) \bmod P_{раб}(z) = (0,0,0,...,\ \alpha_k(z), \gamma_{k+1}^k(z), \gamma_{k+2}^k(z),..., \gamma_{k+1}^k(z)). \end{cases} \quad (6)$$

Подставим выражения (6) в равенство (4).

$$\begin{aligned} A(z) &= (\alpha_1(z), 0, 0, ..., 0, (z), \gamma_{k+1}^1(z), \gamma_{k+2}^1(z), ..., \gamma_{k+r}^1(z)) + \\ &+ (0, \alpha_2(z), 0, ..., 0, \gamma_{k+1}^2(z), \gamma_{k+2}^2(z), ..., \gamma_{k+r}^2(z)) + ... + \\ &+ (0, 0, 0, ..., \alpha_k(z), \gamma_{k+1}^k(z), \gamma_{k+2}^k(z), ..., \gamma_{k+r}^k(z)). \end{aligned} \quad (7)$$

Следовательно,

$$\begin{cases} \alpha_{k+1}(z) = \sum_{j=1}^{k} \gamma_{k+1}^j(z), \bmod p_{k+1}(z), \\ \vdots \\ \alpha_{k+r}(z) = \sum_{j=1}^{k} \gamma_{k+r}^j(z), \bmod p_{k+r}(z). \end{cases} \quad (8)$$

Значит, разность полинома *A(z)*, представленного в ПСКВ, и псевдоортогональных форм, полученных согласно (6), задаёт величину нормированного следа полинома

$$\begin{cases} \gamma_{k+1}(z) = (\alpha_{k+1}(z) - \sum_{j=1}^{k} \gamma_{k+1}^j(z)) \bmod p_{k+1}(z), \\ \gamma_{k+2}(z) = (\alpha_{k+2}(z) - \sum_{j=1}^{k} \gamma_{k+2}^j(z)) \bmod p_{k+2}(z), \\ \gamma_{k+r}(z) = (\alpha_{k+r}(z) - \sum_{j=1}^{k} \gamma_{k+r}^j(z)) \bmod p_{k+r}(z). \end{cases} \quad (9)$$

Определим все псевдоортогональные полиномы для ПСКВ, в которой используются рабочие основания $p_1(z)=z+1$, $p_2(z)=z^2+z+1$, $p_3(z)=z^4+z^3+z^2+z+1$. В качестве контрольных оснований выбраны $p_4(z)=z^4+z^3+1$ и $p_5(z)=z^4+z+1$. При вычислении псевдоортогональных базисов необходимо учитывать невозможность выхода за пределы рабочего диапазона $P_{раб}(z)=z^7+z^6+z^5+\ldots+z^2+z+1$. Полученные значения представлены в табл. 1.

Таблица 1

Псевдоортогональные полиномы ПСКВ поля $GF(2^4)$

Основание ПСКВ	Псевдоортогональный полином
$p_1(z)=z+1$	$(1, 0, 0, z^3+z+1, z)$
$p_2(z)=z^2+z+1$	$(0, 1, 0, z^2+z+1, z^3+1)$
	$(0, z, 0, z^3+z, z^2+z+1)$
	$(0, z+1, 0, z^3+z^2+1, z^3+z^2+z)$
$p_3(z)=z^4+z^3+z^2+z+1$	$(0, 0, 1, z^3+z^2+1, z^3+z)$
	$(0, 0, z, z+1, z^2+z+1)$
	$(0, 0, z+1, z^3+z^2+z, z^3+z^2+1)$
	$(0, 0, z^2, z, z^3)$
	$(0, 0, z^2+1, z^3+z^2+z+1, z)$
	$(0, 0, z^2+z, 1, z^3+z^2+z+1)$
	$(0, 0, z^2+z+1, z^3+z^2, z^2+1)$
	$(0, 0, z^3, z^2, z+1)$
	$(0, 0, z^3+1, z^3+1, z^3+1)$
	$(0, 0, z^3+z, z^2+z+1, z^2)$
	$(0, 0, z^3+z+1, z^3+z, z^3+z^2+z)$
	$(0, 0, z^3+z^2, z^2+z, z^3+z+1)$
	$(0, 0, z^3+z^2+1, z^3+z+1, 1)$
	$(0, 0, z^3+z^2+z, z^2+1, z^3+z^2)$
	$(0, 0, z^3+z^2+z+1, z^3, z^2+z)$

Так как константы нулевизации подобраны таким образом, что в процессе вычитания из исходного полинома $A(z)$ псевдоортогональных форм (5) выход за пределы рабочего диапазона не осуществляется, то по результату (9) можно судить о правильности полинома $A(z)$. Если система равенств (9) обращается в ноль, то исходный полином не содержит ошибки, в противном случае – $A(z)$ является ошибочным. В табл. 2 представлены значения вектора ошибки $(0,\ldots,\Delta\alpha_i(z),\ldots,0)$ для различных значений ошибки ПСКВ.

Таблица 2

Значения вектора ошибки модулярного кода поля $GF(2^4)$

Основание ПСКВ		Значение вектора ошибки
$\gamma_4(z)$	$\gamma_5(z)$	
0	0	(0, 0, 0)
z^3+z+1	z	(1, 0, 0)
z^2+z+1	z^3+1	(0, 1, 0)
z^3+z	z^2+z+1	$(0, z, 0)$
z^3+z^2+1	z^3+z^2+z	$(0, z+1, 0)$
z^3+z^2+1	z^3+z	(0, 0, 1)
$z+1$	z^2+z+1	$(0, 0, z,)$
z^3+z^2+z	z^3+z^2+1	$(0, 0, z+1)$
z	z^3	$(0, 0, z^2)$
z^3+z^2+z+1	z	$(0, 0, z^2+1)$
1	z^3+z^2+z+1	$(0, 0, z^2+z)$
z^3+z^2	z^2+1	$(0, 0, z^2+z+1)$
z^2	$z+1$	$(0, 0, z^3)$
z^3+1	z^3+1	$(0, 0, z^3+1)$
z^2+z+1	z^2	$(0, 0, z^3+z)$
z^3+z	z^3+z^2+z	$(0, 0, z^3+z+1)$
z^2+z	z^3+z+1	$(0, 0, z^3+z^2)$
z^3+z+1	1	$(0, 0, z^3+z^2+1)$
z^2+1	z^3+z^2	$(0, 0, z^3+z^2+z)$
z^3	z^2+z	$(0, 0, z^3+z^2+z+1)$

Применение в качестве констант нулевизации псевдоортогональных полиномов позволяет перейти от последовательной реализации метода нулевизации к параллельной. В связи с этим открываются дополнительные возможности по сокращению временных затрат на реализации процесса определения местоположения ошибки и ее глубины.

Для эффективной реализации математических моделей вычислительных устройств, определенных над конечными полями $GF(p^v)$ или кольцами, необходимо, чтобы арифметические устройства могли эффективно реализовать основные операции данных алгебраических систем. В работе [9] приведена разработанная структура вычислительного устройства для реализации параллельной нулевизации в расширенном поле GF(2^4). При этом аппаратурные затраты будут определяться выражением

$$N = (2^v - 1) + \sum_{j=1}^{u} b_j \left(\lceil j/2 \rceil + 1 \right). \quad (10)$$

где b_j – количество j-входовых сумматоров по модулю два, используемых в устройстве;

$$u = \deg \prod_{i=1}^{k} p_i(z) + 1; \ \sum_j b_j = \sum_{i=k+1}^{k+r} \deg p_i(z).$$

Оценим эффективность представленного метода определения местоположения и глубины ошибки, используя выражение (10). В качестве базового элемента выбираем нейроподобный многовходовой сумматор по модулю два. В таблице 3 приведены данные о затратах оборудования, выраженные в количестве формальных нейронов для различных диапазонов полей Галуа.

Таблица 3

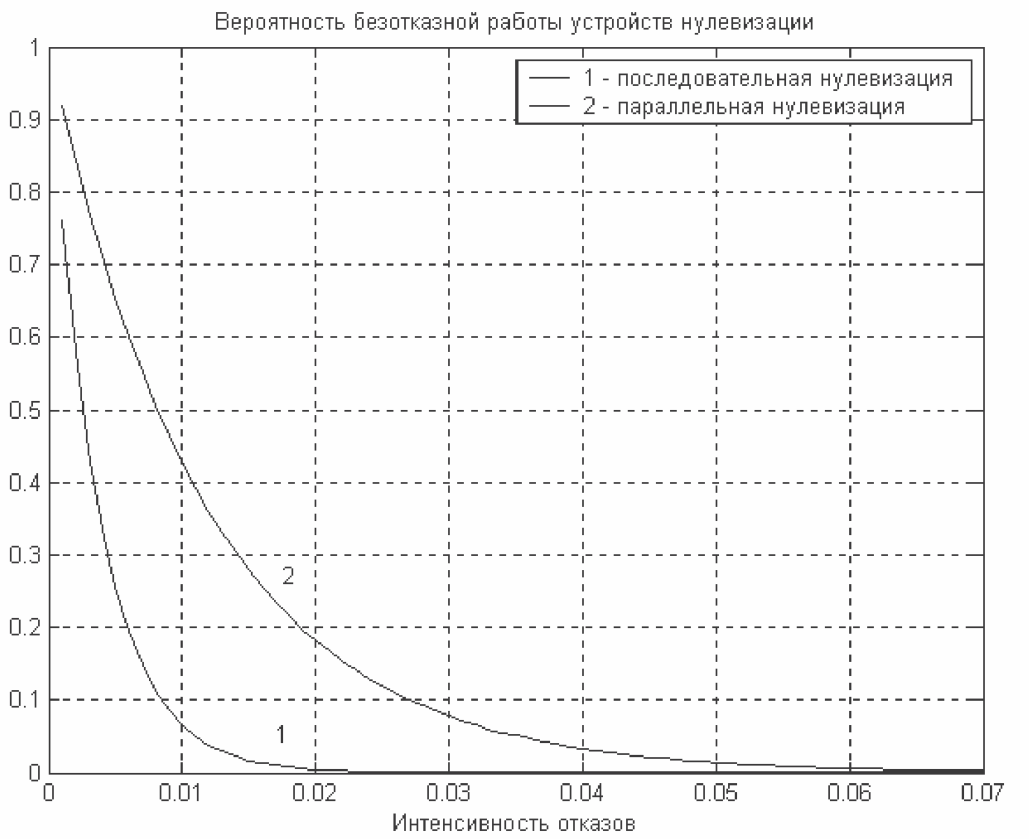
Количество базисных элементов устройства

	Разрядность сумматоров	GF(2^3)	GF(2^4)	GF(2^5)
Количество сумматоров	2	1		
	3		1	
	4	2	3	
	5		2	
	6		2	
	8			8
	10			1
	14			1
Количество нейронов	8	25	54	
Количество нейронов с учетом первого слоя	15	40	85	

На рисунке приведена вероятность безотказной работы устройств, реализующих процедуры последовательной и параллельной нулевизации в полиномиальной системе класса вычетов для полей Галуа $GF(2^5)$.

Из представленного рисунка наглядно видно, что применение метода параллельной нулевизации позволяет сократить аппаратурные затраты необходимые на реализации процедур поиска и локализации в модулярных кодах по сравнению с ранее известным методом последовательной нулевизации. Очевидно, что снижение аппаратурных затрат обеспечивает более надежную работу всего параллельного вычислительного устройства. При этом, очевидно, что с увеличением разрядности обрабатываемых данных эффективность применения метода параллельной нулевизации возрастает. Кроме того, реализация процедуры параллельной нулевизации позволяет осуществить операцию поиска и локализации ошибок всего за одну итерацию, в то время как скорость выполнения последовательной нулевизации обратно пропорциональна количеству рабочих оснований ПСКВ. Таким образом, очевидно, что разработанный метод вычисления позиционной характеристики характеризуется довольно высокой надежностью работы при сравнительно небольших временных затратах на реализацию процедур поиска и определения местоположения ошибочных разрядов.

Выводы. В работе рассмотрены вопросы построения корректирующих кодов полиномиальной системы классов вычетов. Показано, что для выполнения этих операций в код ПСКВ надо вводить контрольные основания. Так введение двух избыточных модулей позволяет исправить все однократные ошибки. В статье приведен усовершенствованный алгоритм вычисления позиционной характеристики след полинома. Применение псевдоортогональных базисов в качестве констант нулевизации позволяет сократить временные и схемные затраты необходимые на вычисление этой позиционной характеристики.



Вероятность безотказной работы устройств для GF(2^5)

СПИСОК ЛИТЕРАТУРЫ

1. Барильская А.В, Фалько А.А., Калмыков И.А., Кихтенко О.А., Дагаева О.И. Устройство спектрального обнаружения и коррекции в кодах полиномиальной системы классов вычетов // Патент России № 2390051. от 09.07.2008.

2. Бережной В.В., Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А. Архитектура отказоустойчивой нейронной сети для цифровой обработки сигналов// Нейрокомпьютеры: разработка и применение. 2004. № 12. С. 51-57.

3. Бережной В.В., Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Шилов А.А. Нейросетевая реализация в полиномиальной системе классов вычетов операций ЦОС повышенной разрядности // Нейрокомпьютеры: разработка и применение. 2004. № 5-6. С. 94.

4. Зиновьев А.В., Емарлукова Я.В., Калмыков И.А., Высокоскоростные систолические отказоустойчивые процессоры цифровой обработки сигналов для инфотелекоммуникационных систем // Инфокоммуникационные технологии. Самара. – 2009. – №2. – С. 31-37

5. Калмыков И.А., Чипига А.Ф. Структура нейронной сети для реализации цифровой обработки сигналов повышенной разрядности // Наука. Инновации. Технологии. 2004. Т.38. С. 46.

6. Калмыков И.А. Устройство для коррекции ошибок в полиномиальной системе классов вычетов с использованием псевдоортогональных полиномов // Патент России № 2294529. 05.05.2005.

7. Калмыков И.А., Хайватов А.Б. Математическая модель отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов // Инфокоммуникационные технологии. – 2007. – Т.5. – №3. – С.39-42.

8. Калмыков И.А., Щелкунова Ю.О., Гахов Р.П., Шилов А.А. Математическая модель коррекции ошибок в полиномиальной системе классов вычетов на основе определения корней интервального полинома // Физика волновых процессов и радиотехнических систем. 2002. Т.6. № 5. С. 30.

9. Резеньков Д.Н., Калмыков И.А., Барильская А.В., Кихтенко О.А., Дагаева О.И. Устройство для коррекции ошибок в полиномиальной системе классов вычетов с использованием псевдоортогональных полиномов // Патент России № 239529 от 29.01.2008.

10. Червяков Н.И., Калмыков И.А., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронной сети для коррекции ошибок в непозиционном коде расширенного поля Галуа // Нейрокомпьютеры: разработка и применение. 2003. № 8-9. С. 10-17.