УДК [517.938 + 519.713/718]: 621.398

А. В. Ушаков, Е. С. Яицкая

РЕКУРРЕНТНОЕ СИСТЕМАТИЧЕСКОЕ ПОМЕХОЗАЩИТНОЕ ПРЕОБРАЗОВАНИЕ КОДОВ: ВОЗМОЖНОСТИ АППАРАТА ЛИНЕЙНЫХ ДВОИЧНЫХ ДИНАМИЧЕСКИХ СИСТЕМ

Рассматривается проблема формирования матричных компонентов векторно-матричного описания двоичных динамических систем помехозащитного преобразования кодов. Показано, что базис представления матричных компонентов зависит от проверочной и образующей матриц помехозащищенного кода, а также от его образующего модулярного многочлена.

Ключевые слова: *двоичная динамическая система, систематический помехозащищенный код, проверочная и образующая матрицы, образующий модулярный многочлен, помехозащитное преобразование кодов.*

В работах [1, 2], посвященных преобразованию кодов (ПК), представленных в виде кодовых последовательностей, получен конструктивный инструментарий модельного представления процедур ПК в виде линейных последовательностных машин (ЛПМ). Так как термин ЛПМ выпадает из общей теории систем, то со временем он был заменен понятием „линейная двоичная динамическая система “ (ЛДДС). Таким образом, ЛДДС, использующая в основном векторно-матричные модельные представления (ВММП) аппарата пространства состояний (АПС), со временем стала инструментом ПК, в том числе и помехозащитного преобразования систематических кодов в задачах кодирования и декодирования [3—5]. Из теории АПС [6] известно, что одной из проблем формирования векторно-матричного модельного представления динамических процессов над бесконечными и конечными полями является поиск базиса представления, в котором матричные компоненты ВММП обладают желаемыми исследователю свойствами. Причем возможность выбора базиса представления при построении ВММП процессов общего вида практически не ограничена. К сожалению, этого нельзя сказать о ВММП ЛДДС, использованных в задачах помехозащитного преобразования кодов.

Известно [7, 8], что систематическое помехозащитное преобразование кодов (ППК) в задачах кодирования и декодирования может быть осуществлено несколькими способами, основанными на различном описании процесса ППК. Тем не менее эти способы имеют единое функциональное представление, структурная реализация которого приведена на рис. 1, здесь КУ — помехозащитное кодирующее устройство, формирующее на своем выходе помехозащищенный код (ПЗК); КС — канал связи, выполняющий функцию среды искажения в задаче ППК; ДКУ — помехозащитное декодирующее устройство, формирующее на своем выходе синдром ошибки (факта или места искажения); ФСК — формирователь сигнала коррекции; $\oplus$ — сумматор по модулю два; $a(*)$ — помехонезащищенный информационный код (ПНЗИК); $y(*)$ — помехозащищенный код передачи; $\xi(*)$ — код помехи, воздействующей на код $y(*)$ при его передаче по КС; $f(*)$ — искаженный в КС ПЗК; $E(*)$ — код синдрома ошибки (факта или места искажения); $\eta(*)$ — код коррекции; $\hat{y}(*)$ — откорректированный принятый из КС код, удовлетворяющий условию

$$\hat{y}(*) = \arg\min_{\eta(*)}\left\{\left\| y(*) - \hat{y}(*)\right\|\right\}.$$

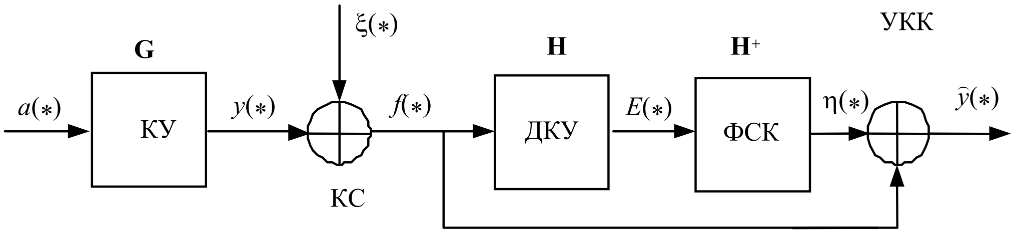

Рис. 1

Символ „$*$“ опускается, если все коды, использованные в процедуре помехозащитного преобразования, рассматриваются как векторы-строки, преобразование которых осуществляется в соответствии с векторно-матричными соотношениями:

$$y = a\mathbf{G},\ f = y + \xi,\ E = f\mathbf{H},\ \eta = E\mathbf{H}^{+},\ \hat{y} = f + \eta. \quad (1)$$

Операцию сложения следует понимать как процедуру суммирования по модулю два; $a:\dim a = k$; $y:\dim y = n$; $f:\dim f = n$; $\xi:\dim\xi = n$; $E:\dim E = m = n-k$; $\eta:\dim\eta = n$; $\hat{y}:\dim\hat{y} = n$; $\mathbf{G}$ — образующая $(k\times n)$-матрица ПЗК; $\mathbf{H}$ — проверочная $(n\times m)$-матрица ПЗК, которая удовлетворяет условию $\{\mathbf{G},\mathbf{H}\} = \arg\{\mathbf{GH} = 0\}$.

Если коды, используемые в процедуре помехозащитного преобразования кодов, рассматриваются как модулярные многочлены (ММ) над полем Галуа $\mathrm{GF}(p)\big|_{p=2}$, то символ „$*$“ принимает значение переменной x. При этом преобразование кодов-ММ осуществляется в соответствии с модулярными полиномиальными соотношениями:

$$\left.\begin{aligned}
&y(x) = a(x)x^m + r(x):\mathrm{rest}\frac{y(x)}{g(x)} = 0,\ r(x) = \mathrm{rest}\frac{a(x)x^m}{g(x)},\\
&f(x) = y(x) + \xi(x),\\
&E(x) = \mathrm{rest}\frac{f(x)}{g(x)} = \mathrm{rest}\frac{\xi(x)}{g(x)},\\
&\eta(x) = \xi(x), \hat{y}(x) = f(x) + \eta(x),
\end{aligned}\right\} \quad (2)$$

в которых $a(x):\deg a(x) = k-1$; $y(x):\deg y(x) = n-1$; $f(x):\deg f(x) = n-1$; $\xi(x):\deg\xi(x) = n-1$; $E(x):\deg E(x) = m-1$; $\eta(x):\deg\eta(x) = n-1$; $\hat{y}(x):\deg\hat{y}(x) = n-1$;

$g(x)$ — образующий модулярный многочлен ПЗК, представляющий собой неприводимый многочлен степени m, имеющий не менее $d_{\min} = 2s+1$ ненулевых элементов.

Символ „$*$“ принимает смысл дискретного времени q, выраженного в числе тактов длительности Δt, при этом все коды, используемые в процедуре помехозащитного преобразования, рассматриваются как кодовые последовательности, преобразование которых осуществляется рекуррентным образом в соответствии с векторно-матричными соотношениями, параметризованными дискретным временем q:

$$x_{\text{к}}(q+1) = \mathbf{A}_{\text{к}}\, x_{\text{к}}(q) + \mathbf{B}_{\text{к}}\, u_{\text{к}}(q);\; y(q) = \mathbf{N}u_{\text{к}}(q), \tag{3}$$

$$x_{\text{к}}(q+1) = \bar{\mathbf{A}}x_{\text{к}}(q);\; y(q) = \mathbf{C}_{\text{к}}x_{\text{к}}(q), \tag{4}$$

$$f(q) = y(q) + \xi(q), \tag{5}$$

$$x_{\text{д}}(q+1) = \mathbf{A}_{\text{д}}x_{\text{д}}(q) + \mathbf{B}_{\text{д}}u_{\text{д}}(q), \tag{6}$$

в которых $u_{\text{к}}(q) = a(q)$ — входная двоичная последовательность, представляющая собой вводимый в КУ ПНЗИК; $x_{\text{к}}$ — вектор состояния КУ, размерности $\dim x_{\text{к}} = m$; $y(q)$ — формируемая ПЗК-последовательность; $\mathbf{A}_{\text{к}}$ — $(m\times m)$-матрица состояния КУ; $\mathbf{B}_{\text{к}}$ — $(m\times 1)$-матрица входа КУ; $\mathbf{C}_{\text{к}} = \left[1\ \mathbf{O}_{1\times(n-1)}\right]$ — матрица выхода КУ; $\mathbf{N} = [1]$ — матрица вход—выход КУ; $\bar{\mathbf{A}}$ — нильпотентная матрица с индексом $\nu = m$; $u_{\text{д}}(q) = f(q)$ — входная двоичная последовательность, представляющая собой принятый из канала связи искаженный систематический ПЗК; $x_{\text{д}}$ — вектор состояния ДКУ размерности $\dim x_{\text{д}} = m$; $\mathbf{A}_{\text{д}}$ — $(m\times m)$-матрица состояния ДКУ; $\mathbf{B}_{\text{д}}$ — $(m\times 1)$-матрица входа ДКУ.

Постановка задачи. Ставится задача синтеза ЛДДС помехозащитного преобразования кодов с матрицами $\mathbf{A}_{\text{к}}, \mathbf{B}_{\text{к}}, \mathbf{A}_{\text{д}}, \mathbf{B}_{\text{д}}$, $\bar{\mathbf{A}}, \mathbf{C}_{\text{к}}, \mathbf{N}$ как функциями образующего модулярного многочлена ПЗК $g(x)$, его проверочной $\mathbf{H}$ и образующей $\mathbf{G}$ матриц:

$$\left\{\mathbf{A}_{\text{к}}, \mathbf{B}_{\text{к}}, \mathbf{A}_{\text{д}}, \mathbf{B}_{\text{д}}, \bar{\mathbf{A}}, \mathbf{C}_{\text{к}}, \mathbf{N}\right\} = \Psi\left(g(x), \mathbf{H}, \mathbf{G}\right).$$

Приведенные выше методы помехозащитного преобразования кодов характеризуются различным уровнем связи их аналитического описания с возможной аппаратной реализацией. Действительно, первый метод, представленный системой выражений (1), использующий векторно-матричное описание ППК, не параметризованное временем, приводит к системе скалярных аналитических выражений (САВ), которые позволяют строить устройства помехозащитного кодирования и декодирования [8].

Второй метод, представленный системой выражений (2), приводит к двум видам аппаратной реализации ППК: схемотехнической и программной, описываемой рекуррентными процедурами параметризованной дискретным временем q, задаваемыми соотношениями (3)—(6). Схемотехническая реализация ППК имеет две версии: первая строится по схеме „$g(x) \to (G, H) \to$ САВ“; вторая — по схеме „$g(x) \to$ УДММ $: \Phi(d) = g^{-1}(d) \to$ СР$\Phi(d)$“, УДММ — устройство деления ММ, СР$\Phi(d)$ — структурная реализация передаточной функции $\Phi(d)$.

Для формирования программной реализации устройств ППК в форме (3)—(6) сформулируем необходимые определение и утверждение.

Определение 1. Помехозащищенный (n,k)-код, множество кодовых комбинаций которого y_i мощностью $[y_i]=2^k$, описываемых модулярными многочленами $y_i(x)$, обладающими рекуррентным свойством

$$\operatorname{rest}\frac{y_i(x)}{g(x)}=0, \tag{7}$$

называется циклическим помехозащищенным кодом. □

Утверждение 1. Код, множество кодовых комбинаций которого формируется в соответствии с первым соотношением системы (2), обладает рекуррентным свойством (7), т.е. является циклическим ПЗК. □

Доказательство утверждения сводится к доказательству наличия у кода с ММ (2) рекуррентного свойства (7). Для этой цели полиномиальный компонент $a(x)x^m$ представим в форме $a(x)x^m=Q(x)g(x)+r(x)$. Если полученное выражение подставить в первое соотношение системы (2) и осуществить приведение по модулю два, то получим

$$y(x)=\{Q(x)g(x)+r(x)+r(x)\}\operatorname{mod}2=Q(x)g(x). \tag{8}$$

Нетрудно видеть, что представление (8) определяет наличие у $y(x)$ рекуррентного свойства (7). ■

По существу, первое выражение представления (2) ММ $y(x)$ циклического ПЗК содержит алгоритм его формирования в среде рекуррентного кодирующего устройства. При этом КУ функционирует посредством коммутации структуры. Это вызвано тем, что при формировании (n,k)-кода в течение первых *k* тактов *k*-разрядная информационная часть в виде кодовой последовательности одновременно подается в КС и на вход УДММ для вычисления остатка в форме

$$x^T(Q)=K\left\{\operatorname{rest}\left(\frac{a(x)x^m}{g(x)}\right)\right\}.$$

По принятии информационной части из источника дискретной информации (ИДИ) вход КС переключается с выхода ИДИ на выход УДММ, в котором сформировался остаток. Все обратные связи в УДММ в этот момент разрываются, процесс деления останавливается, а УДММ без связей становится *m*-разрядным регистром сдвига. Все перечисленные коммутации цепей и связей осуществляются специально вводимым в состав КУ устройством коммутации (УК). Таким образом, помехозащитное КУ представляет собой объединение УДММ и УК, функционирующее в два этапа. На первом оно описывается ЛДДС вида (3), а на втором — вида (4).

Третье выражение представления (2) ММ $E(x)$ синдрома ошибки по существу описывает алгоритм функционирования рекуррентного декодирующего устройства, который предназначен для проверки сохранности рекуррентного свойства (7) применительно к принятому из КС искаженному коду с ММ $f(x)=y(x)+\xi(x)$ путем деления этого многочлена на образующий $g(x)$. Если $E(x)=0$, то принимается решение, что $f(x)=y(x)$. Если $E(x)\neq0$, то синдром используется как адрес искажений кода. Помехозащитное ДКУ есть функциональное объединение УДММ и устройства съема синдрома, отражающее состояние УДММ в момент $q=n$ так, что код

$$K\{E(x)\}=x_{\text{Д}}^T(q)\Big|_{q=n}.$$

Таким образом, УДММ в фазе вычисления остатка описывается ЛДДС вида (6).

Утверждение 2. Матрица $\mathbf{B}_{\text{к}}$ ЛДДС УДММ кодирующего устройства (3) с точностью до операции транспонирования совпадает с последней (k-й) строкой $\tilde{\mathbf{G}}^k$ матрицы $\tilde{\mathbf{G}}$, входящей в состав образующей матрицы $\mathbf{G} = \begin{bmatrix} \mathrm{I}_{(k \times k)} & \tilde{\mathbf{G}} \end{bmatrix}$ так, что выполняется соотношение

$$\mathbf{B}_{\text{к}}^T = \tilde{\mathbf{G}}^k = \mathrm{K}\left\{ g(x) + x^m \right\}, \tag{9}$$

где $\mathrm{K}\left\{ (\bullet) \right\}$ — код ММ $(\bullet)$. □

Доказательство. Рассмотрим процесс кодирования для случая помехонезащищенного кода a, имеющего единицу только в младшем разряде, а в остальных — нули $\left\{ \text{ММ} : a(x) = 1 \right\}$. Это значит, что входная последовательность $u_{\text{к}}(q)$ с учетом передачи кодов и ММ старшим разрядом вперед будет иметь вид

$$u_{\text{к}}(q) = \left[u_{\text{к}}(0) = 0,\, u_{\text{к}}(1) = 0, \ldots,\, u_{\text{к}}(k-2) = 0,\; u_{\text{к}}(k-1) = 1, u_{\text{к}}(k) = 0 \ldots \right].$$

В течение первых $(k-1)$ тактов ЛДДС УДММ кодирующее устройство будет находиться в нулевом состоянии. При приеме элемента $u_{\text{к}}(q)\big|_{q=k-1} = 1$ ЛДДС устройство деления модулярного многочлена КУ в силу (3) перейдет в состояние

$$x_{\text{к}}(q+1)\big|_{q+1=k} = A_{\text{к}} x_{\text{к}}(q)\Big|_{x_{\text{к}}(q)\big|_{q=\overline{0,k-1}} = 0} + B_{\text{к}}\, u_{\text{к}}(q)\Big|_{u_{\text{к}}(q)\big|_{q=k-1} = 1}\; \Bigg| = \mathbf{B}_{\text{к}}.$$

Данное соотношение в транспонированном виде $\left\{ x_{\text{к}}(k) = \mathbf{B}_{\text{к}} \right\}^T$ определяет код

$$\mathrm{K}\left\{ \operatorname{rest} \frac{a(x) x^m}{g(x)} \Bigg|_{a(x)=1} = \operatorname{rest} \frac{x^m}{g(x)} = g(x) + x^m \right\}$$

остатка от деления, выводимый из КУ и задаваемый последней k-й строкой $\tilde{\mathbf{G}}^k$ матрицы $\tilde{\mathbf{G}}$ кодов остатков так, что выполняется цепочка равенств

$$x_{\text{к}}^T(k) = \mathbf{B}_{\text{к}}^T = \tilde{\mathbf{G}}^k = \mathrm{K}\left\{ g(x) + x^m \right\}. \qquad \blacksquare$$

Соотношение (9) совместно с представлением функционирования рекуррентного КУ позволяет сконструировать его векторно-матричное описание в форме ЛДДС вида (3)—(4).

Алгоритм 1 (А1) формирования матриц $\left\{ \mathbf{A}_{\text{к}}, \mathbf{B}_{\text{к}}, \overline{\mathbf{A}}, \mathbf{C}_{\text{к}}, \mathbf{N} \right\} = \Psi\left(g(x), \mathbf{G} \right)$

ЛДДС рекуррентного помехозащитного кодирования

1. По заданному информационному массиву W мощности $\left[W \right] = V_u$ определить размерность k помехонезащищенного информационного кода в силу соотношения $k = \min \arg \left\{ 2^k \geq V_u = \left[W \right] \right\}$.

2. По заданным категории системы, характеризующейся величиной $P_{\text{доп}}$ — допустимой вероятностью приема ложной команды, и параметру модели двоичного канала связи в форме p — вероятностью искажения разряда (бита) кода, заданному выражением $p = \max\left\{ p_{01}, p_{10} \right\}$, определить кратность исправляемой ошибки s

$$s = \min \arg \left\{ N_{\text{с}} = 2^m - 1 \geq N_{\text{ош}} = \sum_{i=1}^{s} C_n^i \;\&\; \sum_{i=s+1}^{n} C_n^i p^i (1-p)^{n-i} \leq P_{\text{доп}} \right\},$$

где $N_{\text{с}}$ — число синдромов, $N_{\text{ош}}$ — число исправляемых ошибок.

3. В зависимости от величины s-кратности исправляемой ошибки — выбрать из таблиц неприводимых многочленов или сформировать с помощью БЧХ-технологии [9] реализацию образующего ММ $g(x)$ степени m и сформировать (n,k)-формат помехозащищенного кода, где n удовлетворяет условию $n = k + m$.

4. Вычислить D-образ ММ $g(x)$ в форме

$$g(d) = \mathsf{D}\{g(x)\} = \tilde{g}\left(x^{-1}\right)\Big|_{x^{-1}=d}, \text{ где } \tilde{g}\left(x^{-1}\right) = x^{-m}g(x).$$

5. Сконструировать передаточную функцию $\Phi_{\text{к}}(d)$ УДММ КУ на образующий ММ $g(x)$ в форме $\Phi_{\text{к}}(d) = \dfrac{1}{g(d)}$.

6. Пользуясь правилом Мейсона не касающихся контуров, построить две предварительные структурные реализации передаточной функции $\Phi_{\text{к}}(d)$ на элементах памяти (ЭП) с передаточной функцией $\Phi_{\text{ЭП}}(d) = d$ в двух канонических базисах.

7. Произвести разметку входов и выходов ЭП каждой структурной реализации переменными $x_{\text{к}i}(q+1)$ на входе и $x_{\text{к}i}(q)$ на выходе, присвоив выходу самого правого ЭП переменную $x_{\text{к}1}(q)$, а его входу — $x_{\text{к}1}(q+1)$, и сформировать векторно-матричное описание (ВМО) автономной версии УДММ $x_{\text{к}}(q+1) = \mathbf{A}_{\text{к}} x_{\text{к}}(q)$, „списав“ реализации матриц $\mathbf{A}_{\text{к}}$ с отмеченных структурных реализаций $\Phi_{\text{к}}(d)$.

8. Сформировать матрицу входа $\mathbf{B}_{\text{к}}$ УДММ КУ (3) в форме (9).

9. Структурно с использованием правила Мейсона или аналитически определить передаточные функции УДММ КУ (3) для двух базисных реализаций матрицы $\mathbf{A}_{\text{к}}$ состояния УДММ для процесса кодирования как $\Phi_{\text{к}}(d) = \mathbf{C}_{\text{к}}\left(d^{-1}\mathbf{I} + \mathbf{A}_{\text{к}}\right)^{-1}\mathbf{B}_{\text{к}}$.

10. Выбрать для дальнейшего использования структурную реализацию передаточной функции УДММ КУ, отмеченная версия которой характеризуется матрицей $\mathbf{A}_{\text{к}}$ ее состояния, удовлетворяющей условию $\mathbf{A}_{\text{к}} = \arg\left\{g^{-1}(d) = \mathbf{C}_{\text{к}}\left(d^{-1}\mathbf{I} + \mathbf{A}_{\text{к}}\right)^{-1}\mathbf{B}_{\text{к}}\right\}$.

11. Сформировать матрицу $\bar{\mathbf{A}}$ УДММ КУ, переведенного в режим регистра сдвига, по отмеченной версии, выбранной в п. 10 структурной реализации $\Phi(d)$ с разорванными обратными связями.

12. Дополнить УДММ УК устройством коммутации структуры УДММ и точки подключения входа канала связи с выхода ИДИ на выход устройства деления модулярных многочленов.

13. На конкретном примере проверить правильность функционирования устройства рекуррентного кодирования, задаваемого парой ВМО (3) и (4) со сформированными матрицами $(\mathbf{A}_{\text{к}}, \mathbf{B}_{\text{к}}, \mathbf{N})$ и $(\bar{\mathbf{A}}, \mathbf{C}_{\text{к}})$. ■

Утверждение 3. Матрица $\mathbf{B}_{\text{д}}$ входа декодирующего рекуррентного устройства (6) удовлетворяет соотношению

$$\mathbf{B}_{\text{д}} = \left(\mathbf{H}^{n}\right)^{T}. \tag{10}$$

Доказательство этого утверждения использует тот факт, что синдром E, вычисляемый в соответствии с соотношением $E = f\mathbf{H}$, удовлетворяет цепочке

$E = f\mathbf{H} = \left(y + \xi\right)\mathbf{H} = \left(a\mathbf{G} + \xi\right)\mathbf{H} = a\mathbf{GH} + \xi\mathbf{H}\Big|_{\mathbf{GH}=0} = \xi\mathbf{H}$ равенств. Это соотношение показывает, что в ВМО (6) процесса декодирования можно положить $u_д\left(q\right) = \xi\left(q\right)$ так, что оно с учетом (5) принимает вид

$$x_д\left(q+1\right) = \mathbf{A}_д x_д\left(q\right) + \mathbf{B}_д \xi\left(q\right),\ x_д\left(0\right)=0. \tag{11}$$

Выражение (11) используем при формировании синдромов ошибок, которые образуют строки проверочной матрицы $\mathbf{H}$ в силу соотношения $\mathbf{H}^{n+1-i} = E^i$, где E^i — синдром ошибки в i-м разряде принятого из КС искаженного ПЗК, $\mathbf{H}^{n+1-i}$ — $\left(n+1-i\right)$-я строка матрицы $\mathbf{H}$. Тогда в соответствии с (6) и при условии $\xi\left(q\right): 000\ldots001$ входная последовательность $u_д\left(q\right)$ будет иметь вид $u_д\left(q\right) = \left[\, u_д\left(0\right) = 0,\ u_д\left(1\right) = 0, \ldots, u_д\left(n-2\right) = 0,\ u_д\left(n-1\right) = 1, u_д\left(n\right) = 0\ldots\right]$.

В течение первых $\left(n-1\right)$ тактов ЛДДС устройство деления модулярных многочленов ДКУ будет находиться в нулевом состоянии. При приеме элемента $u_д\left(q\right)\Big|_{q=n-1} = 1$ ЛДДС УДММ КУ в соответствии с (6) перейдет в состояние

$$x_д\left(q+1\right)\Big|_{q+1=n} = A_д x_д\left(q\right)\Big|_{x_д\left(q\right)\big|_{q=\overline{0,n-1}}=0} + B_д\, u_д\left(q\right)\Big|_{u_д\left(q\right)\big|_{q=n-1}=1}\Bigg| = \mathbf{B}_д\,.$$

Данное соотношение в транспонированном виде $\left\{x_д\left(n\right) = \mathbf{B}_д\right\}^T$ определяет код

$$\mathrm{K}\left\{\mathrm{rest}\,\frac{\xi\left(x\right)}{g\left(x\right)}\Bigg|_{\xi\left(x\right)=1} = \mathrm{rest}\,\frac{1}{g\left(x\right)} = 1\right\}$$

остатка от деления, вводимого из КС в ДКУ кода ошибки с ММ $\xi\left(x\right) = 1$, задающей синдром E ошибки в младшем разряде и задаваемой последней (n-й) строкой $\mathbf{H}^n$ проверочной матрицы $\mathbf{H}$ так, что выполняется цепочка равенств

$$E^i\Big|_{i=1} = x_д^{\ T}\left(n\right)\Big|_{\substack{u_д\left(n-1\right)=1 \\ u_д\left(q\right)=0;\, q=\overline{0,n-2}}} = \mathbf{B}_д^{\ T} = \mathbf{H}^{n+1-i}\Big|_{i=1} = \mathbf{H}^n\,. \qquad \blacksquare$$

Соотношение (10) совместно с описанием функционирования рекуррентного ДКУ позволяет сконструировать его векторно-матричное описание в форме ЛДДС вида (6).

Алгоритм 2 (А2) формирования матриц $\left\{\mathbf{A}_д, \mathbf{B}_д\right\} = \Psi\left(g\left(x\right),\ \mathbf{H}\right)$

ЛДДС рекуррентного помехозащитного декодирования

1. Выполнить пп. 1—4 алгоритма А1 синтеза рекуррентного КУ.

2. Сконструировать передаточную матрицу-столбец $\Phi_д\left(d\right) = \arg\left\{x_д\left(d\right) = \Phi_д\left(d\right) u_д\left(d\right)\right\}$ УДММ ДКУ на образующий ММ $g\left(x\right)$ в форме $\Phi_д\left(d\right) = \dfrac{1}{g\left(d\right)}\mathrm{col}\left(\Phi_j\left(d\right); j = \overline{1,m}\right)$, где передаточные функции $\left(\Phi_j\left(d\right); j = \overline{1,m}\right)$ подлежат вычислению.

3. В качестве матрицы $\mathbf{A}_д$ состояния векторно-матричного описания УДММ ДКУ (6) принять матрицу $\mathbf{A}_к$, удовлетворяющую условиям п. 9 алгоритма А1 так, что становится справедливым матричное соотношение $\mathbf{A}_д = \mathbf{A}_к = \mathbf{A}$.

4. Сформировать матрицу $\mathbf{B}_д$ входа ВМО (6) УДММ ДКУ с помощью соотношения (10).

5. Структурно, реализовав ВМО (6) УДММ ДКУ с матрицами $\left(\mathbf{A}_{\text{Д}}, \mathbf{B}_{\text{Д}}\right)$, сформированными в п. 3, 4, графически, с помощью правила Мейсона, или аналитически, с помощью соотношения $\Phi_{\text{Д}}(d) = \left(d^{-1}\mathbf{I} + \mathbf{A}_{\text{Д}}\right)^{-1} \mathbf{B}_{\text{Д}}$, сформировать передаточную матрицу-столбец $\Phi_{\text{Д}}(d) = g^{-1}(d)\mathrm{col}\left(\Phi_j(d); j = \overline{1,m}\right)$, с последующим вычислением $\mathrm{col}\left(\Phi_j(d); j = \overline{1,m}\right) = g(d)\left(d^{-1}\mathbf{I} + \mathbf{A}_{\text{Д}}\right)^{-1} \mathbf{B}_{\text{Д}}$.

6. На конкретном примере проверить правильность функционирования устройства рекуррентного декодирования (6) со сформированной парой матриц $\left(\mathbf{A}_{\text{Д}}, \mathbf{B}_{\text{Д}}\right)$. ■

Пример. На основе использования алгоритмов синтеза рекуррентных кодирующих и декодирующих устройств осуществлено их проектирование по следующим исходным данным. Пусть массив сообщений W характеризуется мощностью $\left[W\right] = V_u = 120$ и кратностью исправляемой ошибки $s = 2$. Схемы кодирующего и декодирующего устройств приведены на рис. 2 и 3 соответственно.

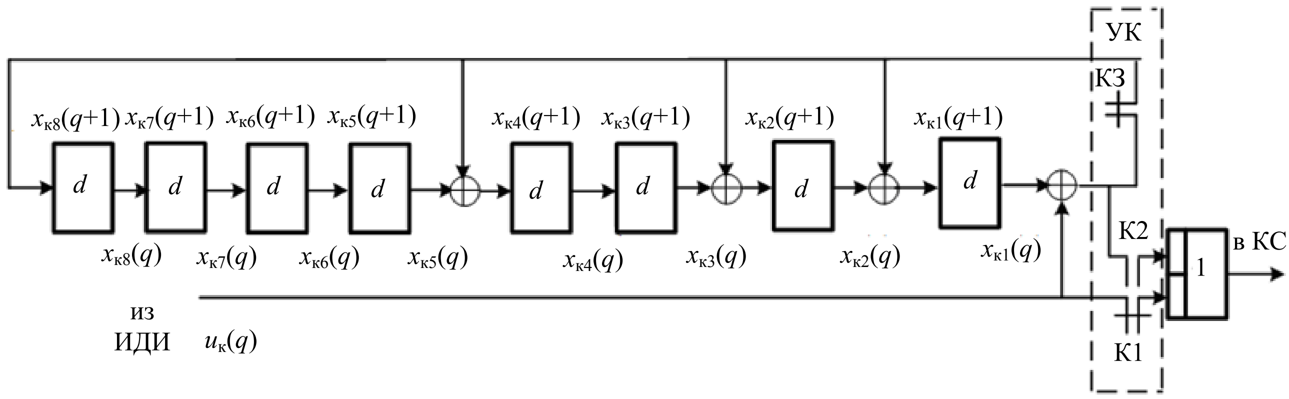

Рис. 2

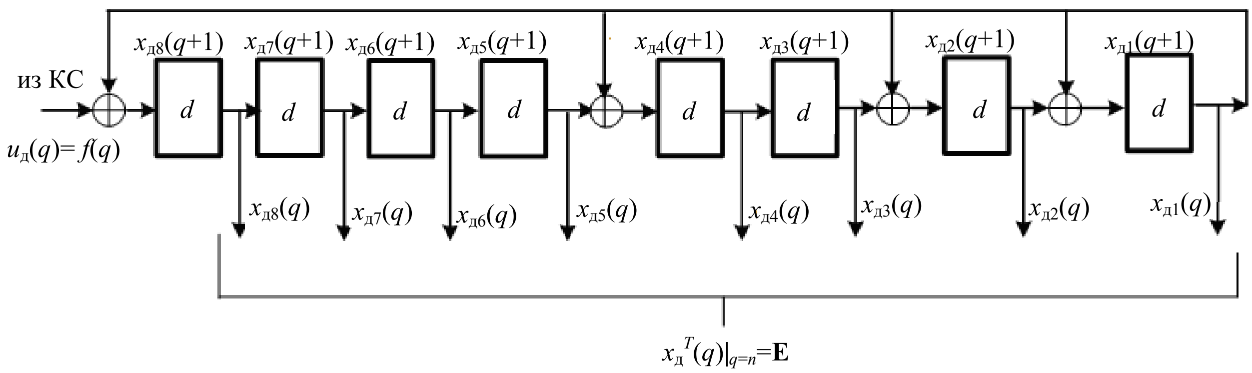

Рис. 3

Заключение. Поставленная задача решена. Показано, что представление процессов преобразования кодов в задаче помехозащитного кодирования и декодирования средствами линейных двоичных динамических систем на основе связи матриц входа с образующей и проверочной матрицами имеет элегантную алгоритмическую поддержку.

СПИСОК ЛИТЕРАТУРЫ

1. *Гилл А.* Линейные последовательностные машины. М.: Наука, 1974.

2. *Фараджев Р. Г.* Линейные последовательностные машины. М.: Сов. радио, 1975.

3. *Кирюшин А. А., Рассветалова Л. А., Ушаков А. В.* Модальное управление в задаче синтеза двоичных динамических систем в логике линейных триггеров // Автоматика и телемеханика. 1993. № 7.
4. *Рассветалова Л. А., Ушаков А. В.* Двоичное динамическое наблюдение в задаче помехоустойчивого кодирования // Автоматика и телемеханика. 1993. № 6.
5. *Ушаков А. В.* Синтез циклических кодирующих и декодирующих устройств в логике произвольных триггеров // Автоматика и телемеханика. 1997. № 11.
6. *Заде Л., Дезоер Ч.* Теория линейных систем. М.: Наука, 1970.
7. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976.
8. *Тутевивич В. Н.* Телемеханика. М.: Высш. школа, 1985.
9. *Мельников А. А., Ушаков А. В.* Двоичные динамические системы дискретной автоматики. СПб: СПбГУ ИТМО, 2005.
10. *Rosenthal J.* Some interesting problems in systems theory which are of fundamental importance in coding theory // Proc. 36th Conf. Decision Control. San Diego, CA, 1997. Vol. 5. P. 4574—4579.

Сведения об авторах

Анатолий Владимирович Ушаков — д-р техн. наук, профессор; Санкт-Петербургский государственный университет информационных технологий, механики и оптики, кафедра систем управления и информатики; E-mail: ushakov-AVG@yandex.ru

Елена Сергеевна Яицкая — аспирант; Санкт-Петербургский государственный университет информационных технологий, механики и оптики, кафедра систем управления и информатики; E-mail: yaitskayaes@mail.ru

Рекомендована кафедрой
систем управления и информатики

Поступила в редакцию
27.09.10 г.