УДК [517.938 + 519.713/.718]: 621.398

ФОРМИРОВАНИЕ БАНКА ПРОВЕРОЧНЫХ МАТРИЦ СИСТЕМАТИЧЕСКИХ ПОМЕХОЗАЩИЩЕННЫХ КОДОВ С ПОМОЩЬЮ МАТРИЧНОГО МУЛЬТИПЛИКАТИВНОГО КОМПОНЕНТА

А.В. Ушаков, Е.С. Яицкая

С помощью невырожденного матричного мультипликативного компонента формируется банк проверочных матриц систематических помехозащищенных кодов.

Ключевые слова: помехозащитное преобразование кодов, проверочная и образующая матрицы.

Помехозащитное преобразование кодов (ППК) представляет собой пятифазный процесс: помехозащитное кодирование (ПК) помехонезащищенного информационного кода (ПНЗИК); искажение помехозащищенного кода (ПЗК) при передаче по двоичному каналу связи (КС); помехозащитное декодирование (ПД) с целью формирования синдрома (опознавателя) ошибки, свидетельствующего о факте, а, возможно, и месте ошибки в коде; формирование сигнала коррекции (ФСК) и коррекция [1].

Алгоритмически ППК может быть описано тремя способами:

1. $y = a\mathbf{G}$; $f = y \oplus \xi$; $E = f\mathbf{H}$; $\hat{\xi} = E\mathbf{H}^{+}$; $\hat{y} = f \oplus \hat{\xi}$;
2. $y(x) = \arg\left\{rest\left(y(x)g^{-1}(x) = 0\right)\right\}$; $f(x) = y(x) \oplus \xi(x)$; $E(x) = rest\left(f(x)g^{-1}(x)\right)$; $\hat{\xi}(x) = \hat{\xi}(E(x))$; $\hat{y}(x) = f(x) \oplus \hat{\xi}(x)$;
3. $y(k) = \mathbf{N}a(k)$; $x_{\text{к}}(k+1) = \mathbf{A}x_{\text{к}}(k) \oplus \mathbf{B}_{\text{к}}a(k),\ k = \overline{1, k_{\text{и}}}$; $\bar{x}_{\text{к}}(k+1) = \bar{\mathbf{A}}\bar{x}_{\text{к}}(k), k = \overline{1, m}$; $\bar{x}_{\text{к}}(0) = x_{\text{к}}(k_{\text{и}})$; $y(k) = \mathbf{C}\bar{x}_{\text{к}}(k)$; $f(k) = y(k) \oplus \xi(k)$; $x_{\text{д}}(k+1) = \mathbf{A}x_{\text{д}}(k) \oplus \mathbf{B}_{\text{д}}f(k), k = \overline{1, n}$; $E = x_{\text{д}}^{'}(n)$; $\hat{\xi} = E\mathbf{H}^{+}$; $\hat{y} = \text{row}\left\{f(k), k = \overline{1, n}\right\} \oplus \hat{\xi}$,

где $a(*)$ – ПНЗИК; $y(*)$ – ПЗК; $\xi(*)$ – код помехи в КС, искажающей код $y(*)$ в аддитивной форме; $f(*)$ – искаженный в КС ПЗК; $E(*)$ – код синдрома факта или места искажения; $\hat{\xi}(*)$ – код коррекции; $\hat{y}(*)$ – откорректированный принятый из КС код, удовлетворяющий условию $\hat{y}(*) = \arg\min\limits_{\hat{\xi}(*)}\left\{\left\|y(*) - \hat{y}(*)\right\|\right\}$;

$x_{\text{к}}, \bar{x}_{\text{к}}$ – векторы состояния кодирующего устройства (КУ), размерности $\dim x_{\text{к}} = \dim \bar{x}_{\text{к}} = m$; $\mathbf{B}_{\text{к}}$ – $(m \times 1)$-матрица входа КУ; $\mathbf{C} = \left[1\ \mathbf{O}_{1\times(n-1)}\right]$- матрица выхода КУ [2]; $\mathbf{N} = [1]$ – матрица вход-выход КУ; $\bar{\mathbf{A}}$ – нильпотентная матрица с индексом $v = m$; $x_{\text{д}}$ – вектор состояния декодирующего устройства (ДКУ), размерности $\dim x_{\text{д}} = m$; $\mathbf{A}$ – $(m \times m)$-матрица состояния КУ и ДКУ; $\mathbf{B}_{\text{д}}$ – $(m \times 1)$ - матрица входа ДКУ [2]; $\mathbf{G} - (k_{\text{и}} \times n)$-образующая матрица ПЗК; $\mathbf{H} - (n \times m)$- проверочная матрица ПЗК.

Символ «$*$» опускается, если все коды, задействованные в процедуре ППК, рассматриваются как вектора-строки; принимает значение переменной x, если коды рассматриваются как модулярные многочлены (ММ) над полем Галуа $GF(p)\big|_{p=2}$; принимает смысл дискретного времени k, выраженного в числе тактов длительности Δt, если все коды рассматриваются как кодовые последовательности, преобразование которых осуществляется рекуррентным образом в силу векторно-матричных соотношений, параметризованных дискретным временем k.

Примечание 1. Помехозащитное ДКУ формирует:

1. нулевой код синдрома $\text{E} = 0$ в случае отсутствия искажений в принятом коде ($\xi = 0$);
2. ненулевой код синдрома $\text{E} \neq 0$ в случае наличия искажений в принятом коде ($\xi \neq 0$).

Выясним, каким свойством должна обладать пара матриц $(\mathbf{G}, \mathbf{H})$ с тем, чтобы она порождала ПЗК. С этой целью сформулируем утверждение.

Утверждение 1 (У.1). Пара $(\mathbf{G}, \mathbf{H})$ порождает ПЗК при необходимом условии $\mathbf{GH} = \mathbf{O}$. □ (1)

Доказательство строится на использовании системы соотношений

$y = a\mathbf{G}; f = y \oplus \xi; E = f\mathbf{H} = (y \oplus \xi)\mathbf{H} = (a\mathbf{G} \oplus \xi)\mathbf{H} = a\mathbf{GH} \oplus \xi\mathbf{H}\big|_{\xi=0} = a\mathbf{GH} = \mathbf{O} \rightarrow \mathbf{GH} = \mathbf{O}$. ■

Ставится задача формирования банка проверочных матриц систематических ПЗК с помощью невырожденного матричного мультипликативного компонента.

Основным результатом исследования является следующее утверждение.

Утверждение 2 (У.2). Умножение проверочной матрицы $\mathbf{H}$ справа на невырожденную произвольную $(m \times m)$-матрицу $\mathbf{P}$ порождает матрицу $\tilde{\mathbf{H}} = \arg\left\{\mathbf{G}\tilde{\mathbf{H}} = \mathbf{O}\right\}$, при этом $\tilde{\mathbf{H}}$ также является проверочной матрицей ПЗК. □

Доказательство. Подстановка $\tilde{\mathbf{H}} = \mathbf{HP}$ в (1) дает: $\mathbf{G}\tilde{\mathbf{H}} = \mathbf{GHP} = (\mathbf{GH})\mathbf{P} = (\mathbf{O})\mathbf{P} = \mathbf{O}$. ■

Примечание 2. Максимальная мощность банка проверочных матриц $\tilde{\mathbf{H}}$ достигается при $\mathbf{P}=\mathbf{A}^l$, $l=\overline{0,n-1}$, если $(m\times m)$-матрица $\mathbf{A}$ имеет неприводимый характеристический ММ и принадлежит показателю $\mu=2^m-1$.

Для подтверждения основного результата приведем иллюстративный пример.

Рассмотрим ПЗК, задаваемый неприводимым ММ $g(x)=x^3+x+1$. Тогда ППК характеризуется следующими компонентами:

$$\mathbf{H}=\begin{bmatrix}1&0&1\\1&1&1\\1&1&0\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix};\mathbf{G}=\begin{bmatrix}1&0&0&0&1&0&1\\0&1&0&0&1&1&1\\0&0&1&0&1&1&0\\0&0&0&1&0&1&1\end{bmatrix};\mathbf{A}=\begin{bmatrix}0&1&0\\1&0&1\\1&0&0\end{bmatrix},$$

причем условие (1) выполняется, и матрица $\mathbf{A}$ принадлежит показателю $\mu=2^m-1=2^3-1=7$.

Сформируем проверочную матрицу $\tilde{\mathbf{H}}$ согласно утверждению **У.2**, приняв $\mathbf{P}=\mathbf{A}^4=\begin{bmatrix}1&1&1\\0&1&1\\1&1&0\end{bmatrix}$:

$$\tilde{\mathbf{H}}=\mathbf{HP}=\begin{bmatrix}1&0&1\\1&1&1\\1&1&0\\0&1&1\\1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}1&1&1\\0&1&1\\1&1&0\end{bmatrix}=\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\\1&0&1\\1&1&1\\0&1&1\\1&1&0\end{bmatrix},$$

при этом выполняется условие утверждения **У.1** $\mathbf{G}\tilde{\mathbf{H}}=\mathbf{O}$, т.е. пара матриц $\left(\mathbf{G},\tilde{\mathbf{H}}\right)$ порождает ПЗК.

Полученный банк проверочных матриц позволяет обеспечить скрытность процесса ППК.

1. Ушаков А.В., Яицкая Е.С. Рекуррентное систематическое помехозащитное преобразование кодов: возможности аппарата линейных двоичных динамических систем // Изв. вузов. Приборостроение. – 2011. – Т. 54. – № 3. – С. 17–25.
2. Ушаков А.В., Яицкая Е.С. Динамическое наблюдение нелинейных двоичных динамических систем // Научно-технический вестник СПбГУ ИТМО. – 2010. – Т. 68. – № 4. – С. 38–44.

Ушаков Анатолий Владимирович – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, доктор технических наук, профессор, ushakov-AVG@yandex.ru
Яицкая Елена Сергеевна – Санкт-Петербургский государственный университет информационных технологий, механики и оптики, аспирант, yaitskayaes@mail.ru