СИСТЕМЫ ОБРАБОТКИ И ЗАЩИТЫ ИНФОРМАЦИИ

УДК 681.3.06:519.248.681

И.Д. ГОРБЕНКО, д-р техн. наук, А.А. ЗАМУЛА, д-р техн. наук

АНАЛИТИЧЕСКАЯ ОЦЕНКА ЗНАЧЕНИЙ МАКСИМАЛЬНЫХ БОКОВЫХ ЛЕПЕСТКОВ ФУНКЦИЙ КОРРЕЛЯЦИИ СЛОЖНЫХ НЕЛИНЕЙНЫХ ДИСКРЕТНЫХ СИГНАЛОВ

Введение

Используемые в информационно-коммуникационных системах (ИКС) в качестве физических переносчиков данных множества линейных дискретных сигналов не позволяют в ряде случаев обеспечить необходимые показатели информационной безопасности и помехозащищенности [1 – 5]. Они могут быть улучшены посредством применения систем нелинейных дискретных сигналов. Однако для этого необходимо оценивать граничные значения корреляционных функций, например минимаксные свойства и соответствие границе «плотной упаковки».

В [3] указаны принципиально достижимые значения максимальных боковых пиков периодической функции автокорреляции (ПФАК), т.е. соответствие границы «плотной упаковки» в зависимости от заданного периода последовательности N:

$$R_{max}^{a} \geq \begin{cases} 0, \text{ если } N \equiv 0 (\text{mod } 4); \\ 1, \text{ если } N \equiv 1 (\text{mod } 4); \\ 2, \text{ если } N \equiv 2 (\text{mod } 4); \\ -1, \text{ если } N \equiv 3 (\text{mod } 4), \end{cases} \quad (1)$$

Приведенные границы устанавливают критерий синтеза множества ДП (сигнатур). Ансамбли, со значениями R_{max}, достигающие предела, предсказываемого границами (1), являются оптимальными по критерию корреляционного пика и называются минимаксными.

Цель настоящей статьи – получение аналитических соотношений минимаксных оценок корреляционных свойств широкого класса нелинейных дискретных сигналов с учетом ограничений (1).

Постановка задачи исследований

К числу привлекательных для рассмотрения, с точки зрения корреляционных и ансамблевых свойств, отнесем нелинейные характеристические дискретные сигналы (ХДС) с числом позиций $N = 4x + 2$ и $N = 4x, x = 1, 2, \ldots$[5]. Построение данных ХДС базируется на использовании характера мультипликативной группы $\Psi(x)$ поля $GF\left(P^n\right), n \geq 1$.

Правило построения таких ДП для $L = 4x + 2$ имеет вид:

$$\mu = \{\mu_i : i = 0, 1, ..., P - 2\}$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } P), \quad (2)$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0 (\text{mod } P), \quad (3)$$

где Θ – первообразный элемент поля $GF(P)$.

Для $L = 4x$ правило кодирования имеет вид:

$$\mu = \{\mu_i : i = 0, 1, ..., P - 2\}$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\text{mod } P),$$

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0(\text{mod } P), \quad (4)$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0(\text{mod } P),$$

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0(\text{mod } P). \quad (5)$$

В [5] показано, что мощность метода данного класса сигналов (M) равна числу классов не инверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы на смежные классы по классу автоморфных коэффициентов, и определяется как $M = \phi(L)/2\cdot$, где (φ(L)) – функция Эйлера. Известно также [5], что правила (2) – (5) приводят к ДП с двухуровневой периодической функцией автокорреляции (ПФАК) и значения боковых пиков ПФАК для правил (2) – (3) составляет $R_\mu = \{-2, 2\}$, а для правил кодирования (4) и (5) значения боковых пиков ПФАК составляет $R_\mu = \{0, -4\}$ и $R_\mu = \{0, 4\}$ соответственно.

В соответствии с (1) системы таких нелинейных ХДС являются плотноупакованными по периодической функции корреляции (ПФАК), существуют для большого спектра длительностей N, однако размерность ансамбля ХДС ограничена значением функции Эйлера от периода сигнала. Проведенные исследования показали [6 – 10], что дальнейшее увеличение размерности ансамбля и улучшение структурных свойств сигналов, составляющих ансамбль, может быть достигнуто на основе использования L-позиционных (производных) нелинейных сигналов, построение которых осуществляется посредством образования последовательного произведения $Z_i, i = \overline{1,k}$, символов W_j^i нелинейных сигналов с одно- или двухуровневой ПФАК.

Аналитические оценки корреляционных свойств производных нелинейных сигналов

Правило построения символов W_i^p производных нелинейных сигналов (ПНС) сформулируем в виде

$$W_i^p = \prod_{j=1}^{k} W_{i(\text{mod}\, L_i),j} \quad (6)$$

Значения боковых пиков ПФАК, для ПНС, построенных по (1), найдем, используя соотношение $r_j(l) = \sum_{i=1}^{L-m} W_i^j \left(W_{i+l}^j\right)^*$:

$$R_w^p(l) = \sum_{i=0}^{L-1} \prod_{j=r}^{K_1} W_{i(\text{mod}\, L_i),j} \prod_{j=1}^{K_2} W_{i+l(\text{mod}\, L_i),j}, \quad (7)$$

где $K_1 \neq K_2$.

Анализ корреляционных свойств с использованием (45) в общем виде затруднен, поэтому рассмотрим ряд частных случаев, важных как с теоретической, так и с практической точек зрения.

1. Пусть $K_1 = K_2$, а $L_1 \neq L_2$, тогда (7) имеет вид

$$R_w(l) = \sum_{i=0}^{L-1} W_{i(\text{mod}\, L_1),i} \cdot W_{i+l(\text{mod}\, L_1),1} \cdot W_{i(\text{mod}\, L_1),2} \cdot W_{i+l(\text{mod}\, L_2),2}. \quad (8)$$

Для преобразования (8) представим индекс суммирования i в L_2-ричной системе счисления как

$$i = \upsilon L_2 + \varepsilon, \quad 0 \le \varepsilon \le L_2, \; 0 \le \upsilon \le L_1 \tag{9}$$

$$R_w(l) = \sum_{\upsilon=0}^{L_1-1}\sum_{\varepsilon=0}^{L_2-1} W_{\upsilon L_2+\varepsilon(\mathrm{mod}\,L_1),1}\cdot W_{\upsilon L_2+\varepsilon(\mathrm{mod}\,L_2),2}\cdot W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}\,L_1),2}\cdot W_{\upsilon L_2+\varepsilon l(\mathrm{mod}\,L_2),2} = \sum_{\varepsilon=0}^{L_1-1} W_{\varepsilon(\mathrm{mod}\,L_1),1}\cdot \tag{10}$$

$$\times W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}\,L1),1}.$$

С учетом, того, что $r_j(l) = \sum_{i=1}^{L-m} W_i^j \left(W_{i+l}^j\right)^*$,

$$\sum_{\varepsilon=0}^{L_2-1} W_{\varepsilon(\mathrm{mod}\,L_2),2}\cdot W_{\varepsilon+l(\mathrm{mod}\,L_2),2} = R_{W_2}(l) \tag{11}$$

Кроме того, если υ принимает значение из множества вычетов по $\mathrm{mod}\,L_1$, то $\upsilon L_2 + \varepsilon$ пробегает значения по модулю L_1, поэтому

$$\sum_{\varepsilon=0}^{L_1-1} W_{\upsilon L_2+\varepsilon(\mathrm{mod}\,L_1),1}\cdot W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}\,L_1),1} = \sum_{q=0}^{L_1-1} W_{q(\mathrm{mod}\,L_1),1}\cdot W_{q+\varepsilon(\mathrm{mod}\,L_1),1} = R_{W_1}(l) \tag{12}$$

и ПФАК ПНС может быть рассчитана с использованием выражения

$$R_{W^n}(l) = R_{W_1}(l)\cdot R_{W_2}(l). \tag{13}$$

Но, так как $R_{W_1}(l)$ и $R_{W_2}(l)$ могут принимать соответственно значения L_1 и L_2 при $l = 0$, $R_{W_1}(l)$ и $R_{W_2}(l)$ при $l = \overline{1, L-1}$, то

$$R_{W^n}(l) = \begin{cases} L, & \text{при } l \equiv 0(\mathrm{mod}\,L); \\ L_2 R_{W_1}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_2),\ L \ne 0\ (\mathrm{mod}\,L_1); \\ L_1 R_{W_2}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_1),\ l \ne 0(\mathrm{mod}\,L_2); \\ R_{W_1}(l)\cdot R_{W_2}(l), & \text{при } l \ne 0(\mathrm{mod}\,L_1, \mathrm{mod}\,L_2). \end{cases} \tag{14}$$

Анализ (14) показывает, что минимальные боковые лепестки ПНС имеют место в случае, если L_2, $R_{w_1}(l)$, L_1, $R_{w_2}(l)$ принимают минимальные значения.

2. Пусть $K = 3$, а $L_1 \ne L_2 \ne L_3$. В этом случае по аналогии с (14) выражение (7) можно представить в виде

$$R_{W^n}(l) = R_{W_1}(l)\cdot R_{W_2}(l)\cdot R_{W_3}(l), \tag{15}$$

или

$$R_{W^n}(l) = \begin{cases} L, & \text{при } l \equiv 0(\mathrm{mod}\,L); \\ R_{W_1}(l)\cdot R_{W_2}(l)\cdot R_{W_3}(l), & \text{при } l \ne 0(\mathrm{mod}\,L_1, L_2, L_3); \\ L_1\cdot R_{W_2}(l)\cdot R_{W_3}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_1),\ l \ne 0(\mathrm{mod}\,L_2, L_3); \\ L_2\cdot R_{W_1}(l)\cdot R_{W_3}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_2),\ l \ne 0(\mathrm{mod}\,L_1, L_3); \\ L_3\cdot R_{W_1}(l)\cdot R_{W_2}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_3),\ l \ne 0(\mathrm{mod}\,L_1, L_2); \\ L_1\cdot R_{W_2}(l)\cdot L_3, & \text{при } l \equiv 0(\mathrm{mod}\,L_1, L_3),\ l \ne 0(\mathrm{mod}\,L_2); \\ L_1\cdot L_2\cdot R_{W_3}(l), & \text{при } l \equiv 0(\mathrm{mod}\,L_1, L_2),\ l \ne 0(\mathrm{mod}\,L_3); \\ R_{W_1}(l)\cdot L_2\cdot L_3, & \text{при } l \equiv 0(\mathrm{mod}\,L_2, L_3),\ l \ne 0(\mathrm{mod}\,L_1). \end{cases} \tag{16}$$

Анализ (16) показывает, что для минимизации $R_{W^n}(l)$ необходимо и достаточно, чтобы $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W3}(l)$ были минимальными, а L_1, L_2 и L_3 – минимальными и взаимно простыми. Минимальное значение R_{W_i}, $i=\overline{1,3}$, равное 0, достигается только при использовании в качестве W_1 последовательности [3] вида {1 1 1 -1}. В этом случае выражение (16) принимает вид

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\text{mod } L); & \text{а)}\\ L_1\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\text{mod } L_1),\ l\neq 0(\text{mod } L_2, L_3); & \text{б)}\\ L_1\cdot R_{W_3}(l)\cdot L_2, \quad \text{при } l\equiv 0(\text{mod } L_1, L_2),\ l\neq 0(\text{mod } L_3); & \text{в)}\\ L_1\cdot R_{W_2}(l)\cdot L_3, \quad \text{при } l\equiv 0(\text{mod } L_1, L_3),\ l\neq 0(\text{mod } L_2). & \text{г)} \end{cases} \qquad (17)$$

Исследование выражений (17) (а, б и г), показывает, что для их минимизации необходимо, чтобы как принимаемые значения ПФАК $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W_3}(l)$, так и значения их длительностей были минимальными. С учетом того, что $L_1=4$, максимальные значения ПФАК $R_W(l)$ дают слагаемые в) и г) (выражение (17). Если L_2 и L_3 – взаимно простые, то минимальные значения $R_{W_2}(l)$ и $R_{W_3}(l)$ могут быть соответственно равны $\{\pm 1\}$ и $\{-4, 0\}$ или $\{0, 4\}$, или $\{2, -2\}$, поэтому

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\text{mod } L); & \text{а)}\\ \pm 4, \quad \text{при } l\equiv 0(\text{mod } L_1),\ l\neq 0(\text{mod } L_2, L_3); & \text{б)}\\ \pm 4L_1L_2, \quad \text{при } l\equiv 0(\text{mod } L_1, L_2),\ l\neq 0(\text{mod } L_3); & \text{в)}\\ \pm L_1L_3, \quad \text{при } l\equiv 0(\text{mod } L_1, L_3),\ l\neq 0(\text{mod } L_2). & \text{г)} \end{cases} \qquad (18)$$

Если L_1 и L_2 – взаимнопростые, то выражение $\pm 4L_1L_2$ принимает значение либо $\pm 4L_1R_{W_2}(l)$, либо $\pm 4R_{W_1}(l)L_2$, поэтому максимальный боковой лепесток дает составляющая $\pm L_1L_3$.

Из приведенного следует, что для минимизации боковых лепестков необходимо, чтобы L_1, L_2 и L_3 были взаимнопростыми. Этого можно достичь, если L_1 и L_2 – простые, а $L_3\equiv 0(\text{mod } 2)$. При этих условиях составляющие (11) принимают значения

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\text{mod } L);\\ R_{W_1}(l)\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\neq 0(\text{mod } L_1, L_2, L_3);\\ L_1\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\text{mod } L_1),\ l\neq 0(\text{mod } L_2, L_3);\\ L_2\cdot R_{W_1}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\text{mod } L_2),\ l\neq 0(\text{mod } L_1, L_3);\\ L_3\cdot R_{W_1}(l)\cdot R_{W_2}(l), \quad \text{при } l\equiv 0(\text{mod } L_3),\ l\neq 0(\text{mod } L_1, L_3). \end{cases} \qquad (19)$$

3. Пусть $L_1=L_2=L_K=L$, а $K_1=K_2=K$. Для этих условий с учетом (2) выражение для ПФАК ПНС можно представить в виде

$$R_{W_n}(l)=\sum_{i=0}^{L-1}\prod_{j=1}^{K}W_{i,j}^{q}\prod_{j=1}^{K}W_{i+l,j}, \qquad (20)$$

причем (20) позволяет вычислить ПФАК, если положить, что $q=r$.

Проведенные исследования показали, что для рсчетов (20) можно получить оценки, если воспользоваться теорией двухзначных характеров, в частности, тем, что для любого нетривиального характера справедливо [5]

$$\sum_{y \in GF(P)} \Psi(ay+b) = \sum_{\substack{y \in GF(P^W) \\ y \neq 0 (\mathrm{mod}\, P)}} \Psi(ay+b) + \Psi(b) = 0,$$

и фиксированными правилами кодирования. Например, для наиболее мощного класса двухуровневых последовательностей – последовательностей характеристического типа с числом символов $L = 2x = P^n - 1$, $x = 1, 2, 3, \ldots, z, \ldots$

$$W^q = \left\{ W_i^q, \quad i = \overline{0, P^n - 1} \right\};$$

$$W_i^q = \begin{cases} \Psi(\Theta_q^i + 1), & \text{если } \Theta_q^i + 1 \neq 0 [\mathrm{mod}\, f(x), P]; \\ 1, & \text{если } \Theta_q^i + 1 \equiv 0 [\mathrm{mod}\, f(x), P]; \end{cases} \quad \text{а)}$$

либо

$$W_i^q = \begin{cases} \Psi(\Theta_q^i + 1), & \text{если } \Theta_q^i + 1 \neq 0 [\mathrm{mod}\, f_m(x), P]; \\ -1, & \text{если } \Theta_q^i + 1 \equiv 0 [\mathrm{mod}\, f_m(x), P]; \end{cases} \quad \text{б)} \qquad (21)$$

где Θ_q – q-й первообразный элемент поля $GF(P)$, а $f_m(x)$ – m-й первообразный примитивный полином степени n.

Приведем вывод аналитического выражения для ПФАК ПНС. Используя (19) и полагая, что $q \neq r$, имеем

$$R_{W_n}(l) = \sum_{i=0}^{L-1} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1). \qquad (22)$$

С учетом того, что $\Psi(0) = 0$, [ ], при $l \neq 0 (\mathrm{mod}\, L)$

$$R_{W_n}(l) = \sum_{i=0}^{P^n - 2} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1) \pm Z, \qquad (23)$$

где Z – учитывает сумму слагаемых, входящих в (23), для которых

$$\left(\Theta_q^i + 1\right) \equiv 0 \vee \left(\Theta_q^{i+l} + 1\right) \equiv \left(\Theta_r^i + 1\right) \equiv \left(\Theta_r^{i+l} + 1\right) \equiv 0 [\mathrm{mod}\, f_m(x), P] \qquad (24)$$

Более точно структуру (62) определяют сформулированные ниже утверждения.

Утверждение 1. Пусть $\Theta_\upsilon^i + 1$ и $\Theta_\upsilon^{i+l} + 1$ есть элементы поля $GF(P^n)$ а Θ_υ^υ – υ-й первообразный элемент, тогда при $l' \neq 0 (\mathrm{mod}\, L)$ $\Theta_\upsilon^i + 1$ и $\Theta_\upsilon^{i+l} + 1$ никогда не сравнимы с $0 [\mathrm{mod}\, f_m(x), P]$. Доказательство утверждения следует из цикличности поля $GF(P^n)$ [4].

Утверждение 2. Пусть $\Theta_\upsilon^r + 1$ и $\Theta_k^m + 1$ – элементы поля $GF(P^n)$, а Θ_υ и Θ_k – первообразные. Существуют T^{s1} и T^{s2} автоморфные преобразования, при которых

$$\Theta_\upsilon^r + 1 \equiv \Theta_k^m + 1 \equiv 0 (\mathrm{mod}\, L).$$

Доказательство утверждения следует из авто- и изоморфных свойств поля $GF(P^n)$ [5].

Выражение (24) распадается на следующие логические высказывания.

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^{i+l} \neq 0 (\mathrm{mod}\, L); \quad \text{а)}$$

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_r^i + 1 \equiv 0 \wedge \Theta_r^{i+l} + 1 \neq 0 (\mathrm{mod}\, L); \quad \text{б)}$$

$$\Theta_q^i + 1 \equiv 0 \wedge \Theta_q^{i+l} + 1 \neq 0 \wedge \Theta_r^i + 1 \neq 0 \wedge \Theta_r^{i+l} + 1 \equiv 0 (\mathrm{mod}\, L); \quad \text{в)} \qquad (25)$$

$$\Theta_q^i + 1 \neq 0 \wedge \Theta_q^{i+l} + 1 \equiv 0 \wedge \Theta_r^i + 1 \neq 0 \wedge \Theta_r^{i+l} + 1 \neq 0 (\mathrm{mod}\, L); \quad \text{г)}$$

$$\Theta_q^i+1\neq 0\wedge\Theta_q^{i+l}+1\equiv 0\wedge\Theta_r^i+1\equiv 0\wedge\Theta_r^{i+l}+1\neq 0(\mathrm{mod}\,L);\qquad \text{д)}$$

$$\Theta_q^i+1\neq 0\wedge\Theta_q^{i+l}+1\equiv 0\wedge\Theta_r^i+1\neq 0\wedge\Theta_r^{i+l}+1\equiv 0(\mathrm{mod}\,L);\qquad \text{е)}$$

$$\Theta_q^i+1\neq 0\wedge\Theta_q^{i+l}+1\neq 0\wedge\Theta_r^i+1\equiv 0\wedge\Theta_r^{i+l}+1\neq 0(\mathrm{mod}\,L);\qquad \text{ж}$$

$$\Theta_q^i+1\neq 0\wedge\Theta_q^{i+l}+1\neq 0\wedge\Theta_r^i+1\neq 0\wedge\Theta_r^{i+l}+1\equiv 0(\mathrm{mod}\,L).\qquad \text{з)}$$

Анализ (25) показывает, что исключающими являются высказывания а), г), ж), з), поэтому

$$\begin{gathered}Z=\Psi\left(-\Theta_q^{i+l}+1\right)\cdot\Psi\left(-\Theta_r^i+1\right)\cdot\Psi\left(-\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_q^{-l}+1\right)\cdot\Psi\left(\Theta_r^i+1\right),\\ \Psi=\left(\Theta_r^{i+l}+1\right)+\Psi\left(-\Theta_r^l+1\right)\cdot\Psi\left(\Theta_q^i+1\right)\Psi\left(\Theta_q^{i+l}+1\right)+\\ +\Psi\left(-\Theta_r^{-l}+1\right)\Psi\left(\Theta_q^i+1\right)\Psi\left(\Theta_q^{i+l}+1\right)\end{gathered}. \tag{26}$$

Действительно, если истинно выражение (63), а), то $\Psi\left(\Theta_q^i+1\right)=0$, так как $\Theta_q^i+1\equiv 0(\mathrm{mod}\,L)$ [5], поэтому

$$\Psi\left(\Theta_q^{i+l}+1\right)=\Psi\left[\Theta_q^l\left(\Theta_q^i+\Theta_q^{-l}\right)\right]=\Psi\left[\Theta_q^l\left(\Theta_q^{-l}-1\right)\right]=\Psi\left(\Theta_q^l\cdot\Theta_q^{-l}-\Theta_q^l\right)=\Psi\left(1-\Theta_q^l\right)=\Psi\left(-\Theta_q^l+1\right).$$

В случае, если $\Theta^{i+l}+1\equiv 0(\mathrm{mod}\,L)$, то

$$\Psi\left(\Theta_q^i+1\right)=-\Psi\left(\Theta_q^i\cdot\Theta_q^l\cdot\Theta_1^{-l}+1\right)=\Psi\left[\Theta_q^{-l}\left(\Theta_q^{i+l}+\Theta_q^{-l}\right)\right]=\Psi\left[\Theta_q^{-l}\left(\Theta_q^{-l}-1\right)\right]=\Psi\left(-\Theta_q^{-l}+1\right).$$

Преобразуем выражение (23), используя свойство характера Ψ [5], обозначив его переменной X:

$$\begin{gathered}X=\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^i+1\right)\cdot\Psi\left(\Theta_q^{i+l}+1\right)\cdot\Psi\left(\Theta_r^i+1\right)\cdot\Psi\left(\Theta_r^{i+l}+1\right)=\\ =\Psi\left(\Theta_q^i\right)\cdot\Psi\left(\Theta_r^i\right)\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^i+1\right)\cdot\Psi\left(\Theta_q^i+\Theta_q^{-l}\right)\cdot\Psi\left(\Theta_r^i+1\right)\cdot\Psi\left(\Theta_r^i+\Theta_r^{-l}\right)=\Psi\left(\Theta_q^l\right)\cdot\Psi\left(\Theta_r^l\right)\cdot Q\end{gathered} \tag{27}$$

Проанализируем выражение

$$Q=\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^i+1\right)\cdot\Psi\left(\Theta_q^i+\Theta_q^{-l}\right)\cdot\Psi\left(\Theta_r^i+1\right)\cdot\Psi\left(\Theta_r^i+\Theta_r^{-l}\right).$$

Учитывая, что если i принимает значения индексов суммирования, то степени первообразных элементов Θ_q и Θ_r принимают значения всех ненулевых элементов поля $GF(P^n)$. Обозначая ненулевые элементы поля через a_i и b_i соответственно для первообразных Θ_q и Θ_r, при $i=\overline{0,P^n-2}$, перейдем к сумме произведения характеров ненулевых элементов

$$Q=\sum_{a_i,b_i\in GF(P^n)}\Psi\left(a_i+1\right)\cdot\Psi\left(a_i+\Theta_q^{-l}\right)\cdot\Psi\left(b_i+1\right)\cdot\Psi\left(b_i+\Theta_r^{-l}\right). \tag{28}$$

Полагая в (28) $c_i=a_i+1$ и $d_i=b_i+1$, проанализируем все c_i и d_i, если a_i и b_i пробегают все значения ненулевых элементов поля $GF(P^n)$, то c_i и d_i так же пробегают все ненулевые элементы поля $GF(P^n)$ исключая 1, поэтому

$$Q=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 1(\mathrm{mod}\,P)}}\Psi\left(c_i\right)\cdot\Psi\left(c_i+\Theta_q^{-l}+1\right)\cdot\Psi\left(d_i\right)\cdot\Psi\left(d_i+\Theta_r^{-l}-1\right). \tag{29}$$

Если же

$$\begin{aligned} &c_i = 1, \quad \text{то } Q_1 = \Psi\left(\Theta_1^{-l}\right)\Psi\left(d_i\right)\Psi\left(d_i + \Theta_r^{-l} - 1\right); && \text{а)} \\ &d_i = 1, \quad \text{то } Q_2 = \Psi\left(c_i\right)\Psi\left(c_i + \Theta_q^{-l} - 1\right)\Psi\left(\Theta_r^{-l}\right); && \text{б)} \\ &c_i = 1, d_i = 1, \quad \text{то } Q_3 = \Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right); && \text{в)} \end{aligned} \tag{30}$$

Исключим в (28) условие $c_i, d_i \neq 1 (\mathrm{mod}\, P)$, для этого добавим в него и вычтем Q_1, Q_2 и Q_3. В результате получим

$$\begin{aligned} Q = &\sum \Psi\left(c_i\right)\Psi\left(c_i + \Theta_q^{-l} - 1\right)\Psi\left(d_i\right)\Psi\left(d_i + \Theta_r^{-l}\right) - \Psi\left(\Theta_q^{-l}\right)\Psi\left(d_i\right)\Psi\left(d_i + \Theta_r^{-l} - 1\right) - \\ &-\Psi\left(c_i\right)\Psi\left(c_i + \Theta_q^{-l} - 1\right)\Psi\left(\Theta_r^{-l}\right) - \Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right) = \\ = &\sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0 (\mathrm{mod}\, P)}} \Psi\left(c_i^{\,2}\right)\Psi\left(1 + \left(\Theta_q^{-l} - 1\right)c_i^{-1}\right)\Psi\left(d_i^{\,2}\right)\Psi\left[1 + \left(\Theta_r^{-l} - 1\right)d_i^{-1}\right] - Q_1 - Q_2 - Q_3. \end{aligned} \tag{31}$$

Принимая во внимание, что $\Theta_q^{-l} - 1$ и $\Theta_r^{-l} - 1 \in GF(P^n)$ являются постоянными, обозначив их как $q_1 = \Theta_q^{-p} - 1$ и $q_2 = \Theta_r^{-l} - 1$, $q_1, q_2 \neq 0 (\mathrm{mod}\, P)$, а также обозначив $x_i = c_i^{-1}$ и $y_i = d_i^{-1}$, которые пробегают так же все элементы поля $GF(P^n)$, получим

$$Q = \sum_{\substack{x_i, y_i \in GF(P^n) \\ x_i, y_i \neq 0 (\mathrm{mod}\, P)}} \Psi\left(1 + q_i x_i\right)\Psi\left(1 + q_2 y_2\right) - Q_1 - Q_2 - Q_3.$$

С учетом (26), (28), (30), выражение (23) может быть представлено как:

$$\begin{aligned} R_{W^n}(l) = &\Psi\left(\Theta_q^{l}\right)\Psi\left(\Theta_r^{l}\right)\{\sum_{\substack{x_i, y_i \in GF(P^n) \\ x_i, y_i \neq 0 (\mathrm{mod}\, P)}} \Psi\left(1 + q_i x_i\right)\Psi\left(1 + q_2 y_1\right) - [\Psi\left(\Theta_q^{-l}\right) \cdot \Psi\left(d_i\right)\Psi\left(d_i - \Theta_r^{-l} - 1\right) + \\ &+\Psi\left(c_i\right)\Psi\left(c_i + \Theta_q^{-l} - 1\right)\Psi\left(\Theta_r^{-l}\right) + \Psi\left(\Theta_q^{-l}\right)\Psi\left(\Theta_r^{-l}\right)]\} + \{\Psi\left(-\Theta_q^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_q^{-l} + 1\right)\Psi\left(\Theta_r^{i} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \Psi\left(-\Theta_r^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_r^{-l} + 1\right)\Psi\left(\Theta_r^{-l} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \Psi\left(-\Theta_r^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_r^{-l} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right)\}, \end{aligned} \tag{32}$$

где запись $\{y\}$ означает, что слагаемые в скобках необходимо брать со знаками $+(-)$ во всевозможных сочетаниях, то есть 2^k сочетаний, если k – число слагаемых.

Упростим (32) учитывая, что все слагаемые

$$\begin{aligned} &\Psi\left(\Theta_q^{l}\right), \Psi\left(\Theta_r^{l}\right)\Psi\left(\Theta_q^{-l}\right), \Psi\left(d_i\right), \Psi\left(d_i - \Theta_r^{-l} - 1\right), \ldots, \\ &\Psi\left(-\Theta_r^{-l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) \in \{1; -1\}. \end{aligned} \tag{33}$$

Из (32) непосредственно следует, что

$$\begin{aligned} Z = \pm\{&\Psi\left(-\Theta_q^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \Psi\left(-\Theta_q^{-l} + 1\right)\Psi\left(\Theta_r^{i} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_r^{l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) + \Psi\left(-\Theta_r^{-l} + 1\right)\Psi\left(\Theta_q^{i} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right)\} \end{aligned}$$

принимает значение на множестве чисел $Z' = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. Поэтому, используя (33), выражение (32) можно представить в виде

$$R_{W^n}(l)=\{\pm\sum_{\substack{x_i,y_i\in GF(P^n)\\ x_i,y_i\neq 0(\mathrm{mod}\,P)}}\Psi\left(1+q_1x_i\right)\Psi\left(1+q_2y_i\right)\pm[3]\}\pm[4], \tag{34}$$

где запись [3] и [4] означает, что вместо [3] при анализе необходимо использовать числа $(-3,-2,-1,0,1,2,3)$, а вместо [4] – числа $(-4,-3,-2,-1,0,1,2,3,4)$.

Рассмотрим вывод аналитического выражения для ПФВК ПНС. Используя выражение для расчета функции взаимной корреляции

$$R^{\upsilon}_{j,m}(l)=\sum_{i=1}^{L-k}W_i^{\upsilon}\left(W_{i+1}^{j}\right)^*+\sum_{i=L-k+1}^{L}W_i^{\upsilon}\left(W_{i-L+k}^{m}\right)^*,$$

получим $(j=m)$

$$R^{B}_{W^n}(l)=\sum_{i=0}^{L-1}\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_3}\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right). \tag{35}$$

Приведем вывод выражения для оценки выбросов ПФВК

$$R^{B}_{W^n}(l)=\sum_{i=0}^{L-1}\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_3}+1\right)\Psi\left(\Theta^{i-l}_{r_4}+1\right). \tag{36}$$

Далее, аналогично выражению (36)

$$R_{W_n}(l)=\sum_{i=0}^{P^n-1}\Psi(\Theta^i_{r_1}+1)\cdot\Psi(\Theta^i_{r_2}+1)\cdot\Psi(\Theta^{i+l}_{r_3}-1)\cdot\Psi\left(\Theta^{i+l}_{r_4}-1\right)\pm Z, \tag{37}$$

где Z представляет собой сумму слагаемых, входящих в (36), для которых $\Theta^i_{r_1}+1\equiv 0\vee\left(\Theta^i_{r_2}+1\right)\equiv 0\vee\left(\Theta^{i+l}_{r_3}+1\right)\equiv 0\vee\left(\Theta^{i+l}_{r_4}+1\right)\equiv 0$, что эквивалентно:

$$\Theta^i_{r_1}+1\equiv 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i+l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad \text{а)}$$

$$\Theta^i_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\equiv 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i+l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad \text{б)}$$

$$\Theta^i_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\equiv 0\wedge\Theta^{i+l}_{r_4}+1\neq 0(\mathrm{mod}\,L); \quad \text{в)}$$

$$\Theta^i_{r_1}+1\neq 0\vee\Theta^{i+l}_{q}+1\neq 0\wedge\Theta^{i+l}_{r_3}+1\neq 0\wedge\Theta^{i+l}_{r_4}+1\equiv 0(\mathrm{mod}\,L); \quad \text{г)}$$

поэтому:

$$\begin{aligned}Z=\pm\{&\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_3}+1\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right)+\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^{i+l}_{r_3}+1\right)\Psi\left(\Theta^{i+l}_{r4}+1\right)+\\&+\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta_{r_3i+l}+1\right)+\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\Psi\left(\Theta^{i+l}_{r_4}+1\right)\},\end{aligned} \tag{38}$$

может принимать значения на множестве $Z'=\{-4,-3,-2,-1,0,1,2,3,4\}$, следовательно (37) есть

$$R_{W_n}(l)=\sum_{i=0}^{P^n-1}\Psi(\Theta^i_{r_1}+1)\cdot\Psi(\Theta^i_{r_2}+1)\cdot\Psi(\Theta^{i+l}_{r_3}+1)\cdot\Psi\left(\Theta^{i+l}_{r_4}+1\right)\pm[4]=x\pm[4]. \tag{39}$$

Преобразуем выражение для x следующим образом:

$$\begin{aligned}x=&\Psi\left(\Theta^l_{r_3}\right)\Psi\left(\Theta^l_{r_4}\right)\sum_{i=0}^{P^n-1}\Psi(\Theta^i_{r_1}+1)\Psi(\Theta^i_{r_2}+1)\Psi(\Theta^i_{r_3}+\Theta^{-l}_{r_3})\Psi(\Theta^i_{r_4}+\Theta^{-l}_{r_4})=\\&=\Psi(\Theta^l_{r_3})\Psi(\Theta^l_{r_4})\cdot Q.\end{aligned} \tag{40}$$

Далее, выражение для Q (обозначив $\Theta^i_{r_1}+1=a_i$ и $\Theta^i_{r_2}+1=b_i$), представим в виде

$$Q=\sum_{\substack{a_i,b_i\in GF(P^n)\\ a_i,b_i\neq 1(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi\left(\Theta^i_{r_3}+\Theta^{-1}_{r_3}\right)\Psi\left(\Theta^i_{r_4}+\Theta^{-1}_{r_4}\right).$$

С учетом (29), (30), а также учитывая, что $\Theta^{-1}_{r_3}$ и $\Theta^{-1}_{r_4}$ могут принимать все значения из $GF(P^n)$, обозначив $c_i=\Theta^i_{r_s}+\Theta^{-1}_{r_s}$ и $d_i=\Theta^4_{r_4}+\Theta^{-1}_{r_4}$, причем, так как, во-первых, $\Theta^i_{r_3}\neq 0(\mathrm{mod}\,P)$ и $\Theta^{-1}_{r_3}\neq 1(\mathrm{mod}\,P)$, $\Theta^i_{r_3}+\Theta^{-1}_{r_3}\neq 1(\mathrm{mod}\,P)$, а во-вторых, при $\Theta^i_{r_4}\neq 0(\mathrm{mod}\,P)$ и $\Theta^{-1}_{r_4}\neq 1(\mathrm{mod}\,P)$, $\Theta^i_{r_4}+\Theta^{-1}_{r_4}\neq 1(\mathrm{mod}\,P)$, (40) можно представить в виде

$$\begin{aligned}R^B_{W^n}(l)&=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)=\\ &=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[4]\pm[15]=\\ &=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[19].\end{aligned}\qquad(41)$$

Анализ (41) показывает, что элементы полей c_i,d_i представляют собой автоморфизмы полей $\Theta^i_{r_3}$ и $\Theta^i_{r_4}$ при $i=\overline{0,P^{n-2}}$. Сумма в нем берется по всевозможным произведениям характеров над $a_i,b_i,c_i,d_i\in GF(P^n)$ и дает оценку для максимально достигаемого выброса $R^B_{W^n}(l)_{max}$. С учетом того, что элементы a_i, b_i, c_i и d_i строятся по различным первообразным и пары условий

$$\Psi(a_i)=\Psi(1)\wedge\Psi(b_i)=\Psi(1);$$
$$\Psi(c_i)=\Psi(1)\wedge\Psi(d_i)=\Psi(1)$$

не истинны, и (41) имеет вид

$$\begin{aligned}R_{W^n}(l)&=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[8]\pm[4]=\\ &=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[4]\pm[12].\end{aligned}\qquad(42)$$

Важной задачей является несбалансированность ПНС по числу символов $(+1)$ и (-1). Если $\Theta_1,\Theta_2,\ldots,\Theta_k$ – первообразные элементы поля $GF(P^n)$, то несбалансированность в числе символов есть

$$R_{W^n}(0)=\sum_{i=0}^{L-1}\prod_{j=1}^{k}\Psi\left(\Theta^i_j+1\right).$$

При $k=2$ аналогично (37)

$$R_{W^n}(0)=\sum_{i=0}^{P^n-2}\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)=\sum_{i=0}^{P^n-2}\Psi\left(\Theta^i_{r_1}+1\right)\Psi\left(\Theta^i_{r_2}+1\right)\pm Z,$$

где Z представляет собой сумму слагаемых, для которых

$$\Theta^{i}_{r_1}+1=0\vee\Theta^{i}_{r_2}+1\equiv 0(\mathrm{mod}\,P), \tag{43}$$

то есть

$$Z=\pm\Psi\left(\Theta^{i}_{r_1}+1\right)+\Psi\left(\Theta^{i}_{r_2}+1\right)\to\pm 2 \tag{44}$$

Далее обозначив $a_i=\Theta^{i}_{r_1}$ и $b_i=\Theta^{i}_{r_2}$, а затем $c_i=a_i+1$ и $d_i=b_i+1$ аналогично (26) – (30), имеем

$$\begin{aligned} x=&\sum_{\substack{a_i,b_i\in GF(P^n)\\ a_i,b_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i+1)\Psi(b_i+1)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 1(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)=\\ &\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)-\Psi(c_i)-\Psi(d_i)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)\pm[2]\end{aligned} \tag{45}$$

С учетом (45)

$$R^{B}_{W^n}(0)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)\pm[4]. \tag{46}$$

Заметим, что для случая $k=4$, $R_{W^n}(0)$ можно оценить, используя соотношения (42), то есть

$$R^{B}_{W^n}(0)=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[12]. \tag{47}$$

Анализ (47) показывает, что несбалансированность, а следовательно, и шумы неортогональности с увеличением k увеличиваются и уже при $k=4$ достигают значительной величины, даже без учета результатов сумм в (46) и (47).

Особенности вычисления выражений (34), (42) и оценки их значений рассмотрим с использованием выражения (47). Воспользовавшись свойством функции характеров, имеем

$$R^{B}_{W^n}(0)=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i,b_i,c_i,d_i)\pm 12. \tag{48}$$

Для случая двухзначного характера

$$R^{B}_{W^n}(0)=\sum_{u^{*}_i\in GF(P^n)}\exp\left(-j\pi u^{*}_i\right)\pm 12. \tag{49}$$

Исследование мощности изоморфного кодирования (объема системы сигналов или ансамбль сигналов), предпочтительно выполнять на основе изучения изоморфизмов разностных множеств. В [5] показано, что каждому коэффициенту разностных множеств может быть поставлен в соответствие первообразный элемент поля $GF(p^n)$.

В табл. 1 приведены значения объема системы сигналов M для некоторых значений периода последовательности L характеристических дискретных сигналов (ХДС).

Таблица 1

L_i	40	70	100	256	508	520	1020	1030	2052	2068	2080	2082	2098
M	8	12	20	64	126	96	125	204	515	460	384	346	524

Важной составляющей ансамблевых свойств системы сигналов является спектр значений периода сигналов, для которых могут быть синтезированы сигналы данной системы. В табл. 2 приведены значения числа ХДС, которые могут быть синтезированы в некотором интервале ς периодов сигналов.

Таблица 2

ς	2-100	100-200	200-300	300-400	400-500	500-600	600-700	700-800	800-900	900-1000	1000-1200
K	30	20	16	16	17	14	15	14	15	14	28

В табл. 3 приведены обобщенные данные о числе значений длин сигналов и объеме системы сигналов для m-последовательностей и ХДС.

Таблица 3

	Число значений L		Объем системы	
ΔL	ХДС	m-последовательностей	ХДС	m-последовательностей
$0-10^2$	30	4	456	8
$0-10^3$	186	9	29291	79
$0-10^4$	1269	11	2152943	554

Анализ приведенных в табл. 1 – 3 данных свидетельствует о том, что ХДС, с точки зрения ансамблевых свойств, являются более предпочтительными по сравнению с целым рядом широко используемых в различных приложениях ИКС линейных классов сигналов (m-последовательности, последовательности Лежандра и другие). Например, на интервале длин от 50 до 1500 m-последовательности существуют только для пяти значений периода, доступное число последовательностей Лежандра составляет 114, число характеристических сигналов для этого интервала длин составляет 225. Более того, мощность метода кодирования для ХДС определяется числом классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы $\mathbf{T} = \{t\}\ \{t, N\} = 1$ на смежные классы по классу автоморфных коэффициентов и равна $\Psi(N)/2n$. Так для ХДС с числом элементов $N = 2052$ существует 515 изоморфизмов данного кода, в то время как для m-последовательностей ($N = 2047$) только 88 изоморфизмов. Объем системы, составленной из ХДС в интервале длительностей до 10000 символов, более чем в 10^3 раз превышает объем системы, составленной из m-последовательностей. Система сигналов может быть расширена за счет привлечения автоморфизмов (циклических сдвигов) изоморфных сигналов. Указанное становится возможным в том случае, если все множество циклических сдвигов (или отдельные автоморфизмы) обладают необходимыми корреляционными свойствами. Мощность авто- и изоморфного кодирования $M_{аи}$ в классе характеристических дискретных сигналов при заданном периоде последовательности N может быть определена из соотношения

$$M_{аи} = N\varphi(N)/2n. \qquad (50)$$

В классе производных характеристических сигналов, построенных по правилу (2) при k = 2, мощность производного авто- и изоморфного кодирования

$$M_{паи} = (N+2)\varphi(N)(\varphi(N) - 2n)/\ 8n^2\ . \qquad (51)$$

В табл. 4 приведены значения $M_{паи}$ для некоторых значений L, вычисленных с использованием соотношения (51).

Таблица 4

L	66	100	130	256	508	1018	2098
$M_{паи}$	$3{,}1\ 10^3$	$1{,}9\cdot10^4$	$3{,}7\cdot10^4$	$5{,}2\cdot10^5$	$4{,}0\cdot10^6$	$3{,}3\cdot10^7$	$2{,}9\cdot10^8$
L	3000	4000	5002	6010	7012	8008	9010
$M_{паи}$	$2{,}4\cdot10^8$	$1{,}3\cdot10^8$	$3{,}6\cdot10^9$	$4{,}3\cdot10^9$	$1{,}1\cdot10^{10}$	$8{,}3\cdot10^9$	$1{,}2\cdot10^{10}$

Таким образом, аналитические соотношения (14), (19) а также и (41) – (48) позволяют получить минимаксные оценки корреляционных свойств класса производных характеристи-

ческих дискретных сигналов. Такой подход применим и для оценки корреляционных свойств и других классов дискретных плотно упакованных по ПФАК дискретных сигналов.

Выводы

Анализ выражения (49) показывает, что оценка максимальных боковых лепестков ПФАК, ПФВК и несбалансированности в числе символов (1) и (-1) может быть сведена к изучению несбалансированности по четности и нечетности индексов производного поля, элементами которого являются числа (полиномы) вида $x_i = a_i \cdot b_i \cdot c_i \cdot d_i\left[\mathrm{mod}\, f(x), P\right]$. Анализ выражения (48) показывает, что для анализа нелинейных сигналов (ПНС) по критерию минимума максимальных выбросов $R^{B}_{W}(l)\left(R^{B}_{W^n}(l)\right)$, с точки зрения вычислительной сложности, предпочтительнее использовать алгоритм (48), а при вычислении основных статистических характеристик – алгоритм (49). Характеристические дискретные сигналы, с точки зрения корреляционных свойства автокорреляционной функции, отвечают границе «плотной упаковки» (1). Указанное позволяет обеспечить высокие показатели помехоустойчивости приема сигналов в условиях воздействия структурных, имитационных, ретранслированных и некоторых других типов помех.

Использование в современных ИКС производных нелинейных характеристических дискретных сигналов позволит существенно улучшить ансамблевые свойства физических переносчиков данных, что, в свою очередь, повысит уровень крипто- и имитозащищенности информационного обмена.

Список литературы: 1. *Горбенко, І.Д., Горбенко, Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І Горбенко. – Харків : Форт, 2012. – 880 с. 2. *Горбенко, Ю.І.* Методи побудування та аналізу, стандартизація та застосування криптографічних систем / Ю.І. Горбенко. – Харків : Форт, 2016. – 959 с. 3. *Варакин, Л. Е.* Системы связи с шумоподобными сигналами / Л. Е Варакин. – М. : Радио и связь, 1985. – 384 с. 4. *Замула, А.А.* Перспективы применения нелинейных дискретних сигналов в современных телекоммуникационных системах и сетях / Замула А.А., Семенко Е.А // Системи обробки інформації. – Харків : ХУПС, 2015. – Вип. 5 (130).– С. 129–134. 5. *Свердлик, М.Б.* Оптимальные дискретные сигналы / М.Б.Свердлик. – М. : Сов.радио, 1975. – 200 с. 6. *Gorbenko, I.D., Zamula, A.A., Semenko, Ye.A.* Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. – Volume 75, 2016 Issue 2. P. 169 – 178. 7. *Ipatov, Valery P.* Spread Spectrum and CDMA. Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. – John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. – 2005. – 385 p. 8. *Sarvate, D.V.* Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun. – 1980. – Vol. Com 68 – P. 59–90. 9. *Gold, R.* Optimal binary sequences for spread spectrum multiplexing // IEEE Trans. Inform. Theory.– 1967. – Vol. 13. – P. 619–621. 9. *Замула, А.А.* Ансамбли дискретных сигналов с минимальными значениями боковых лепестков функций корреляции / Замула А.А. // Системи обробки інформації. – Харків : ХУПС, 2015. – Вип. 10 (135).– С. 35-39. 10. *Горбенко, И.Д., Замула, А.А., Морозов, В.Л., Семенко, Е.А.* Метод синтеза производных систем сигналов на основе криптографических дискретных последовательностей символов // Радиотехника. – 2017. – Вып. 186. – С. 107 – 116.

Харьковский национальный
университет имени В.Н. Каразина

Поступила в редколлегию 07.10.2017