УДК 621.396

ФОРМИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ МЕТОДОВ АЛГЕБРАИЧЕСКОГО КОДИРОВАНИЯ

А.А. Кузнецов, А.М. Носик, А.Н. Коваленко
Харьковский университет воздушных сил им. И. Кожедуба

Исследуются методы построения больших ансамблей слабо коррелированных между собой дискретных сигналов. Предлагается метод формирования псевдослучайных последовательностей с улучшенными авто – и взаимокорреляционными свойствами.

ПОСТАНОВКА ПРОБЛЕМЫ В ОБЩЕМ ВИДЕ И АНАЛИЗ ЛИТЕРАТУРЫ

Перспективным направлением обеспечения высокой помехозащищенности, имитостойкости и скрытности радиоканалов управления является использование широкополосных систем связи [1-4]. Их функционирование основано на использовании больших ансамблей слабо коррелированных между собой сигналов [5, 6].

В современных широкополосных системах связи сложные сигналы формируются, как правило, на основе псевдослучайных последовательностей [1 - 6]. Таким образом, актуальной задачей является формирование больших ансамблей псевдослучайных последовательностей с требуемыми корреляционными свойствами.

Целью статьи является разработка метода формирования псевдослучайных последовательностей с улучшенными авто – и взаимокорреляционными свойствами. Для построения ансамблей дискретных сигналов предлагается использовать методы алгебраического кодирования [6-9] и перестановочные преобразования, широко используемые в блочно-симметричных криптоалгоритмах [10-13].

ПРИМЕНЕНИЕ МЕТОДОВ АЛГЕБРАИЧЕСКОГО КОДИРОВАНИЯ ДЛЯ ПОСТРОЕНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В соответствии с общей постановкой задачи синтеза ансамбля дискретных сигналов с требуемыми авто - и взаимокорреляционными свойствами необходимо сформировать множество псевдослучайных последовательностей, функции корреляции которых удовлетворяют совокупности систем нелинейных неравенств вида [1-4]:

$$\begin{cases} R_0^{ii} = S_1^i S_1^{i*} + S_2^i S_2^{i*} + \cdots + S_n^i S_n^{i*} = 1 \\ R_{1\min}^{ii} \le S_1^i S_2^{i*} + S_2^i S_3^{i*} + \cdots + S_n^i S_1^{i*} \le R_{1\max}^{ii} \\ \cdots \\ R_{(n-1)\min}^{ii} \le S_1^i S_n^{i*} + S_2^i S_1^{i*} + \cdots + S_n^i S_{n-1}^{i*} \le R_{(n-1)\max}^{ii} \end{cases}, \qquad (1)$$

$$\begin{cases} R_0^{ij} \le S_1^i S_1^{j*} + S_2^i S_2^{j*} + \cdots + S_n^i S_n^{j*} \le R_{0\max}^{ij} \\ R_{1\min}^{ij} \le S_1^i S_2^{j*} + S_2^i S_3^{j*} + \cdots + S_n^i S_1^{j*} \le R_{1\max}^{ij} \\ \cdots \\ R_{(n-1)\min}^{ij} \le S_1^i S_n^{j*} + S_2^i S_1^{j*} + \cdots + S_n^i S_{n-1}^{j*} \le R_{(n-1)\max}^{ij} \end{cases}, \qquad (2)$$

где системы (1) и (2) определяют компоненты функций авто - и взаимокорреляции;

$R^{ii}_{k\min}$ и $R^{ii}_{k\max}$ - минимально и максимально допустимый уровень боковых лепестков функции автокорреляции i-го сигнала при сдвижке на k- элементов;

$R^{ij}_{k\min}$ и $R^{ij}_{k\max}$ - минимально и максимально допустимый уровень боковых лепестков функции взаимной корреляции i-го и j-го сигналов при сдвижке j-го сигнала относительно i-го на k-элементов, полученных в результате решения системы неравенств (1).

Нормированная *функция корреляции* для двоичных дискретных последовательностей описывается выражением

$$R^{ij}_l(\tau = lT_e) = \frac{1}{n}\left(S^i_0 S^j_l + S^i_1 S^j_{l+1} + \cdots + S^i_{n-1} S^j_{l+n-1}\right) = \frac{1}{n}\sum_{\xi=0}^{n-1} S^i_\xi S^j_{l+\xi}\ , \qquad (3)$$

где T_e – длительность элемента последовательности; l – число тактов, на которые две последовательности сдвинуты одна относительно другой; τ – временной сдвиг между двумя последовательностями; n – число элементов в последовательности; S^i_ξ – ξ-й элемент i-й последовательности; $S^j_{l+\xi}$ – ξ-й элемент j-й последовательности, сдвинутой на l тактов.

Функция автокорреляции (ФАК) дискретной последовательности количественно характеризует меру подобия последовательности ей самой, только сдвинутой во времени.

Различают две функции автокорреляции: апериодическую функцию автокорреляции (АФАК) и периодическую функцию автокорреляции (ПФАК).

АФАК характеризует отклик оборудования на ожидаемый сигнал и описывается выражением

$$R^{ii}_l(\tau = lT_e) = \frac{1}{n}\left(S^i_0 S^i_l + S^i_1 S^i_{l+1} + \cdots + S^i_{n-1} S^i_{l+n-1}\right) = \frac{1}{n}\sum_{\xi=0}^{n-1} S^i_\xi S^i_{l+\xi}\ . \qquad (4)$$

Эта функция имеет максимальное значение при $\tau = 0$:

$$R^{ii}_l(\tau = 0) = \frac{1}{n}\left(S^i_0 S^i_0 + S^i_1 S^i_1 + \cdots + S^i_{n-1} S^i_{n-1}\right) = \frac{1}{n}\sum_{\xi=0}^{n-1}\left(S^i_\xi\right)^2 = 1\ . \qquad (5)$$

ПФАК характеризует отклик оборудования на периодическую последовательность ожидаемых сигналов и может быть определена по выражению

$$R^{ii}_l(\tau = lT_e) = \frac{1}{n}\left(S^i_0 S^i_l + S^i_1 S^i_{l+1} + \cdots + S^i_{n-1} S^i_{(l+n-1)\bmod n}\right) = \frac{1}{n}\sum_{\xi=0}^{n-1} S^i_\xi S^i_{(l+\xi)\bmod n}\ . \qquad (6)$$

Для характеристики свойств последовательностей используют такие виды функций взаимной корреляции (ФВК):

– апериодическую (АФВК), которая характеризует отклик оборудования на сигнал, отличный от ожидаемого, и описывается выражением (3);

– периодическую (ПФВК), которая характеризует отклик оборудования на периодическую последовательность сигналов, отличных от ожидаемого, и описывается выражением

$$R_l^{ij}(\tau = lT_e) = \frac{1}{n}\left(S_0^i S_l^j + S_1^i S_{l+1}^j + \cdots + S_{n-1}^i S_{(l+n-1) \bmod n}^j\right) = \frac{1}{n}\sum_{\xi=0}^{n-1} S_\xi^i S_{(l+\xi) \bmod n}^j \text{ ; (7)}$$

– стыковую (СФВК), которая характеризует отклик оборудования на чередующуюся последовательность сигналов, равных и отличных ожидаемому. В общем виде она задается выражением

$$R_l^{ij}(\tau = lT_e) = \frac{1}{n}\left(S_0^i \Sigma_l^j + S_1^i \Sigma_{l+1}^j + \cdots + S_{n-1}^i \Sigma_{l+n-1}^j\right) = \frac{1}{n}\sum_{\xi=0}^{n-1} S_\xi^i \Sigma_{l+\xi}^j \text{ , } \quad (8)$$

где $l = 0,1,\ldots,2n-1$, а последовательность

$$\Sigma^j = \left\{\Sigma_0^j, \Sigma_!^j, \ldots, \Sigma_{3n-1}^j\right\}$$

составлена из чередующейся последовательности сигналов

$$S^j = \left\{S_0^j, S_!^j, \ldots, S_{n-1}^j\right\}$$

и

$$S^i = \left\{S_0^i, S_!^i, \ldots, S_{n-1}^i\right\},$$

т.е.

$$\Sigma^j = \left(\left\{S_0^j, S_!^j, \ldots, S_{n-1}^j\right\}\left\{S_0^i, S_!^i, \ldots, S_{n-1}^i\right\}\left\{S_0^j, S_!^j, \ldots, S_{n-1}^j\right\}\right).$$

Предложенный в [9] подход к построению псевдослучайных последовательностей на основе методов кодирования позволяет математически обобщить решение задачи синтеза и в общей постановке решить системы (1) и (2).

Рассмотрим линейный блоковый код с весовым спектром, формально записанным в таблице 1 (первая строка таблицы заполнена возможными значениями весов $w(C^i)$ кодовых слов C^i, значения второй строки соответствуют числу кодовых слов # соответствующего веса $w(C^i)$).

Таблица 1 – Весовой спектр несовершенного кода

$w(C^i)$	0	1	...	d - 1	d	d + 1	...	d*	d* + 1	...	n
Число кодовых слов	1	0	...	0	# d	#d + 1	...	# d*	0	...	0

Если весовой спектр кода ограничен сверху некоторым значением d^*, т.е. для всех $w(C^i) > d^*$ весовой спектр равен нулю (см. таблицу 1). В этом случае периодические авто – и взаимокорреляционные свойства синтезируемых последовательностей (соответствующих кодовым словам линейного блокового кода) удовлетворяют системам ограничений (1) и (2), а минимально и максимально допустимые уровни боковых лепестков функции автокорреляции задаются следующей теоремой.

Теорема 1 [9]

$$R_{k\min}^{ii} \geq \frac{n - 2 \cdot d^*}{n}; \; R_{k\min}^{ij} \geq \frac{n - 2 \cdot d^*}{n}; \quad (9)$$

$$\begin{cases} R^{ii}_{k\max} = 1, \ \textit{если} \ \ \tau = 0 \bmod (\mathrm{n}) \\ R^{ii}_{k\max} \le \dfrac{n - 2 \cdot d}{n}, \ \text{если} \ \ \tau \ne 0 \bmod (\mathrm{n}) \end{cases}; \begin{cases} R^{ij}_{k\max} = 1, \ \text{если} \ \ C^i = \mathrm{C}^{\mathrm{j}}_{\to\tau} \\ R^{ij}_{k\max} \le \dfrac{n - 2 \cdot d}{n}, \ \text{если} \ \ C^i \ne \mathrm{C}^{\mathrm{j}}_{\to\tau} \end{cases}. \quad (10)$$

Таким образом, сигналы, сформированные в соответствии с разработанным в [9] способом, обладают улучшенными автокорреляционными свойствами. Взаимокорреляционные свойства сформированных сигналов имеют теоретически обоснованные выбросы. Остальные значения боковых выбросов лежат в узких пределах, являющихся одними из лучших на сегодняшний день результатов [9].

Для устранения основного недостатка рассмотренного в [9] подхода, а именно – наличия одного максимального выброса боковых лепестков функции взаимной корреляции, предлагается использовать перестановочные преобразования, получившие широкое развитие в теории защиты информации [10-13].

ИССЛЕДОВАНИЕ СВОЙСТВ ПЕРЕСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ

Классическая теория секретных систем оперирует симметричными (блочными и поточными) криптоалгоритмами [10-13]. В основе их построения лежат подходы, сформулированные в работе известного американского ученого Клода Шеннона [10]. Они состоят в построении криптосистемы путем комбинирования простых и хорошо изученных криптографических преобразований (криптопримитивов). В статье другого американского ученого Хорста Файстеля [11], разработчика блочно-симметричного алгоритма шифрования Lucifer – прототипа национального американского стандарта шифрования DES [12], показано, что для построения эффективной составной криптографической системы достаточно использовать «бутерброд» из блоков перестановок (P - блоков) и блоков замен (S - блоков). Этот принцип используется в традиционных схемах [11, 12] и при разработке большинства современных симметричных криптоалгоритмов [13, 14].

В качестве основного примитива, выполняющего перестановочное преобразование входного вектора, для эффективного перемешивания обрабатываемых данных используется блок перестановок (P – блок).

Суть перестановочного преобразования состоит в изменении нумерации входных символов, т.е. выходной вектор – суть перенумерованный входной. Предположим, что

$$a = \{a_1, a_2, \ldots, a_{\mathrm{n}}\} -$$

входной вектор, а

$$a^* = \{a^*_1, a^*_2, \ldots, a^*_{\mathrm{n}}\} -$$

входной вектор, $\forall a_i$, $a^*_i \in GF(q)$.

Тогда перестановочное преобразование можно представить в виде:

$$a^* = a \cdot P, \quad (11)$$

где P – перестановочная матрица, т.е. квадратная матрица размером $n \times n$ ячеек, в каждой строке и в каждом столбце которой находится только по одной единице. На практике перестановочное преобразование проще задавать вектором перестановок

$$p = \{ p_1, p_2, \ldots, p_n\},$$

координаты компонент которого соответствуют индексам входного вектора, а собственные значения компонент – индексам выходного

вектора. Для удобства матрицей P (или соответственно вектором p) будем обозначать в дальнейшем некоторое фиксированное перестановочное преобразование.

Очевидно, что перестановочное преобразование сохраняет вес Хемминга $w_h(a)$, т.е. справедлива

Лемма 1.

$$w_h(a^*) = w_h(a)\,. \tag{12}$$

Сохранение веса Хемминга наблюдается также для разницы двух произвольных векторов равной длины, т.е. в результате перестановочного преобразования над двумя векторами сохраняется расстояние по Хеммингу между ними. Действительно, зафиксируем два вектора a и b равной длины:

$$a = \{a_1, a_2, \ldots, a_n\}\,,\ b = \{b_1, b_2, \ldots, b_n\}\,,\ \forall a_i,\ b_i \in GF(q)$$

и соответствующие им векторы a^* и b^* после выполнения перестановочного преобразования:

$$a^* = \{a^*_1, a^*_2, \ldots, a^*_n\}\,,\ b^* = \{b^*_1, b^*_2, \ldots, b^*_n\}\,,\ \forall a^*_i,\ b^*_i \in GF(q).$$

Пусть $w_h(x, y)$ – расстояние по Хеммингу между векторами x и y, тогда справедлива

Лемма 2.

$$w_h(a, b) = w_h(a^*, b^*)\,. \tag{13}$$

Доказательство. По определению

$$w_h(a, b) = w_h(a - b)\,,\ w_h(a^*, b^*) = w_h(a^* - b^*)\,.$$

Из выражения (11) следует, что перестановочное преобразование – суть линейная операция. Следовательно, справедливо равенство

$$a^* - b^* = a \cdot P - b \cdot P = (a - b) \cdot P = (a - b)^*\,.$$

Но как следует из леммы 1,

$$w_h(a - b)^* = w_h(a - b)\,,$$

откуда имеем цепочку равенств:

$$w_h(a, b) = w_h(a - b) = w_h(a - b)^* = w_h(a^* - b^*) = w_h(a^*, b^*)\,,$$

что и завершает доказательство.

Зафиксируем перестановочное преобразование P. Применим полученные результаты к произвольному линейному блоковому (n, k, d) коду над $GF(q)$. Справедлива следующая теорема.

***Теорема* 2** Перестановочное преобразование P над всеми кодовыми словами линейного блокового (n, k, d) кода над $GF(q)$ образует новый линейный блоковый код с теми же параметрами и весовым спектром.

Доказательство. По определению каждый линейный блоковый (n, k, d) код над $GF(q)$ является подпространством $GF^k(q)$ пространства $GF^n(q)$, т.е.

$$GF^k(q) \subseteq GF^n(q).$$

В результате перестановочного преобразованиями над всеми кодовыми словами линейного блокового кода вес полученных последовательностей в

соответствии с леммой 1 не изменится. В соответствии с леммой 2 сохраниться также расстояние по Хеммингу между двумя произвольными кодовыми словами.

Таким образом, перестановочное преобразование над всеми кодовыми словами (n, k, d) кода переведет последовательности из $GF^k(q)$ в необязательно другие последовательности из $GF^n(q)$. При этом q^k последовательностей из $GF^n(q)$, полученных в результате перестановочного преобразования, в силу линейности перестановочного преобразования образуют линейное подпространство $GF^k(q)$ пространства $GF^n(q)$ – новый линейный блоковый (n, k, d) код с параметрами, равными исходному коду, а при условии сохранения расстояния по Хеммингу между произвольными кодовыми словами (лемма 2) – с тем же весовым спектром.

Таким образом, в результате проведенных исследований выявлены следующие основные свойства перестановочного преобразования:

- линейность – следует из выражения (9);
- сохранение веса Хемминга произвольного вектора – следует из леммы 1;
- сохранение расстояния по Хеммингу между двумя произвольными векторами – следует из леммы 2;
- сохранение дистанционных свойств линейного блокового кода – следует из теоремы 2.

К указанным свойствам следует отнести еще одно. Как можно убедиться на примере, перестановочное преобразование не обязательно сохраняет свойство цикличности кодовых слов. Практически это означает, что после выполнения перестановочного преобразования над всеми кодовыми словами циклический (n, k, d) код преобразуется в необязательно циклический (n, k, d) код с тем же весовым спектром.

Таким образом, в результате проведенных исследований установлено, что перестановочные преобразования, широко используемые в теории защиты информации, позволяют по исходному циклическому коду с фиксированным весовым спектром строить множество других линейных не обязательно циклических блоковых кодов с тем же весовым спектром. Как будет показано ниже, при случайно и независимо сформированной перестановке вероятность сохранения свойства цикличности может быть малой величиной, абсолютное значение которой определяется конструктивными кодовыми параметрами линейного блокового (n, k, d) кода. Исключение свойства цикличности или значительное снижение вероятности его сохранения позволяет, в свою очередь, избавиться или существенно снизить вероятность возникновения боковых выбросов в функции взаимной корреляции дискретных сигналов, формируемых с использованием линейных блоковых кодов. Ниже предлагается метод формирования псевдослучайных последовательностей с улучшенными взаимокорреляционными свойствами.

МЕТОД ФОРМИРОВАНИЯ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С УЛУЧШЕННЫМИ СВОЙСТВАМИ

Для построения ансамблей дискретных сигналов воспользуемся методами алгебраической теории блоковых кодов и рассмотренными выше свойствами перестановочных преобразований. Предлагаемый метод формирования псевдослучайных последовательностей структурно состоит из трех этапов.

1-й этап. В соответствии с требуемыми ансамблевыми и структурными свойствами формируемых псевдослучайных последовательностей выполняются расчет параметров и выбор методов построения линейного блокового кода.

2-й этап. С использованием методов линейной алгебры и процедур построения линейных блоковых кодов формируются кодовые слова выбранного кода.

3-й этап. Выполняется перестановочное преобразование над сформированными кодовыми словами линейного блокового кода. Для этого с использованием методов теории вероятности равновероятно и независимо формируется требуемая перестановка, например, в виде перестановочной матрицы или перестановочного вектора. Сформированная перестановка для повышения скрытности может использоваться как секретная ключевая информация.

В результате выполнения последнего этапа формируется ансамбль псевдослучайных последовательностей.

Пусть задан циклический *(n, k, d)* код над *GF(q)*. Весовой спектр кода в общем случае может быть представлен в виде набора множеств кодовых слов с фиксированным весом

$$\{V_0, V_1, \ldots, V_{d-1}, V_d, V_{d+1}, \ldots, V_n\}, \qquad (14)$$

где V_i – множество кодовых слов веса *i*.

Из определения *(n, k, d)* кода следует, что $|V_0| = 1$, а $V_1, \ldots, V_{d-1}$ – суть пустые множества.

Рассмотрим множества $V_d, V_{d+1}, \ldots, V_n$. Пусть мощность множества V_i для всех $i = d, d+1, \ldots n$ равно $|V_i| = v_i$. Каждое множество V_i содержит все циклические сдвиги всех кодовых слов *(n, k, d)* кода веса *i*. Таким образом, в произвольном циклическом *(n, k, d)* коде содержатся $\geq \frac{v_i}{n}$ ненулевых кодовых слов веса *i* и все их циклические сдвиги (по $\leq n$ сдвигов для каждого слова).

Рассмотрим теперь полное множество W_i последовательностей из $GF(q)^n$ веса *i*. Всего таких последовательностей

$$N_i = C_n^i = \frac{n!}{i! \cdot (n-i)!}.$$

Разобьем множество W_i на $\geq \frac{N_i}{n}$ подмножеств $W_{i,j}$, каждое из которых содержит все циклические сдвиги одной последовательности из $GF(q)^n$ веса *i* (неравенство означает возможность существования симметричной последовательности, для которой соответствующее подмножество W_i будет содержать $\leq n$ сдвигов):

$$W_i = W_{i,1} \cup W_{i,2} \cup \ldots \cup W_{i,\frac{N_i}{n}}, \quad |W_{i,j}| = n, \quad j = 1, 2, \ldots, \frac{N_i}{n}. \qquad (15)$$

Анализ выражений (14) и (15) показывает, что множество V_i кодовых слов циклического кода является или пустым множеством, или объединением конечного числа множеств $W_{i,j}$.

Перестановочное преобразование над всеми кодовыми словами согласно теореме 1 сохраняет дистанционные свойства кода. Другими словами, в результате выполнения перестановочного преобразования при равновероятно и независимо сформированной перестановке *P* кодовые слова из множества V_i преобразуются в последовательности веса *i*,

принадлежащие одному из множеств $W_{i,j}$. Схематично представим процесс перестановочного преобразования над всеми кодовыми словами циклического кода на рис. 1.

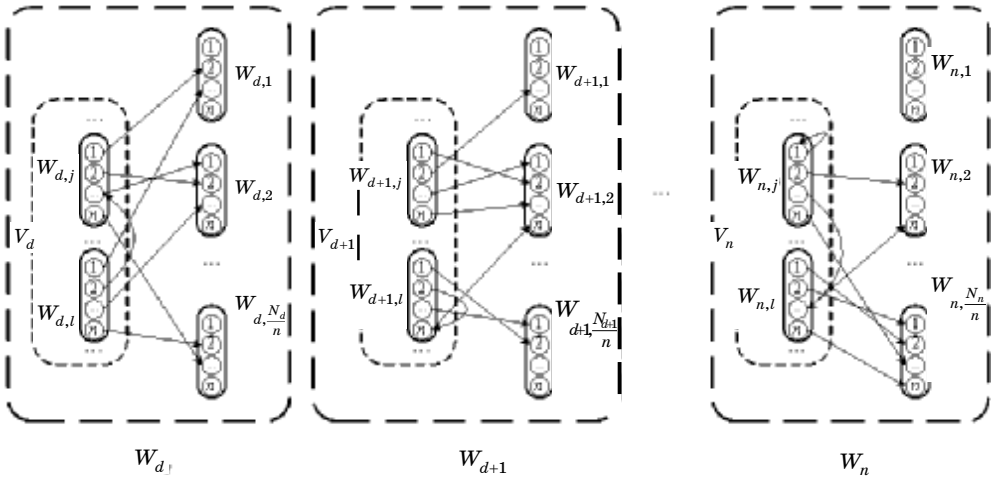

Рисунок 1 – Схема процесса перестановочного преобразования над кодовыми словами циклического кода

Проанализируем влияние процесса перестановочного преобразования на корреляционные свойства формируемых дискретных последовательностей.

Максимальный боковой выброс функции взаимной корреляции дискретных сигналов соответствует случаю принадлежности ансамблю, помимо исходной дискретной последовательности, ее циклической сдвижки. Это полностью соответствует случаю использования в качестве сигнальных последовательностей кодовых слов циклического кода.

В результате выполнения перестановочного преобразования (см. рис. 2.) кодовые слова циклического кода преобразуются в последовательности такого же веса. Сохранение свойства цикличности в результате такого преобразования соответствует попаданию двух и более преобразованных последовательностей в одно подмножество $W_{i,j}$, не обязательно отличное от исходного подмножества кодовых слов циклического кода. Так, например, для случая, приведенного на рис. 2, в результате перестановочного преобразования два кодовых слова преобразованы в последовательности, принадлежащие $W_{d,1}$. Это означает о сохранении цикличности для этой пары последовательности. В множество $W_{d,2}$ переведены три последовательности, откуда следует сохранение между ними свойства цикличности, но при этом свойство цикличности с первыми двумя последовательностями потеряно.

Таким образом, в результате проведенных исследований установлено, что максимальный выброс бокового лепестка функции взаимной корреляции для формируемых в соответствии с предложенным методом дискретных сигналов будет наблюдаться в случае сохранения свойства цикличности преобразуемых последовательностей. Сохранение цикличности последовательностей – суть случайная величина, ее вероятность зависит от мощности множества слов фиксированного веса в $GF(q)^n$ и от весового спектра используемого кода. Проведем статистические исследования свойств дискретных последовательностей, формируемых в соответствии с предложенным методом.

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

При проведении статистических исследований для оценки свойств формируемых дискретных последовательностей воспользуемся методикой, подробно рассмотренной в [1-4]. В ходе статистических исследований для каждой пары последовательностей оценивались следующие параметры ПФВК:

– максимальный выброс бокового лепестка R_{max};

– среднее значение уровня боковых лепестков:

$$m_r = \frac{1}{n}\sum_{i=1}^{n} r_i \quad , \tag{14}$$

где r_i – уровень i-го бокового лепестка ПФВК;

– среднее значение уровня модуля боковых лепестков

$$m_{|r|} = \frac{1}{n}\sum_{i=1}^{n} |r_i| \, ; \tag{15}$$

– дисперсия уровня боковых лепестков

$$d_r = \frac{1}{n-1}\sum_{i=1}^{n} (r_i - m_r)^2 \, ; \tag{16}$$

– дисперсия уровня модуля боковых лепестков

$$d_{|r|} = \frac{1}{n-1}\sum_{i=1}^{n} \left(|r_i| - m_{|r|}\right)^2 \, . \tag{17}$$

Основным параметром, характеризирующим свойства полученных последовательностей, является значение максимального выброса бокового лепестка R_{max} ПФВК. При этом при проведении статистических исследований данный показатель характеризируется его математическим ожиданием $U_{\max}$ и средним квадратическим отклонением (СКО) $\sqrt{D_{U_{\max}}}$.

Далее, исходя из вышесказанного и согласно методике, приведенной в [1-4], производились статистические оценки следующих параметров ПФВК:

$M_{|r|}$ – математическое ожидание модулей уровня боковых лепестков;

M_r – математическое ожидание уровня боковых лепестков;

$\sqrt{D_{m_{|r|}}}$ – СКО модуля среднего значения уровня боковых лепестков;

$\sqrt{D_{m_r}}$ – СКО среднего значения уровня боковых лепестков;

D_r – дисперсия уровня боковых лепестков;

$D_{|r|}$ – дисперсия модуля уровня боковых лепестков;

$\sqrt{D_{d_r}}$ – СКО дисперсии уровня боковых лепестков;

$\sqrt{D_{d_{|r|}}}$ – СКО дисперсии модуля уровня боковых лепестков;

$U_{\max}$ – математическое ожидание максимального выброса боковых лепестков;

$\sqrt{D_{U_{\max}}}$ – СКО максимальных выбросов боковых лепестков.

Естественной оценкой для математического ожидания m случайной величины X является среднее арифметическое ее наблюдаемых значений (или статистическое среднее) [6]:

$$\tilde{m} = \frac{1}{N}\sum_{i=1}^{N} X_i \quad , \tag{18}$$

где N – количество реализаций.

Оценка дисперсии определяется выражением:

$$\tilde{D} = \frac{1}{N-1}\sum_{i=1}^{N}(X_i - \tilde{m})^2 \ . \tag{19}$$

В силу центральной предельной теоремы теории вероятностей: при больших значениях количества реализаций N среднее арифметическое будет иметь распределение, близкое к нормальному [15], с математическим ожиданием

$$M\left[\tilde{m}\right] \approx \tilde{m} \tag{20}$$

и средним квадратическим отклонением:

$$\sigma\left[\tilde{m}\right] \approx \frac{\sigma}{\sqrt{N}}, \tag{21}$$

где σ – среднее квадратическое отклонение оцениваемого параметра.

При этом вероятность того, что оценка $\tilde{m}$ отклоняется от своего математического ожидания меньше, чем на ε (доверительная вероятность), равна [16]:

$$P(\left|\tilde{m} - m\right| < \varepsilon) \approx 2\Phi\left(\frac{\varepsilon}{\sigma\left[\tilde{m}\right]}\right), \tag{22}$$

где – $\Phi(x)$ функция Лапласа, определяемая выражением

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_0^x e^{-\frac{t^2}{2}} dt \ . \tag{23}$$

Полученные в результате проведения статистических исследований характеристики ПФВК представлены в таблице 2.

Статистические характеристики ПФВК, представленные в таблице 2, были получены при количестве реализаций N=10^5. Результаты расчетов

доверительной вероятности полученных оценок с использованием выражения (22) представлены в таблице 3. При этом определение значения функции Лапласа (23) производилось согласно [17].

Таблица 2 – Статистические характеристики ПФВК полученных последовательностей

Параметры ПФВК	Число элементов в сигнале					
	31	63	127	255	511	1023
$M_{\lvert r\rvert}$	0,147	0,102	0,071	0,05	0,035	0,025
M_r	$1{,}1\cdot10^{-3}$	$0{,}26\cdot10^{-3}$	$6{,}24\cdot10^{-5}$	$1{,}54\cdot10^{-5}$	$3{,}74\cdot10^{-6}$	$9{,}85\cdot10^{-7}$
$\sqrt{D_{m_{\lvert r\rvert}}}$	$0{,}2\cdot10^{-1}$	$0{,}96\cdot10^{-2}$	$0{,}48\cdot10^{-2}$	$0{,}24\cdot10^{-2}$	$0{,}12\cdot10^{-2}$	$0{,}59\cdot10^{-3}$
$\sqrt{D_{m_r}}$	$0{,}28\cdot10^{-2}$	$0{,}1\cdot10^{-2}$	$0{,}35\cdot10^{-3}$	$0{,}12\cdot10^{-3}$	$4{,}32\cdot10^{-5}$	$1{,}53\cdot10^{-5}$
D_r	$0{,}34\cdot10^{-1}$	$0{,}16\cdot10^{-1}$	$0{,}8\cdot10^{-2}$	$0{,}39\cdot10^{-2}$	$0{,}2\cdot10^{-2}$	$0{,}98\cdot10^{-3}$
$D_{\lvert r\rvert}$	$0{,}12\cdot10^{-1}$	$0{,}57\cdot10^{-2}$	$0{,}29\cdot10^{-2}$	$0{,}14\cdot10^{-2}$	$0{,}71\cdot10^{-3}$	$0{,}36\cdot10^{-3}$
$\sqrt{D_{d_r}}$	$0{,}85\cdot10^{-2}$	$0{,}29\cdot10^{-2}$	$0{,}1\cdot10^{-2}$	$0{,}35\cdot10^{-3}$	$0{,}12\cdot10^{-3}$	$0{,}1\cdot10^{-3}$
$\sqrt{D_{d_{\lvert r\rvert}}}$	$0{,}34\cdot10^{-2}$	$0{,}12\cdot10^{-2}$	$0{,}43\cdot10^{-3}$	$0{,}15\cdot10^{-3}$	$5{,}31\cdot10^{-5}$	$4{,}34\cdot10^{-5}$
$U_{\max}$	0,37 $2{,}08/\sqrt{\mathrm{L}}$	0,296 $2{,}347/\sqrt{\mathrm{L}}$	0,23 $2{,}6/\sqrt{\mathrm{L}}$	0,18 $2{,}82/\sqrt{\mathrm{L}}$	0,135 $3{,}04/\sqrt{\mathrm{L}}$	0,102 $3{,}25/\sqrt{\mathrm{L}}$
$\sqrt{D_{U_{\max}}}$	$0{,}88\cdot10^{-1}$	$0{,}57\cdot10^{-1}$	$0{,}37\cdot10^{-1}$	$0{,}24\cdot10^{-1}$	$0{,}16\cdot10^{-1}$	$0{,}11\cdot10^{-1}$

Таблица 3 – Доверительная вероятность полученных оценок

Число элементов в сигнале	Точность ε	
	10^{-3}	$5\cdot10^{-4}$
31	0,999674	0,927625
63	0,999999	0,994462
127	1	0,999981
255	1	0,999999
511	1	1
1023	1	1

Анализ полученных результатов, приведенных в таблице 2, показывает, что формируемые последовательности обладают высокими конструктивными свойствами, статистические характеристики ПФВК свидетельствуют о слабой коррелированности формируемых сигналов.

На рисунке 2 представлены гистограммы распределения нормированных значений максимальных выбросов ПФВК R_{max}. По оси абсцисс представлены интервалы значений уровня ПФВК, а по оси ординат показана частота попадания R_{max} в соответствующий интервал. Как видно из приведенных зависимостей, среднее значение максимальных боковых выбросов ПФВК находится в диапазоне $2/\sqrt{\mathrm{L}} - 3/\sqrt{\mathrm{L}}$, что соответствует результатам, приведенным в таблице 2.

В таблице 4 приведены результаты сравнения статистических характеристик линейных рекуррентных последовательностей максимального периода (ЛРПМ), характеристических последовательностей, производных ортогональных последовательностей [1] с синтезированными последовательностями.

Анализ данных таблицы 4 показывает, что по результатам сравнительного анализа формируемые последовательности обладают

улучшенными авто- и взаимокорреляционными свойствами. Как показывают проведенные исследования, математическое ожидание уровня боковых лепестков и математическое ожидание максимального выброса боковых лепестков для всех длин формируемых последовательностей имеют меньшие значения для любого из оцениваемых классов сигналов. Кроме того, оценки дисперсии и среднего квадратического отклонения свидетельствуют о небольшом отклонении оцениваемых параметров от их математического ожидания.

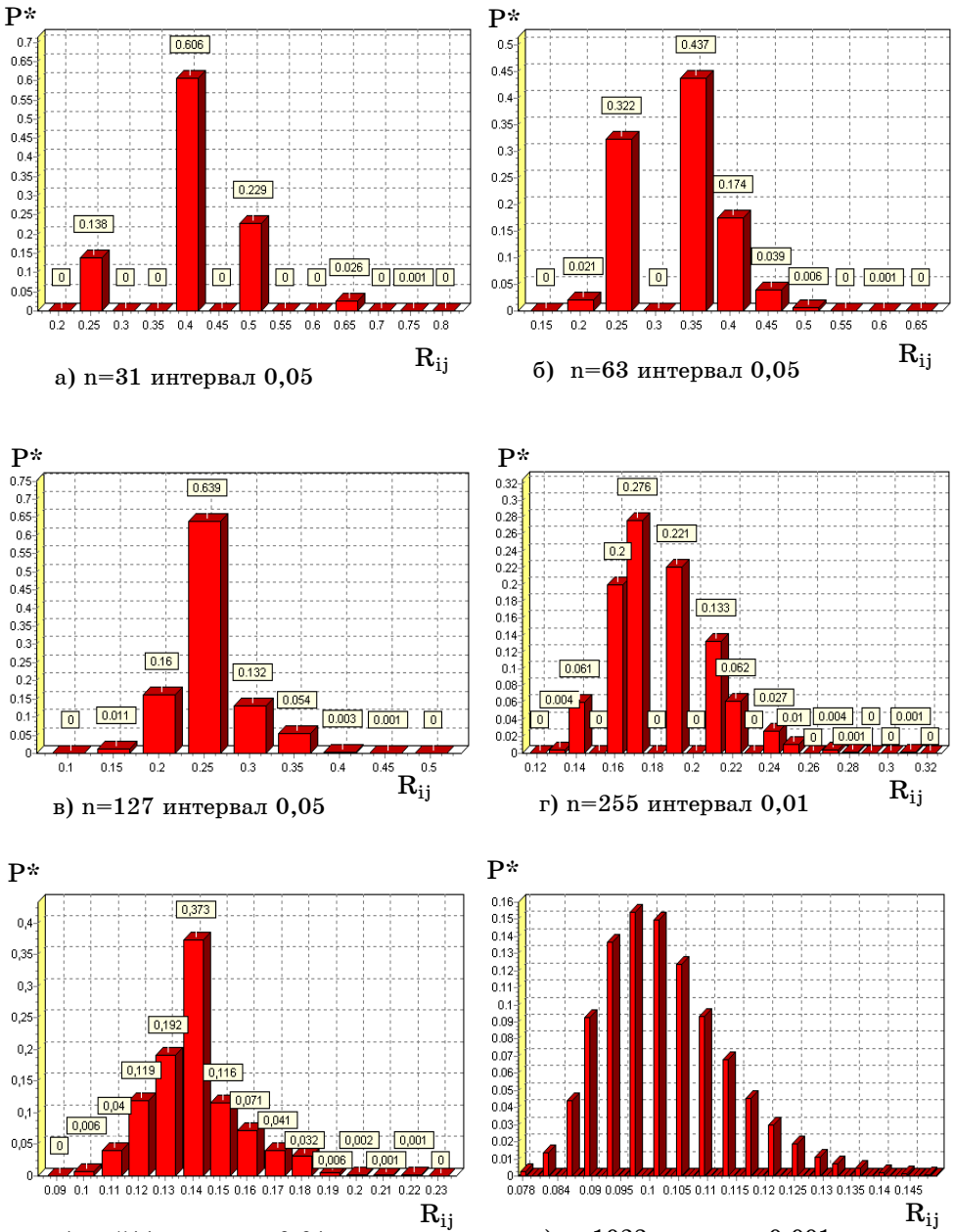

Рисунок 2 – Гистограммы распределения нормированных значений максимальных выбросов ПФВК

Таблица 4 – Сравнительная таблица статистических характеристик ПФВК

Линейные рекуррентные последовательности максимального периода						
Параметры ПФВК	Число элементов в сигнале					
	15	63	255	511	1023	
M	0,24	$0{,}85\cdot10^{-1}$	$0{,}46\cdot10^{-1}$	$0{,}32\cdot10^{-1}$	$0{,}93\cdot10^{-2}$	
$\sqrt{D_M}$	$0{,}5\cdot10^{-1}$	$0{,}94\cdot10^{-1}$	$0{,}2\cdot10^{-1}$	$0{,}63\cdot10^{-2}$	$0{,}54\cdot10^{-2}$	
D	$0{,}21\cdot10^{-1}$	$0{,}91\cdot10^{-2}$	$0{,}17\cdot10^{-2}$	$0{,}93\cdot10^{-3}$	$0{,}67\cdot10^{-3}$	
$\sqrt{D_D}$	0,3	$0{,}31\cdot10^{-1}$	$0{,}14\cdot10^{-1}$	$0{,}7\cdot10^{-2}$	$0{,}8\cdot10^{-2}$	
$U_{\max}$	$2{,}9/\sqrt{L}$	$2{,}5/\sqrt{L}$	$2{,}9/\sqrt{L}$	$3{,}1/\sqrt{L}$	$3{,}1/\sqrt{L}$	
$\sqrt{D_{U_{\max}}}$	$0{,}51\cdot10^{-1}$	$0{,}6\cdot10^{-1}$	$0{,}63\cdot10^{-1}$	$0{,}55\cdot10^{-2}$	$0{,}53\cdot10^{-2}$	
Характеристические последовательности						
Параметры ПФВК	Число элементов в сигнале					
	16	60	256	508	1020	
M	0,21	$0{,}82\cdot10^{-1}$	$0{,}51\cdot10^{-1}$	$0{,}34\cdot10^{-1}$	$0{,}89\cdot10^{-2}$	
$\sqrt{D_M}$	$0{,}71\cdot10^{-1}$	$0{,}98\cdot10^{-1}$	$0{,}29\cdot10^{-1}$	$0{,}73\cdot10^{-1}$	$0{,}59\cdot10^{-2}$	
D	$0{,}27\cdot10^{-1}$	$0{,}81\cdot10^{-2}$	$0{,}27\cdot10^{-2}$	$0{,}11\cdot10^{-1}$	$0{,}75\cdot10^{-3}$	
$\sqrt{D_D}$	0,34	$0{,}35\cdot10^{-1}$	$0{,}19\cdot10^{-1}$	$0{,}66\cdot10^{-2}$	$0{,}84\cdot10^{-2}$	
$U_{\max}$	$3{,}1/\sqrt{L}$	$3/\sqrt{L}$	$3{,}8/\sqrt{L}$	$3{,}2/\sqrt{L}$	$3{,}1/\sqrt{L}$	
$\sqrt{D_{U_{\max}}}$	$0{,}61\cdot10^{-1}$	$0{,}67\cdot10^{-1}$	$0{,}68\cdot10^{-1}$	$0{,}66\cdot10^{-1}$	$0{,}61\cdot10^{-2}$	
Производные ортогональные последовательности						
Параметры ПФВК	Число элементов в сигнале					
	16	60	256	508	1020	
M	$3{,}8\cdot10^{-2}$	$3{,}3\cdot10^{-2}$	$2{,}9\cdot10^{-2}$	$0{,}35\cdot10^{-1}$	$0{,}25\cdot10^{-1}$	
$\sqrt{D_M}$	$7{,}5\cdot10^{-5}$	$0{,}5\cdot10^{-4}$	$8{,}7\cdot10^{-6}$	$0{,}9\cdot10^{-3}$	$0{,}69\cdot10^{-3}$	
D	$5{,}6\cdot10^{-2}$	$1{,}5\cdot10^{-2}$	$4{,}4\cdot10^{-3}$	$0{,}71\cdot10^{-3}$	$0{,}36\cdot10^{-3}$	
$\sqrt{D_D}$	$0{,}4\cdot10^{-1}$	$6{,}4\cdot10^{-7}$	$1{,}2\cdot10^{-6}$	$0{,}64\cdot10^{-3}$	$0{,}57\cdot10^{-3}$	
$U_{\max}$	0,38	0,33	0,19	$3{,}2/\sqrt{L}$	$3{,}8/\sqrt{L}$	
$\sqrt{D_{U_{\max}}}$	$2{,}1\cdot10^{-3}$	$1{,}8\cdot10^{-3}$	$1{,}1\cdot10^{-3}$	$0{,}85\cdot10^{-1}$	$0{,}77\cdot10^{-3}$	
Полученные последовательности						
Параметры ПФВК	Число элементов в сигнале					
	31	63	127	255	511	1023
M	$1{,}1\cdot10^{-3}$	$0{,}26\cdot10^{-3}$	$6{,}24\cdot10^{-5}$	$1{,}54\cdot10^{-5}$	$3{,}74\cdot10^{-6}$	$9{,}85\cdot10^{-7}$
$\sqrt{D_M}$	$0{,}28\cdot10^{-2}$	$0{,}1\cdot10^{-2}$	$0{,}35\cdot10^{-3}$	$0{,}12\cdot10^{-3}$	$4{,}32\cdot10^{-5}$	$1{,}53\cdot10^{-5}$
D	$0{,}34\cdot10^{-1}$	$0{,}16\cdot10^{-1}$	$0{,}8\cdot10^{-2}$	$0{,}39\cdot10^{-2}$	$0{,}2\cdot10^{-2}$	$0{,}98\cdot10^{-3}$
$\sqrt{D_D}$	$0{,}85\cdot10^{-2}$	$0{,}29\cdot10^{-2}$	$0{,}1\cdot10^{-2}$	$0{,}35\cdot10^{-3}$	$0{,}12\cdot10^{-3}$	$0{,}1\cdot10^{-3}$
$U_{\max}$	0,37 $2{,}08/\sqrt{L}$	0,296 $2{,}347/\sqrt{L}$	0,23 $2{,}6/\sqrt{L}$	0,18 $2{,}82/\sqrt{L}$	0,135 $3{,}04/\sqrt{L}$	0,102 $3{,}25/\sqrt{L}$
$\sqrt{D_{U_{\max}}}$	$0{,}88\cdot10^{-1}$	$0{,}57\cdot10^{-1}$	$0{,}37\cdot10^{-1}$	$0{,}24\cdot10^{-1}$	$0{,}16\cdot10^{-1}$	$0{,}11\cdot10^{-1}$

ВЫВОДЫ

В результате проведенных исследований разработан метод формирования псевдослучайных последовательностей, основанный на использовании развитого математического аппарата алгебраической теории кодов и методов защиты информации, который позволяет за счет применения корректирующих кодов реализовать высокие дистанционные свойства формируемых дискретных последовательностей, а посредством перестановочных преобразований обеспечить их псевдослучайность. Как показали проведенные статистические исследования, последовательности, полученные с использованием предложенного метода, обладают улучшенными авто- и взаимокорреляционными свойствами.

SUMMARY

Generation methods of big ensembles weakly correlated discrete signals is analyzed. Pseudorandom sequences with improved auto- and inter- correlation characteristics generation method is proposed.

СПИСОК ЛИТЕРАТУРЫ

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.
2. Горбенко И.Д., Стасев Ю.В., Замула А.А. Теория дискретных сигналов. Ортогональные сигналы. – М.: МО СССР, 1988. – 119с.
3. Стасев Ю.В., Горбенко И.Д. и др. Применение сложных сигналов в командно-телеметрических радиолиниях //Космічна наука і технологія. – 1997. –Т.3, №5/6. – С. 104-108.
4. Горбенко И.Д., Стасев Ю.В. Безопасность информации в космических системах связи и управления //Космічна наука і технологія. – 1996. – Т.2, № 5/6. – С. 24–28.
5. Гряник М.В., Фролов В.И. Технология CDMA – будущее сотовых систем в Украине // Мир связи. – 1998. – № 3. – С. 40–43.
6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. – М.: Вильямс, 2003. – 1104 с.
7. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.
8. Науменко М.І., Стассв Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів: Монографія. – Харків:ХУ ПС, 2005. – 267с.
9. Кузнецов А.А., Носик А.М., Стасев С.Ю. Синтез ансамблей дискретных сигналов с использованием алгебраических методов помехоустойчивого кодирования // Збірник наукових праць ХУ ПС. – Харків: ХУПС, 2006.–Вип.6(12).–С. 40-42
10. Шеннон К. Теория связи в секретных системах // К. Шеннон Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С. 333-402.
11. Horst Feistel. Cryptography and Computer Privacy. // Scientific American. – May 1973. – Vol. 228, No.5. – pp. 15-23.
12. National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard." Oct. 1999. Available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
13. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at http://csrc.nist.gov/publications/fips/ fips197/fips-197.pdf
14. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. April 19, 2004. – p. 836.
15. Вентцель Е.С., Овчаров Л.А. Теория вероятностей и ее инженерные приложения: Учеб. пособие для втузов.– 2-е изд., стер. – М.: Высш. шк., 2000. – 480 с.
16. Коваленко И.Н., Филиппова А.А. Теория вероятностей и математическая статистика: Учеб. пособие для вузов. – М.: Высшая школа, 1973. – 308 с.
17. Rational Chebyshev Approximations for the Error Function, W.J. Cody. Mathematics of Computation 23, n107, 631-637 (July 1969).

А.А. Кузнецов, канд. техн. наук
Харьковский университет воздушных сил им. И. Кожедуба

А.М. Носик
Харьковский университет воздушных сил им. И. Кожедуба

А.Н. Коваленко
Харьковский университет воздушных сил им. И. Кожедуба

Поступила в редакцию 20 февраля 2007 г.