УДК 621.391

Алгоритм и устройство формирования ансамблей псевдослучайных ортогональных последовательностей для систем передачи информации с кодовым разделением каналов

Жук А. П., Студеникин А. В., Жук Е. П.

Постановка задачи: *повышение структурной скрытности систем передачи информации с кодовым разделением каналов выдвигает на передний план задачу построения устройств формирования представительного количества ансамблей ортогональных последовательностей для последующего их использования псевдослучайным образом. Известные технические решения в данной области и алгоритмы их функционирования ограничены незначительным количеством формируемых ансамблей ортогональных последовательностей, узкими возможностями изменения размерности генерируемых ансамблей, низкой точностью формирования и отсутствием возможности автоматической генерации по псевдослучайному алгоритму.* ***Целью работы*** *является повышение количества ансамблей ортогональных последовательностей на основе реализации нового алгоритма их формирования. Предлагается автоматизировать процесс присвоения псевдослучайных исходных данных диагональным коэффициентам симметрической матрицы в генераторе функций Попенко-Турко за счет внедрения в него блока псевдослучайного формирования коэффициентов симметрической матрицы, что обеспечивает автоматическую генерацию ансамблей псевдослучайных ортогональных последовательностей на выходах генератора.* ***Используемые методы****: решение задачи основано на использовании метода векторного синтеза ансамблей ортогональных последовательностей с учетом ограничений на числовой диапазон задаваемых псевдослучайных исходных данных. В качестве основного показателя разработанного генератора используется максимальное количество формируемых структур ансамблей псевдослучайных ортогональных последовательностей.* ***Новизна:*** *элементами новизны являются получение нового алгоритма формирования ансамблей псевдослучайных ортогональных последовательностей на основе использования метода векторного синтеза и схемной реализации генератора ансамблей псевдослучайных ортогональных последовательностей.* ***Результат****: использование разработанного генератора и алгоритма формирования ансамблей псевдослучайных ортогональных последовательностей позволяет формировать их увеличенное количество, которое позволит повысить структурную скрытность систем передачи информации с кодовым разделением каналов. Представленная реализация генератора ансамблей псевдослучайных ортогональных последовательностей и предложенный алгоритм формирования ансамблей псевдослучайных ортогональных последовательностей обеспечивают повышение количества структур ортогональных последовательностей, используемых в системах передачи информации, и, как следствие, увеличение их структурной скрытности. Количество возможных структур ортогональных последовательностей, формируемых на основе разработанного алгоритма, по сравнению с количеством последовательностей рассматриваемого класса, формируемых на основе наиболее известного алгоритма де Брейна, показывает преимущество первого над вторым от 1,5 до 6 раз при различных размерностях ансамблей ортогональных последовательностей.* ***Практическая значимость****: разработанный генератор ансамблей псевдослучайных ортогональных последовательностей, в случае применения в виде компонента системы передачи информации с кодовым разделением каналов, позволит увеличить время, в течение которого не будут повторяться используемые для информационного обмена структуры последовательностей за счет увеличения их количества. Применение увеличенного количества ансамблей псевдослучайных ортогональных последовательностей для реализации информационного обмена в системах передачи информации с кодовым разделением каналов позволит повысить их структурную скрытность.*

Ключевые слова: *система передачи информации с кодовым разделением каналов, генератор псевдослучайных ортогональных последовательностей, структурная скрытность, собственные векторы, симметрическая матрица.*

Библиографическая ссылка на статью:
Жук А. П., Студеникин А. В., Жук Е. П. Алгоритм и устройство формирования ансамблей псевдослучайных ортогональных последовательностей для систем передачи информации с кодовым разделением каналов // Системы управления, связи и безопасности. 2020. № 3. С. 1-21. DOI: 10.24411/2410-9916-2020-10301

Reference for citation:
Zhuk A. P., Studenikin A. V., Zhuk E. P. Algorithm and device for forming ensembles of pseudorandom orthogonal sequences in information transfer systems with code-division multiple access. *Systems of Control, Communication and Security*, 2020, no. 3, pp. 1-21 (in Russian). DOI: 10.24411/2410-9916-2020-10301

Актуальность

Наряду с общей тенденцией развития инфотелекоммуникационных систем выделяется тенденция дальнейшего расширения области применения беспроводных систем связи по причине удобства их использования мобильными пользователями. Достаточно широко беспроводные инфотелекоммуникационные системы и сети применяются в специальных целях. В этом случае они должны обладать дополнительными характеристиками, обеспечивающими возможность их функционирования в условиях радиоэлектронного противоборства [1, 2]. Развитие беспроводных систем передачи информации (БСПИ) специального назначения, с учетом отмеченного обстоятельства, связано с генерацией и обработкой сложных сигналов, имеющих широкую полосу частот спектра, а также применением специальных алгоритмов информационного обмена, обеспечивающих им необходимые характеристики, одной из которых является разведывательная защищённость (разведзащищённость), которая характеризует способность системы связи противостоять всем видам разведки противника. Система связи специального назначения должна иметь возможность препятствовать или затруднять противнику достижение его целей по обнаружению факта работы системы передачи информации, выявлению параметров радиопередачи, выявлению местоположения, перехвату информации, подавлению радиолинии преднамеренными помехами и уничтожению источника излучения. Для этого она должна обеспечить максимальную неопределенность (неосведомленность) противника относительно интересующих его параметров передачи. Одним из основных методов повышения разведзащищенности беспроводных систем передачи информации является применение радиосигналов с быстроменяющимися по псевдослучайному закону (неизвестному противнику) параметрами [2-5].

Особое место среди беспроводных систем передачи информации занимают системы с кодовым разделением каналов (КРК), в которых в качестве сигналов-переносчиков информации используются ортогональные кодовые последовательности [6-14]. БСПИ с КРК имеют ряд положительных свойств, основными из которых является высокая помехоустойчивость, рациональное использование частотного спектра, возможность эффективного функционирования в условиях многолучевого распространения радиоволн и др., поэтому они имеют широкое применение в различных целях. Основополагающим принципом работы данных систем является использование регулярных ортогональных последовательностей, достаточно хорошо известных из математики, таких как Уолша, Голда, Радемахера, Стиффлера, Джеффи и др. [15-18]. В силу незначительного количества, регулярности и широкой известности ортогональных последовательностей, используемых в БСПИ с КРК, можно сделать вывод о том, что они обладают низкой структурной скрытностью, которая не может обеспечить высокую разведывательную защищённость данных систем. По данной причине задача формирования ансамблей ортогональных последовательностей с требуемыми характеристиками и в количестве, достаточном для изменения их параметров по псевдослучайному закону, является актуальной.

DOI: 10.24411/2410-9916-2020-10301
URL: https://sccs.intelgr.com/archive/2020-03/01-Zhuk.pdf

Вопросам разработки способов, обеспечивающих увеличения количества синтезируемых ортогональных последовательностей посвящены работы [19-21]. В них предложены подходы к получению увеличенных наборов ансамблей ортогональных последовательностей, однако они ограничены верхним пределом, недостаточным для их практического использования. В работах [22, 23] предлагается метод векторного синтеза различных наборов ансамблей ортогональных последовательностей, моделируемых собственными векторами симметрических матриц. Однако вопросы построения устройств генерации последовательностей данного типа не рассматривались. В работах [24-27] предложен способ передачи информации на основе хаотически формируемых ансамблей дискретных многоуровневых ортогональных сигналов, в котором в качестве ортогональных расширяющих последовательностей на каждом такте передачи сообщения используется расширяющая последовательность в виде одного из сигналов ортогональной системы сигналов, описываемой собственными векторами диагональной положительно определённой симметрической матрицы (ПОСМ). Однако вопросы построения устройства формирования ансамблей ортогональных последовательностей по псевдослучайному алгоритму в них детально не рассматривались. В работе [28] предложен подход к генерации ортогональных базисов на основе собственных векторов ПОСМ с действительными положительными коэффициентами, принадлежащими интервалу (0; 1). Однако в данной работе вопросы формирования ортогональных последовательностей на основе метода векторного синтеза по псевдослучайному алгоритму авторами не рассматривались.

Предлагается воспользоваться разработанными подходами, связанными с представлением ансамблей ортогональных последовательностей собственными векторами симметрических матриц, способом получения увеличенного количества ансамблей ортогональных последовательностей на основе псевдослучайного задания значений диагональных коэффициентов симметрических матриц и генератором ортогональных базисов на основе собственных векторов ПОСМ с действительными положительными коэффициентами. На их основе разработан новый алгоритм формирования ансамблей псевдослучайных ортогональных последовательностей, базирующийся на методе векторного синтеза, а также схемная реализация генератора ансамблей псевдослучайных ортогональных последовательностей, обеспечивающие формирование увеличенного количества структур рассматриваемых последовательностей.

Постановка задачи

Повышение разведывательной защищённости систем передачи информации с кодовым разделением каналов на основе структурной скрытности канальных сигналов напрямую связано с решением задачи построения устройств формирования представительного количества ансамблей ортогональных последовательностей и последующего их использования по псевдослучайному алгоритму. Известные технические решения в данной области и алгоритмы их функционирования ограничены количеством формируемых ансамблей ортогональных последовательностей, узкими возможностями по изменению размер-

ности генерируемых ансамблей, низкой точностью формирования и отсутствием возможности автоматической генерации по псевдослучайному алгоритму.

Целью работы является повышение количества формируемых ансамблей псевдослучайных ортогональных последовательностей за счет расширения возможностей устройства формирования ортогональных последовательностей по псевдослучайному алгоритму.

Для формальной постановки и решения задачи в работе введены обозначения, представленные в таблице 1.

Таблица 1 – Обозначения и их физический смысл

Обозначение	Физический смысл обозначения
Z_{m+1}	– очередное значение последовательности псевдослучайных чисел $\{Z\}$ на выходе генератора псевдослучайных чисел
$Z_{m+1}= f(Z_{m-k+1}, Z_{m-k+2},\ldots, Z_m)$	– функция преобразования k последних членов последовательности псевдослучайных чисел Z_{m-k+1}, $Z_{m-k+2},\ldots$, Z_m в очередное значение Z_{m+1} последовательности псевдослучайных чисел $\{Z\}$
$A = [a_m],\ m \in [1,k]$	– треугольная матрица, состоящая из k элементов
$A' = \left[a_{ij} \right],\ i \in [1,n],\ j \in \left[1,n\right]$	– квадратная матрица размерностью n
$x^{(j)} = \begin{pmatrix} x_1^{(j)} \\ . \\ . \\ . \\ x_n^{(j)} \end{pmatrix},\ j = (1,2,...,n),$	– j-й собственный вектор квадратной матрицы A', удовлетворяющий условию $A \cdot x^{(j)} = \lambda_j \cdot x^{(j)}$
$x_i^{(j)} = \left(\begin{pmatrix} x_1^{(1)} \\ . \\ . \\ . \\ x_n^{(1)} \end{pmatrix}, \begin{pmatrix} x_1^{(2)} \\ . \\ . \\ . \\ x_n^{(2)} \end{pmatrix}, ..., \begin{pmatrix} x_1^{(j)} \\ . \\ . \\ . \\ x_n^{(j)} \end{pmatrix} \right) \Rightarrow \begin{pmatrix} S_1(t), \\ S_2(t), \\ . \\ . \\ . \\ S_n(t). \end{pmatrix}$	– ансамбль (система) ортогональных последовательностей $S_i(t)$, определяемый совокупностью собственных векторов $x_i^{(j)}$ квадратной матрицы A'
$M_{\text{ПСП}}$	– количество ансамблей ортогональных псевдослучайных последовательностей $S_i(t)$

На формальном уровне постановка задачи исследования имеет следующий вид.

Дано: $M_{\text{И}}$ количество известных ансамблей ортогональных последовательностей; множество $\{PT\}$, определяющее состав элементов генератора функций Попенко-Турко (ГФПТ); оператор E, определяющий алгоритм формирования базисных функций в ГФПТ.

Найти: множество $\{L\}$, определяющее состав элементов генератора псевдослучайных ортогональных последовательностей (ГПСОП), обеспечивающего формирование количества ансамблей псевдослучайных ортогональных последовательностей, превышающее число известных $M_{\text{ПСП}} > M_{\text{И}}$; оператор H, опре-

DOI: 10.24411/2410-9916-2020-10301
URL: https://sccs.intelgr.com/archive/2020-03/01-Zhuk.pdf

деляющий алгоритм формирования ансамблей псевдослучайных ортогональных последовательностей $S_i(t)$, определяемых системами собственных векторов $x_i^{(j)}$ квадратных матриц A' порядка n с псевдослучайными значениями диагональных коэффициентов $[a_{ij}]$.

Разработка структуры генератора псевдослучайных ортогональных последовательностей и алгоритма формирования ансамблей псевдослучайных ортогональных последовательностей

Анализ известных подходов к формированию ансамблей ортогональных последовательностей показывает, что наибольшие возможности по формированию ортогональных функций имеются у генератора функций Попенко – Турко [28]. По этой причине он выбран за основу для построения генератора псевдослучайных ортогональных последовательностей.

Работа ГФПТ основана на вычислении ортогонального базиса положительно определённой симметрической матрицы с действительными положительными коэффициентами, принадлежащими интервалу (0; 1).

$$A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n1} & \dots & a_{nn} \end{pmatrix}. \quad (1)$$

Для обеспечения возможности применения матрица A должна удовлетворять следующим условиям:

- любой коэффициент матрицы A вида (1) должен иметь положительное значение

$$a_{ij} > 0, i \in [1,n],\ j \in [1,n]; \quad (2)$$

- должно соблюдаться свойство симметричности для коэффициентов матрицы, не принадлежащих главной диагонали

$$a_{ij} = a_{ji}, i \in [1,n],\ j \in [1,\mathrm{n}], i \neq j. \quad (3)$$

Недостатками ГФПТ является отсутствие автоматического поступления входных данных, а также отсутствие возможности стохастического формирования ансамблей ортогональных последовательностей различной структуры.

Для устранения указанных недостатков ГФПТ авторами предлагается структура ГПСОП, представленная на рис. 1.

Исходную структуру ГФПТ предлагается дополнить блоком псевдослучайного формирования коэффициентов симметрической матрицы, состоящим из микроконтроллера, генератора псевдослучайных чисел (ГПСЧ), блока накопителя (БН), блока N – разрядного (N – разрядность генерируемых ГПСЧ псевдослучайных коэффициентов матрицы) оперативного запоминающего устройства (ОЗУ), а также исключить обратную связь в трехразрядном регистре, который обеспечивает вывод из блока памяти дискретных базисных функций $S_1(t)$, $S_2(t)$, $S_3(t)$, получаемых на основе расчета собственных векторов матрицы вида (1) для исключения цикличности вывода ортогонального базиса.

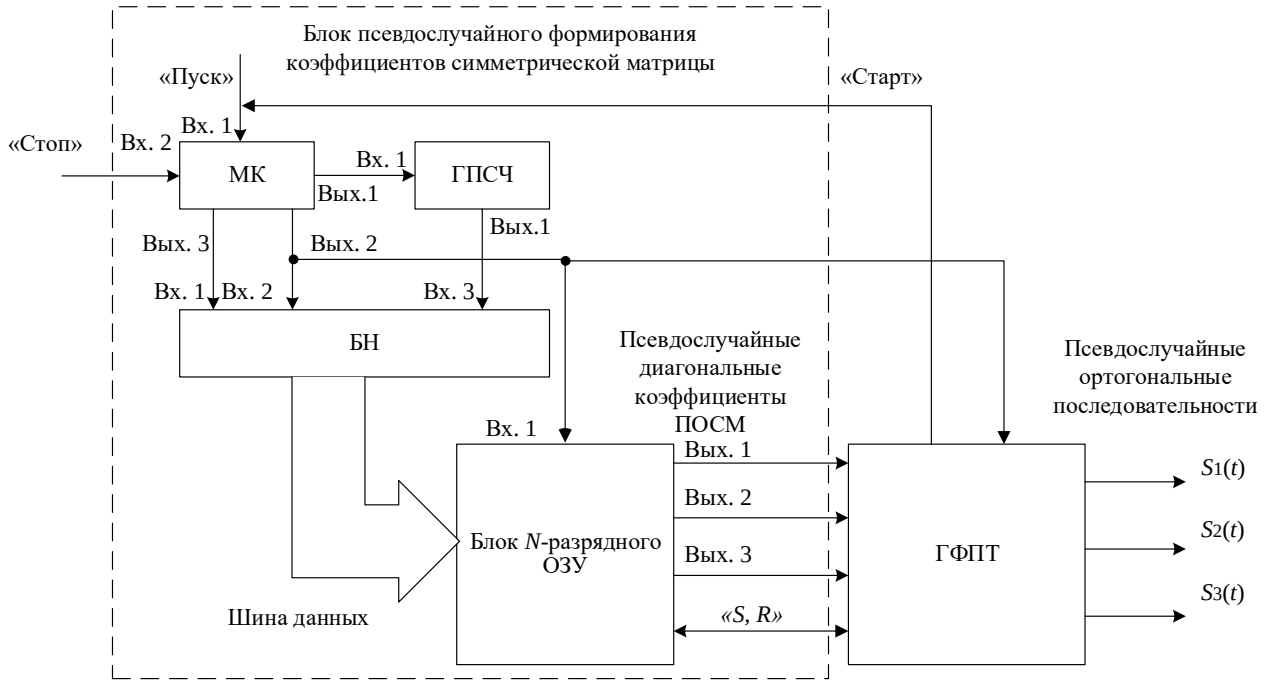

Рис. 1. Структура генератора псевдослучайных ортогональных последовательностей

За счет доработки ГФПТ путем добавления элементов и исключения связей появляется возможность автоматизировать процесс присвоения псевдослучайных исходных данных диагональным коэффициентам симметрической матрицы и тем самым обеспечить формирование различных по форме ансамблей псевдослучайных ортогональных последовательностей.

Алгоритм формирования ансамблей псевдослучайных ортогональных последовательностей представлен на рис. 2 и состоит из одиннадцати этапов. Рассмотрим основное содержание этапов представленного алгоритма.

На первом этапе осуществляется ввод исходных данных, определение начальных значений переменных (комментарий 1, рис. 2). В качестве исходных данных выступают порядок симметрической положительно определённой симметрической матрицы n и время, необходимое генератору псевдослучайных чисел на генерацию псевдослучайного числа $t_{\text{ген}}$. На основании введенных исходных данных производится расчет и присвоение начальных значений переменных k, m=1, S=0, R=0.

С учетом условия (3) для формирования симметрической матрицы A необходимо ввести лишь элементы верхней или нижней её части. Формула расчёта количества элементов k треугольной матрицы порядка n для получения квадратной матрицы вида (1) порядка n выглядит следующим образом [28]:

$$k = \frac{(n^2 - n)}{2} + n. \qquad (4)$$

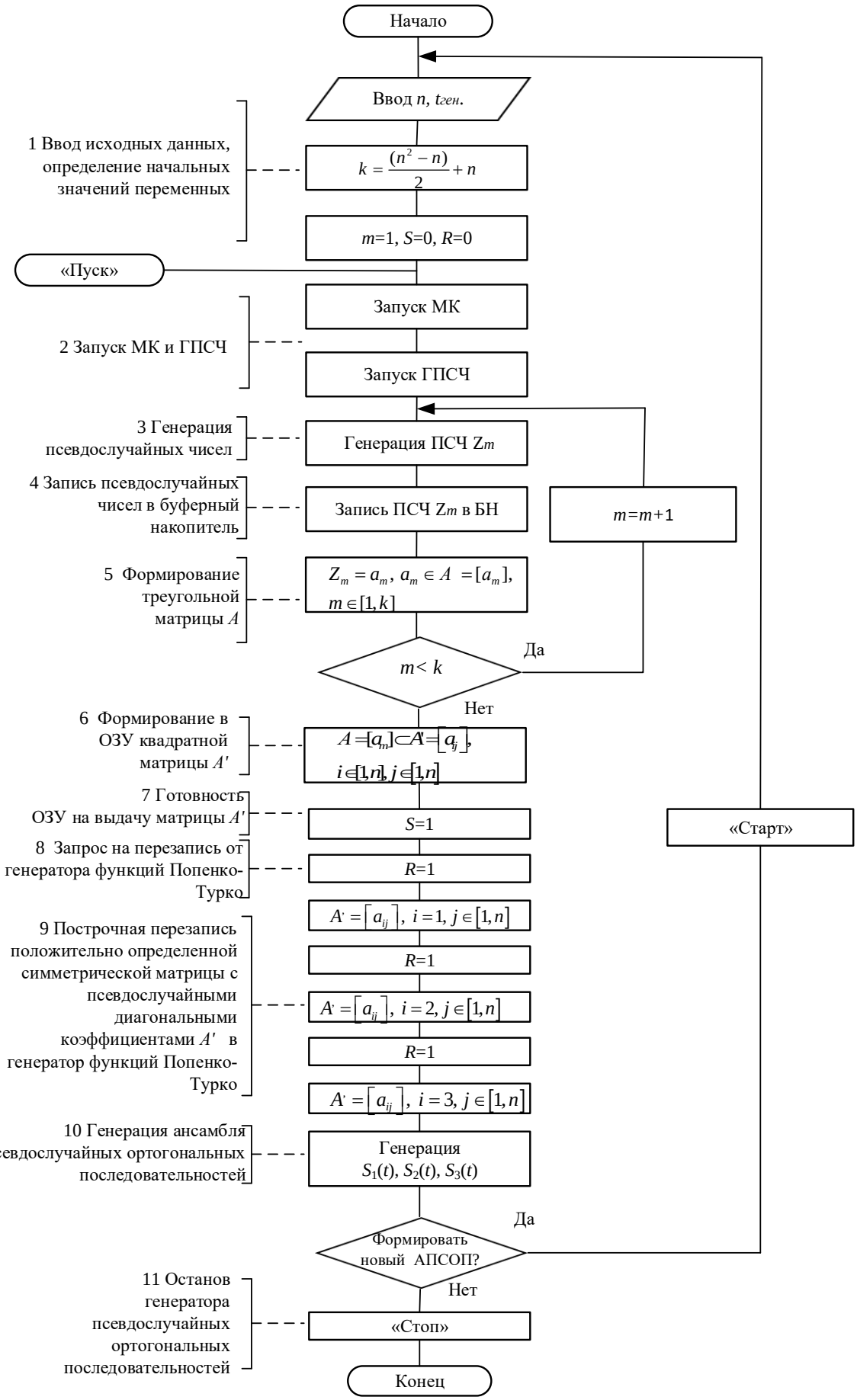

Рис. 2. Алгоритм формирования ансамблей
псевдослучайных ортогональных последовательностей

Второй этап алгоритма начинается с поступления команды «Пуск» на начало работы генератора (комментарий 2, рис. 2). По данной команде запускается в работу микроконтроллер МК, который запускает в работу ГПСЧ.

На третьем этапе генератором псевдослучайных чисел формируется первое псевдослучайное число Z_1 из последовательности k псевдослучайных чисел с определенным временным интервалом $t_{\text{ген}}$ (комментарий 3, рис. 2).

На четвертом этапе осуществляется запись сформированного псевдослучайного числа в буферный накопитель (комментарий 4, рис. 2).

Пятый этап алгоритма характеризуется началом формирования треугольной матрицы A первым псевдослучайным числом (комментарий 5, рис. 2). В результате выполнения k итераций и повторных операций, предусмотренных третьим, четвертым и пятым этапами алгоритма, формируется серия из k псевдослучайных чисел Z_{m-k+1}, Z_{m-k+2},…, Z_m, для формирования треугольной матрицы A в буферном накопителе БН.

На шестом этапе осуществляется формирование в ОЗУ квадратной матрицы A' на основе треугольной матрицы A (комментарий 6, рис. 2).

На седьмом этапе после завершения формирования квадратной матрицы A', из ОЗУ поступает команда готовности в виде сигнала S=1, выдаваемого по линии «S, R», который свидетельствует о возможности выдачи заполненной псевдослучайными числами матрицы A' в качестве исходных данных генератору функций Попенко-Турко (комментарий 7, рис. 2).

На восьмом этапе в ответ на команду готовности из ОЗУ (S=1) генератор функций Попенко-Турко делает запрос в ОЗУ на перезапись от генератора функций Попенко-Турко путем формирования сигнала R=1, выдаваемого по линии «S, R» (комментарий 8, рис. 2).

На девятом этапе реализуется построчная перезапись положительно определенной симметрической матрицы с псевдослучайными диагональными коэффициентами A' в генератор функций Попенко-Турко (комментарий 9, рис. 2).

На десятом этапе осуществляется генерация ансамбля псевдослучайных ортогональных последовательностей, состоящего из набора последовательностей $S_1(t)$, $S_2(t)$, …, $S_n(t)$. В алгоритме показан случай формирования сигналов для n=3 (комментарий 10, рис. 2).

Ансамбль псевдослучайных ортогональных последовательностей описывается совокупностью собственных векторов симметрической положительно определённой матрицей порядка n вида (1), имеющими следующее представление

$$x^{(j)} = \begin{pmatrix} x_1^{(j)} \\ . \\ . \\ . \\ x_n^{(j)} \end{pmatrix}, j = (1, 2, ..., n), \quad (5)$$

являющимися действительными и удовлетворяющими условию ортогональности [29-31]

$$\sum_{i=1}^{n} x_i^{(j)} x_i^{(k)} = 0,\ j \neq k\ . \qquad (6)$$

Таким образом, положительно определённая симметрическая квадратная матрица A' порядка n имеет n собственных векторов, т.е. их число равно порядку матрицы A'.

На одиннадцатом этапе осуществляется следующий цикл работы ГПСОП по команде «Старт», поступающей с генератора функций Попенко-Турко, начиная с этапа ввода исходных данных и определения начальных значений переменных, и заканчивая этапом генерации ансамбля псевдослучайных ортогональных последовательностей $S_1(t)$, $S_2(t)$, …, $S_n(t)$, сгенерированных из нового набора псевдослучайных чисел (комментарий 11, рис. 2).

Остановка генератора псевдослучайных ортогональных последовательностей осуществляется по команде «Стоп», выдаваемой из микроконтроллера МК, в случае отсутствия необходимости формирования следующего ансамбля псевдослучайных ортогональных последовательностей.

Таким образом, данный алгоритм позволяет из наборов последовательностей псевдослучайных чисел, формируемых генератором псевдослучайных чисел, получить наборы различных ансамблей псевдослучайных ортогональных последовательностей. Генерируемые наборы ансамблей псевдослучайных ортогональных последовательностей будут отличаться друг от друга по форме, а в случае их использования в качестве расширяющих последовательностей в БСПИ с КРК с учетом их представительного количества могут в течение длительного времени не повторяться.

Пример реализации алгоритма формирования ансамбля псевдослучайных ортогональных последовательностей

Для примера рассмотрим реализацию алгоритма формирования ансамбля, состоящего из трех псевдослучайных ортогональных последовательностей.

Для этого в качестве исходных данных зададим порядок матрицы A n=3. С учетом (4) число вводимых диагональных коэффициентов матрицы будет равно k=6.

По команде «Пуск» запускается микроконтроллер МК, который далее запускает генератор псевдослучайных чисел ГПСЧ.

Для заполнения матрицы A псевдослучайными числами от ГПСЧ достаточно будет сформировать 6 псевдослучайных чисел Z_1–Z_6. ГПСЧ формирует псевдослучайное число Z_1 и со своего первого выхода передает его на третий вход блока накопителя БН для временного хранения. По прошествии определенного времени, равному $t_{\text{ген}}$, необходимого ГПСЧ на выработку псевдослучайного числа Z_1, микроконтроллер МК с первого выхода подает на первый вход ГПСЧ команду на генерацию следующего псевдослучайного числа Z_2. Величина $t_{\text{ген}}$ выбирается согласно соответствующей характеристике аппаратной реализации ГПСОП и записывается предварительно в память микроконтроллера МК. Микроконтроллер МК одновременно с третьего выхода подает команду на первый вход блока накопителя БН на запоминание им выработанного ГПСЧ

Z_2 и с первого выхода подает на первый вход ГПСЧ команду на генерацию следующего псевдослучайного числа Z_3.

Микроконтроллер МК одновременно с третьего выхода подает команду на первый вход блока накопителя БН на запоминание им выработанного ГПСЧ Z_3. Далее описанный процесс продолжается аналогичным образом, пока по командам микроконтроллера с помощью ГПСЧ не будут сформированы шесть псевдослучайных чисел Z_1–Z_6. Из буферного накопителя сформированные псевдослучайные числа Z_1–Z_6 поступают в блок N – разрядного ОЗУ, где они преобразуются в массив данных, в виде шести псевдослучайных чисел, присвоенных диагональным коэффициентам ПОСМ A.

Окончание процесса формирования массива псевдослучайных данных отмечается сигналом S=1, поступающим с выхода ОЗУ на вход ГФПТ по управляющей линии «*S, R*». Массив исходных данных может временно храниться в ОЗУ до момента поступления запроса в виде сигнала R=1 от ГФПТ по управляющей линии «*S, R*».

После этого ГФПТ для вычисления ансамбля псевдослучайных ортогональных последовательностей дает команду запроса R=1 на вход Вх. 2 блока N – разрядного ОЗУ. По этой команде из блока N – разрядного ОЗУ по выходу Вых. 1 выдаются значения первой строки записанного ранее массива данных, которые в течение времени записи $t_{зап}$ поступают в ГФПТ и присваиваются в качестве исходных данных коэффициентам первой строки ПОСМ. Далее по окончании записи первой строки ГФПТ формирует сигнал запроса R=1 на управляющую линию «*S, R*» для получения второй строки массива данных. По этой команде из блока N – разрядного ОЗУ по выходу Вых. 2 выдаются значения второй строки записанного ранее массива данных, которые в течение времени записи $t_{зап}$ поступают в ГФПТ и присваиваются в качестве исходных данных коэффициентам второй строки ПОСМ. Далее по окончании записи второй строки ГФПТ формирует сигнал запроса R=1 на управляющую линию «*S, R*» для получения третьей строки массива данных. По этой команде из блока N – разрядного ОЗУ по выходу Вых. 3 выдаются значения третьей строки записанного ранее массива данных, которые в течение времени записи $t_{зап}$ поступают в ГФПТ и присваиваются в качестве исходных данных коэффициентам третьей строки ПОСМ. После этого считается, что массив исходных данных в виде псевдослучайных чисел диагональных коэффициентов ПОСМ для работы ГФПТ задан. На основании заданного набора псевдослучайных диагональных коэффициентов ПОСМ генератор функций Попенко-Турко в течение некоторого времени $t_{выч}$ производит расчет собственных векторов этой матрицы, которые представляют собой следующий ансамбль псевдослучайных ортогональных последовательностей $S_1(t)$, $S_2(t)$, $S_3(t)$ на его выходах

$$x_i^{(j)} = \left(\begin{pmatrix} x_1^{(1)} \\ \cdot \\ \cdot \\ \cdot \\ x_n^{(1)} \end{pmatrix}, \begin{pmatrix} x_1^{(2)} \\ \cdot \\ \cdot \\ \cdot \\ x_n^{(2)} \end{pmatrix}, ..., \begin{pmatrix} x_1^{(j)} \\ \cdot \\ \cdot \\ \cdot \\ x_n^{(j)} \end{pmatrix} \right) \Rightarrow \begin{pmatrix} S_1(t), \\ S_2(t), \\ \cdot \\ \cdot \\ \cdot \\ S_n(t). \end{pmatrix}. \quad (7)$$

DOI: 10.24411/2410-9916-2020-10301
URL: https://sccs.intelgr.com/archive/2020-03/01-Zhuk.pdf

В последующем с помощью тактового генератора в моменты времени $t_{так}$ ансамбль псевдослучайных ортогональных последовательностей $S_1(t)$, $S_2(t)$, $S_3(t)$ по параллельным выходам выдается на выходы ГФПТ. После формирования ансамбля псевдослучайных ортогональных последовательностей $S_1(t)$, $S_2(t)$, $S_3(t)$ на основании первого массива псевдослучайных данных ГФПТ выдает команду «Старт» на первый вход микроконтроллера МК. На основании этой команды микроконтроллер МК формирует команду на первый вход ГПСЧ на генерацию следующего набора псевдослучайных чисел Z_1–Z_6. Эта процедура выполняется согласно описанного выше алгоритма. На основании сформированного набора Z_1–Z_6 с помощью ГФПТ будет сформирован новый ансамбль псевдослучайных ортогональных последовательностей вида (7). С учетом того, что последующие наборы Z_1–Z_6 каждый раз будут отличны от предшествующих, ансамбли псевдослучайных ортогональных последовательностей $S_1(t)$, $S_2(t)$, $S_3(t)$, которые получены на их основе, тоже будут отличаться друг от друга. За счет этого будет обеспечиваться уникальность формируемых ансамблей псевдослучайных ортогональных последовательностей на выходах ГПСОП.

Остановка процесса формирования ансамблей псевдослучайных ортогональных последовательностей на выходах ГПСОП осуществляется командой «Стоп», поступающей в необходимый момент времени на вход Вх. 2 микропроцессора МК, который блокирует работу ГПСЧ, блока накопителя БН, блока N – разрядного ОЗУ и ГФПТ. Описанный выше процесс иллюстрируется на рис. 3.

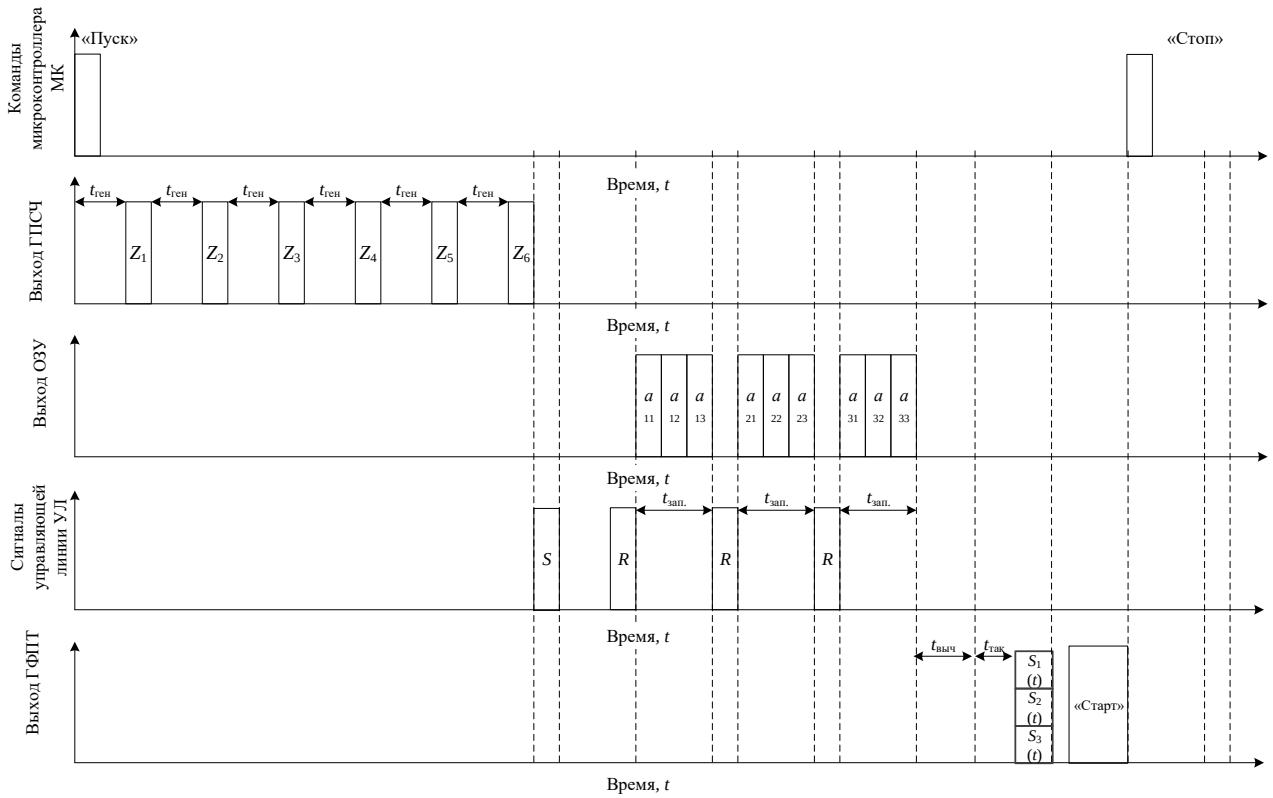

Рис. 3. Временные диаграммы работы генератора псевдослучайных ортогональных последовательностей

На рис.3 показаны следующие временные диаграммы (сверху вниз):
- запуска и остановки микроконтроллера МК;
- работы ГПСЧ по формированию Z_1–Z_6;
- построчной выдачи псевдослучайных значений диагональных коэффициентов ПОСМ;
- работы управляющей линии «*S, R*» при окончании формирования набора псевдослучайных чисел Z_1–Z_6 и поступлении запроса на их перезапись в ГФПТ;
- работы ГФПТ при формировании ансамбля псевдослучайных ортогональных последовательностей $S_1(t)$, $S_2(t)$, $S_3(t)$ и останове генератора.

Результаты моделирования процесса формирования псевдослучайных ортогональных последовательностей и оценка их количества

Для примера рассмотрим генерацию ортогональных последовательностей рассматриваемым ГПСОП. Предположим, что с помощью ГПСЧ данного генератора была сформирована положительно определенная симметрическая матрица A 3-го порядка (n=3).

$$A = \begin{bmatrix} 4 & 2 & 2 \\ 2 & 5 & 1 \\ 2 & 1 & 6 \end{bmatrix}. \qquad (8)$$

В результате выполнения описанных выше процедур в ГПСОП на его выходе будет сформирована система дискретных базисных функций $S_1(t)$, $S_2(t)$, $S_3(t)$, представляющих собой ансамбль псевдослучайных ортогональных последовательностей:

$$\begin{pmatrix} S_1(t) = (0,8077;\ 0,7720;\ 1) \\ S_2(t) = (0,2170;\ 1;\ -0,9473) \\ S_3(t) = (1;\ -0,5673;\ -0,3698) \end{pmatrix}. \qquad (9)$$

В ортогональности функций $S_1(t)$, $S_2(t)$, $S_3(t)$ легко убедиться посредством умножения одной из них на любую из двух других.

На рис. 4 представлена временная реализация ансамбля псевдослучайных ортогональных последовательностей (ПСОП) вида (9), формируемая на выходе предложенного ГПСОП, для случая использования в качестве исходных данных диагональной симметрической матрицы (8).

Разработанный генератор псевдослучайных ортогональных последовательностей может иметь широкую область применения, заключающуюся в генерировании ансамблей псевдослучайных ортогональных последовательностей, число которых может быть отлично от 2^m (m – натуральное число), имеющих широкий набор значений периодов генерируемых функций и большое число значений ортогональных базисных функций за счёт автоматизации процесса присвоения псевдослучайных значений диагональных коэффициентов симметрической матрицы A вида (1).

Нелинейность формируемых структур ортогональных последовательностей достигается за счет того, что на каждом такте его работы ансамбль псевдослучайных ортогональных последовательностей, представляемый собственны-

ми векторами диагональной ПОСМ, формируется путем псевдослучайного задания набора её диагональных коэффициентов с помощью ГПСЧ.

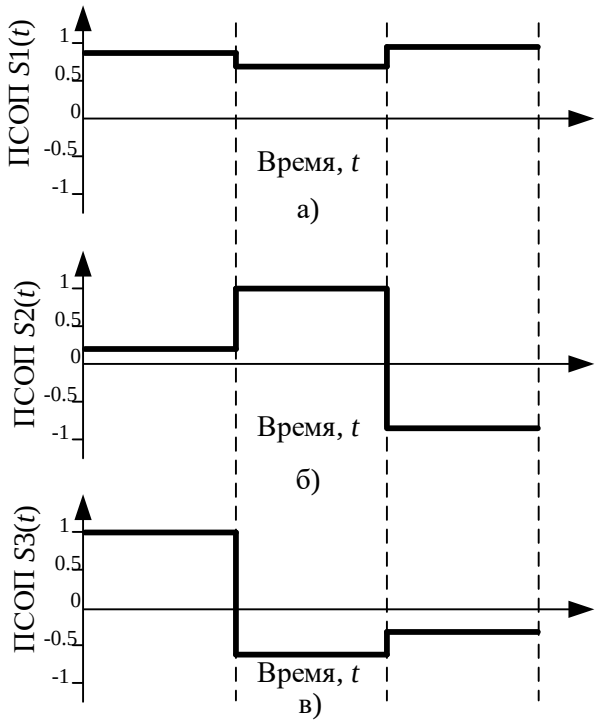

Рис. 4. Структура формируемого ансамбля псевдослучайных ортогональных последовательностей

Для оценки количества структур ансамблей псевдослучайных дискретных ортогональных последовательностей воспользуемся подходом, предложенным в [24].

Для расчета количества структур сигналов $M_{\text{ПСП}}$, которое можно получить с помощью разработанного алгоритма и генератора, использовалось выражение для неупорядоченных сочетаний с повторением элементов [24]:

$$M_{\text{ПСП}} = C_p^r = \left(\frac{(p+r-1)!}{r! \cdot (p-1)!} \right); \; r = \frac{n^2 - n}{2}. \qquad (10)$$

где: p – диапазон возможных значений диагональных коэффициентов матрицы A (например p=5); r – количество элементов диагональной симметрической матрицы A порядка n, находящихся ниже или выше главной диагонали.

В результате расчетов с учетом, что диапазон возможных значений диагональных коэффициентов матрицы A выбран равный p=5, для различных порядков матриц n в соответствии с (10) были получены значения количества возможных структур $M_{\text{ПСП}}$ ансамблей ортогональных последовательностей, представленные в таблице 2.

Аналогичным образом было определено количество возможных структур ортогональных последовательностей для ортогональных последовательностей, полученных на основе наиболее известного алгоритма де Брейна, которое представлено в [21, 32]. Анализ таблицы 2 и [21, 32] показывает, что даже при диапазоне возможных значений диагональных коэффициентов положительно

определенной симметрической матрицы A равном p=5 с ростом её порядка существенно возрастает количество возможных структур ортогональных последовательностей, формируемых предложенным генератором.

Таблица 2 – Количество возможных структур ортогональных последовательностей для различных размерностей симметрических матриц

Порядок диагональной симметрической матрицы, n	Количество возможных структур ортогональных последовательностей, $M_{ПСП}$
3	$6{,}3\cdot10^{2}$
4	$4{,}0\cdot10^{3}$
8	$4{,}19\cdot10^{5}$
16	$1{,}4\cdot10^{8}$
32	$8{,}0\cdot10^{10}$
64	$4{,}4\cdot10^{13}$
128	$8{,}8\cdot10^{16}$
256	$2{,}5\cdot10^{20}$

Сравнение количества возможных структур ортогональных последовательностей, формируемых предложенным генератором псевдослучайных ортогональных последовательностей с количеством подобных последовательностей, формируемых на основе наиболее известного алгоритма де Брейна, показывает преимущество первого над вторым от 1,5 до более 6 раз, при различных размерностях последовательностей.

Выводы

Представленный генератор ансамблей псевдослучайных ортогональных последовательностей позволяет автоматически формировать на выходах ансамбли псевдослучайных ортогональных последовательностей, получаемых на основе метода векторного синтеза и определяемых системой собственных векторов $x_i^{(j)}$ квадратной матрицы A'. Элементом новизны является структура блока псевдослучайного формирования коэффициентов симметрической матрицы, состоящая из микроконтроллера, генератора псевдослучайных чисел, блока накопителя, блока N – разрядного оперативного запоминающего устройства, совмещенная с известным генератором функций Попенко-Турко.

Разработан алгоритм формирования ансамблей псевдослучайных ортогональных последовательностей, состоящий из одиннадцати этапов и реализующий следующие процедуры: ввод исходных данных и определение начальных значений переменных; запуск в работу микроконтроллера МК и ГПСЧ; формирование первого псевдослучайного числа Z_1 из последовательности k псевдослучайных чисел; запись сформированного псевдослучайного числа в буферный накопитель; формирование треугольной матрицы A; формирование серии из k псевдослучайных чисел Z_{m-k+1}, Z_{m-k+2},…, Z_m, для построения треугольной матрицы A в буферном накопителе БН; формирование в ОЗУ квадратной матрицы A' на основе треугольной матрицы A; формирования сигнала S=1, выдаваемого по линии «S, R», свидетельствующего о возможности выдать заполненную псевдослучайными числами матрицу A' в качестве исходных данных гене-

ратору функций Попенко-Турко; формирование генератором функций Попенко-Турко сигнала запроса R=1, выдаваемого по линии «S, R» в ОЗУ; построчная перезапись положительно определенной симметрической матрицы с псевдослучайными диагональными коэффициентами A' в генератор функций Попенко-Турко; генерация ансамбля псевдослучайных ортогональных последовательностей, состоящего из набора последовательностей $S_1(t)$, $S_2(t)$, …, $S_n(t)$; осуществление следующего цикла работы ГПСОП по команде «Старт», поступающей с генератора функций Попенко-Турко или останов генератора по команде «Стоп», поступающей от микропроцессора МК. Элементами новизны в представленном алгоритме являются реализация процедур генерации псевдослучайных чисел, запись их в буферный накопитель, формирование треугольной матрицы A путем присвоения диагональным коэффициентам значений псевдослучайных чисел, построение квадратной матрицы A' на основе треугольной матрицы A.

Сравнение количества возможных структур ортогональных последовательностей, формируемых предложенным генератором псевдослучайных ортогональных последовательностей с количеством подобных последовательностей, формируемых на основе наиболее известного алгоритма де Брейна, показывает преимущество первого над вторым.

В дальнейшем планируется развитие представленной схемы генератора ансамблей псевдослучайных ортогональных последовательностей и алгоритма формирования ансамблей псевдослучайных ортогональных последовательностей с учетом возможности использования не только положительных, но и отрицательных псевдослучайных чисел, а также дополнение структуры предложенного генератора дополнительным запоминающим устройством и устройством сравнения, для выявления случаев повторений формируемых ансамблей псевдослучайных ортогональных последовательностей, с целью исключения повторяемых последовательностей.

Работа финансировалось Российским фондом фундаментальных исследований в ходе выполнения исследовательского проекта № 18-07-01020.

Литература

1. Борисов В. И., Зинчук В. М. Помехозащищённость систем радиосвязи. Вероятностно-временной подход. – М.: РадиоСофт, 2008. – 260 с.

2. Борисов В. И., Зинчук В. М., Лимарев А. Е., Мухин Н П., Нахмансон Г. С. Помехозащищённость систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / под общ. ред. В. И. Борисова. – М.: Радио и связь, 2003. – 640 с.

3. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

4. Урядников Ю. Ф., Аджемов С. С. Сверхширокополосная связь. Теория и применение. – М.: СОЛОН-Пресс, 2005. – 368 с.

5. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. – СПб.: Свое издательство, 2013. – 166 с.

6. Proakis J. Digital Communications. – N. Y.: McGraw-Hill, 2001. – 928 p.

7. Sklar B. Digital Communications. Fundamentals and Applications. – Upper Saddle River NJ, Prentice-Hall, 1988. – 1104 p.

8. Golomb S. Digital communications with space applications. – Upper Saddle River NJ, Prentice-Hall, 1964. – 210 p.

9. Петрович Н. Т., Размахнин М. К. Системы связи с шумоподобными сигналами. – М.: Советское радио, 1969. – 232 с.

10. Golomb S. W., Gong G. Signal design for good correlation for wireless communication, cryptography, and radar. – Cambridge: University press, 2005. – 438 p.

11. Viterbi A. J. CDMA: Principles of spread spectrum communication. Reading, – MA: Addison-Wesley, 1995. – 245 p.

12. Ziemer R. E., Peterson R. L., Borth D. E. Introduction to spread spectrum communications. – Englewood Cliffs, NJ: Prentice Hall, 1995. – 695 p.

13. Nunn C. J., Coxson G. E. Polyphase pulse compression codes with optimal peak and integrated sidelobes // IEEE Transactions on Aerospace and Electronic Systems. 2009. Vol. AES-45, № 2. P. 775-781.

14. Rushanan J. Weil sequences: a family of binary sequences with good correlation properties // IEEE International Symposium on Information Theory, Seattle, WA, July 9–14, 2006 / Seattle convention center. Seattle, WA, USA, 2006. P. 1648-1652.

15. Дядюнов Н. Г., Сенин А. И. Ортогональные и квазиортогональные сигналы. – М.: Связь, 1977. – 224 с.

16. Dixon R. Spread spectrum systems. – New York NY, Wiley, 1976. – 318 p.

17. Ипатов В. П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. – М.: Радио и связь, 1992. – 152 с.

18. Варакин Л. Е. Теория сложных сигналов. – М.: Советское радио, 1978. – 199 с.

19. Литюк В. И., Литюк Л. В. Методы цифровой многопроцессорной обработки ансамблей радиосигналов. – М.: Солон-Пресс, 2007. – 592 с.

20. Жук А. П., Черняк З. В., Сазонов В. В. О целесообразности использования ансамблей ортогональных сигналов с изменяющейся размерностью в системе CDMA // Известия ЮФУ. Технические науки. 2008. № 8 (85). С. 190-195.

21. Жук А. П., Петренко В. И., Кузьминов Ю. В., Жук Е. П., Луганская Л. А. Совершенствование способов обмена информацией в высокоскоростных беспроводных информационных сетях с использованием новых типов ансамблей дискретных последовательностей // Современные проблемы науки и образования. 2013. № 5. С. 144.

22. Попенко В. С. Оценка ширины спектра дискретных сигналов // Радиотехника. 1996. № 11. С. 57-59.

23. Попенко В. С. Векторный синтез ансамблей ортогональных сигналов. Часть 2. – Ставрополь: МО РФ, 1993. – 131 с.

24. Жук А. П., Бурмистров В. А., Гавришев А. А. Система передачи информации с использованием стохастических ортогональных ансамблей дискретных многоуровневых сигналов // Современные информационные технологии и ИТ-образование. 2015. Т. 2. № 11. С. 493-498.

25. Жук А. П., Жук Е. П., Трошков А. М. Способ передачи информации с псевдослучайной перестройкой формы сигналов для систем связи с кодовым разделением каналов // Информационная безопасность-2012: материалы XII Международной научно-практической конференции. Ч. 1. – Таганрог: ТТИ ЮФУ. 2012. – С. 346.

26. Гавришев А. А., Луганская Л. А., Лысенко А. А., Бурмистров В. А., Орел Д. В., Осипов Д. Л., Петренко В. И., Жук А. П. Генератор стохастических ортогональных кодов // Патент на изобретение RU 2615322 C1, опубл. 04.04.2017, бюл. № 10. – URL: http://elibrary.ru/item.asp?id=38261914 (дата обращения 27.06.2020).

27. Косякин С. И., Москвитин И. А., Смирнов А. А. Способ передачи информации в системах с кодовым разделением каналов и устройство для его осуществления // Патент на изобретение RU 2234191 C2, опубл. 10.08.2004. – URL: http://elibrary.ru/item.asp?id=37941753 (дата обращения 28.06.2020).

28. Попенко В. С., Турко С. А. Генератор функций Попенко-Турко // Патент на изобретение SU 1753464 A1, опубл. 06.03.1990. – URL: http://elibrary.ru/ item.asp?id=23014440 (дата обращения 27.06.2020).

29. Вержбицкий В. М. Численные методы (линейная алгебра и нелинейные уравнения): учебное пособие для вузов. – М.: Издательский дом ОНИКС 21 век, 2005. – 432 с.

30. Головина Л. И. Линейная алгебра и некоторые ее приложения. – М.: Наука, 1971. – 340 с.

31. Демидович Б. П., Марон И. А. Основы вычислительной математики. – М.: Наука, 1970. – 664 с.

32. Жук А. П., Иванов А. С. Повышение структурной скрытности системы передачи информации с кодовым разделением каналов // Наукоемкие технологии в космических исследованиях Земли. 2011. № 1. С. 26-28.

References

1. Borisov V. I., Zinchuk V. M. *Pomekhozashchishchennost' sistem radiosviazi. Veroiatnostno-vremennoi podkhod* [Interference protection of radio communication systems. Time-and-probability approach]. Moscow, RadioSoft Publ., 2008. 260 p. (in Russian).

2. Borisov V. I., Zinchuk V. M., Limarev A. E., Muhin N. P., Nahmanson G. S. *Pomekhozashchishchennost' sistem radiosviazi s rasshireniem spektra signalov moduliatsiei nesushchei psevdosluchainoi posledovatel'nost'iu* [Interference protection of radio communication systems with expansion of signals spectrum by modulation of the carrier with pseudorandom sequence]. Moscow, Radio i sviaz' Publ., 2003. 640 p. (in Russian).

3. Varakin L. E. *Sistemy sviazi s shumopodobnymi signalami* [Communication systems with noise-like signals]. Moscow, Radio i sviaz' Publ., 1985. 384 p. (in Russian).

4. Uriadnikov Y. F. Adzhemov S. S. *Sverkhshirokopolosnaia sviaz'. Teoriia i primenenie* [Ultra-wide-band communication. Theory and application]. Moscow, Solon-Press Publ., 2005. 368 p. (in Russian).

5. Makarenko S. I., Ivanov M. S., Popov S. A. *Pomekhozashchishchennost' sistem svyazi s psevdosluchajnoj perestrojkoj rabochej chastoty* [Noise immunity of communication systems with pseudorandom tuning of the operating frequency]. Saint-Petersburg, Svoe izdatel'stvo Publ., 2013. 166 p. (in Russian).

6. Proakis J. *Digital Communications*. New York NY, McGraw-Hill, 2001. 928 p.

7. Sklar B. *Digital Communications: Fundamentals and Applications*. Upper Saddle River NJ, Prentice-Hall, 1988. 1104 p.

8. Golomb S. *Digital communications with space applications*. Upper Saddle River NJ, Prentice-Hall, 1964. 210 p.

9. Petrovich N. T., Razmakhnin M. K. *Sistemy sviazi s shumopodobnymi signalami* [Communication systems with noise-like signals]. Moscow, Sovetskoe radio Publ., 1969. 232 p. (in Russian).

10. Golomb S. W., Gong G. *Signal design for good correlation for wireless communication, cryptography, and radar*. Cambridge: University press, 2005. 438 p.

11. Viterbi A. J. *CDMA: Principles of spread spectrum communication.* Reading, MA, Addison-Wesley, 1995. 245 p.

12. Ziemer R. E., Peterson R. L., Borth D. E. *Introduction to spread spectrum communications.* Englewood Cliffs, NJ, Prentice Hall, 1995. 695 p.

13. Nunn C. J., Coxson G. E. Polyphase pulse compression codes with optimal peak and integrated sidelobes. *IEEE Transactions on Aerospace and Electronic Systems.* 2009, vol. 45, no. 2, pp. 775–781.

14. Rushanan J. Weil sequences: a family of binary sequences with good correlation properties. *IEEE International Symposium on Information Theory, Seattle, WA, July 9–14, 2006, Seattle convention center*. Seattle, WA, USA, 2006. pp. 1648–1652.

15. Diadiunov N. G., Senin A. I. *Ortogonal'nye i kvaziortogonal'nye signaly* [Orthogonal and quasi-orthogonal signals]. Moscow, Sviaz' Publ., 1977. 224 p. (in Russian).

16. Dixon R. *Spread spectrum systems*. New York NY, Wiley, 1976. 318 p.

17. Ipatov V. P. *Periodicheskie diskretnye signaly s optimal'nymi korreliatsionnymi svoistvami* [Periodic discrete signals with optimal correlation properties]. Moscow, Radio i sviaz' Publ., 1992. 152 p. (in Russian).

18. Varakin L. E. *Teoriia slozhnykh signalov* [Theory of complex signals]. Moscow, Sovetskoe radio Publ., 1978. 199 p. (in Russian).

19. Lityuk V. I., Lityuk L. V. *Metody cifrovoj mnogoprocessornoj obrabotki ansamblej radiosignalov* [Methods of digital multiprocessor processing of radio signal ensembles]. Moscow, Solon-Press, 2007. 592 p. (in Russian).

20. Zhuk A. P., Cherniak Z. V., Sazonov V. V. *O tselesoobraznosti ispol'zovaniia ansamblei ortogonal'nykh signalov s izmeniaiushcheisia razmernost'iu v sisteme CDMA* [On the feasibility of using ensembles of orthogonal signals with varying dimensions in the CDMA system]. *Izvestiya SFedU. Engineering Sciences.*

Tematicheskii vypusk. Informatsionnaia bezopasnost', 2008, vol. 85, no. 8, pp. 190-195 (in Russian).

21. Zhuk A. P., Petrenko V. I., Kuz'minov Iu. V., Zhuk E. P., Luganskaia L. A. *Sovershenstvovanie sposobov obmena informatsiei v vysokoskorostnykh besprovodnykh informatsionnykh setiakh s ispol'zovaniem novykh tipov ansamblei diskretnykh posledovatel'nostei* [Improving information exchange methods in high-speed wireless information networks using new types of discrete sequence ensembles]. *Modern problems of science and education*, 2013, no. 5. (in Russian).

22. Popenko V. S. *Otsenka shiriny spektra diskretnykh signalov* [Estimation of the discrete signal's spectrum width]. *Radiotekhnika*, 1996, no. 11, pp. 57-59 (in Russian).

23. Popenko V. S. *Vektornyi sintez ansamblei ortogonal'nykh signalov. Chast' 2* [Vector synthesis of orthogonal signal ensembles. Part 2]. Stavropol, Stavropol Higher Military Engineering College of Communications, 1993. 131 p. (in Russian).

24. Zhuk A. P., Burmistrov V. A., Gavrishev A. A. *Sistema peredachi informatsii s ispol'zovaniem stokhasticheskikh ortogonal'nykh ansamblei diskretnykh mnogourovnevykh signalov* [Information transfer system using stochastic orthogonal ensembles of discrete multilevel signals]. *Modern Information Technology and IT-education*, 2015, vol. 2, no. 11, pp. 493-498 (in Russian).

25. Zhuk A. P., Zhuk E. P., Troshkov A. M. *Sposob peredachi informatsii s psevdosluchainoi perestroikoi formy signalov dlia sistem sviazi s kodovym razdeleniem kanalov* [A method for transmitting information with pseudorandom rearrangement of the signal form for communication systems with code-division multiple access]. *Informatsionnaia bezopasnost'-2012: materialy XII Mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Information security-2012: materials of the XII International scientific and practical Conference]. Taganrog, Southern Federal University, 2012, p. 346 (in Russian).

26. Gavrishev A. A., Luganskaia L. A., Lysenko A. A., Burmistrov V. A., Orel D. V., Osipov D. L., Petrenko V. I., Zhuk A. P. *Generator stokhasticheskikh ortogonal'nykh kodov* [Stochastic Orthogonal Codes Generator]. Patent Russia, no. RU2615322C1, 2017.

27. Kosjakin S. I., Moskvitin I. A., Smirnov A. A. *Sposob peredachi informacii v sistemah s kodovym razdeleniem kanalov i ustrojstvo dlja ego osushhestvlenija* [Method of transmitting information in systems with code division of channels and the device for its implementation]. Patent Russia, no. 2234191. 2004.

28. Popenko V. S., Turko S. A. *Generator funktsii Popenko-Turko* [Popenko-Turko function generator]. Patent Russia, no. SU 1753464A1, 1992.

29. Verzhbitskii V. M. *Chislennye metody (lineinaia algebra i nelineinye uravneniia)* [Numerical methods (linear algebra and nonlinear equations)]. Moscow, Izdatel'skii dom ONIKS 21 vek Publ., 2005. 432 p. (in Russian).

30. Golovina L. I. *Lineinaia algebra i nekotorye ee prilozheniia* [Linear algebra and some of its applications]. Moscow, Nauka Publ., 1971. 340 p. (in Russian).

31. Demidovich B. P., Maron I. A. *Osnovy vychislitel'noi matematiki* [Fundamentals of computational mathematics]. Moscow, Nauka Publ., 1970. 664 p. (in Russian).

32. Zhuk A.P., Ivanov A.S. *Povyshenie strukturnoi skrytnosti sistemy peredachi informatsii s kodovym razdeleniem kanalov* [Increasing the structural secrecy of the information transmission system with code division of channels]. *H&ES Research,* 2011, no. 1, pp. 26-28 (in Russian).

Статья поступила 13 июня 2020 г.

Информация об авторах

Жук Александр Павлович – кандидат технических наук, профессор. Профессор кафедры организации и технологии защиты информации. ФГАОУ ВО «Северо-Кавказский федеральный университет». Область научных интересов: развитие теории и методов защиты информации в беспроводных телекоммуникационных системах; теория и практика применения биометрических методов идентификации пользователей инфокоммуникационных систем. E-mail: alekszhuk@mail.ru

Студеникин Андрей Владимирович – соискатель ученой степени кандидата технических наук. Аспирант кафедры организации и технологии защиты информации. ФГАОУ ВО «Северо-Кавказский федеральный университет». Область научных интересов: разработка методов защиты информации в беспроводных телекоммуникационных системах. E-mail: studentstavropol@mail.ru

Жук Елена Павловна – кандидат педагогических наук, доцент. Доцент кафедры организации и технологии защиты информации. ФГАОУ ВО «Северо-Кавказский федеральный университет». Область научных интересов: теория и практика применения биометрических методов идентификации пользователей инфокоммуникационных систем; разработка методов защиты информации в беспроводных телекоммуникационных системах. E-mail: zhuk1966@yandex.ru

Адрес: 355017, Россия, г. Ставрополь, ул. Пушкина, д. 1.

Algorithm and device for forming ensembles of pseudorandom orthogonal sequences in information transfer systems with code-division multiple access

A. P. Zhuk, A. V. Studenikin, E. P. Zhuk

Formulation of the task. *Improving the structural secrecy of information transfer systems with code-division multiple access highlights the task of constructing devices for the formation of a representative number of ensembles of orthogonal sequences for its subsequent use in a pseudorandom manner. Known technical solutions in this field and algorithms for their functioning are limited by a negligible quantity of formed ensembles of orthogonal sequences, narrow possibilities for changing the dimension of generated ensembles, low accuracy of formation and the lack of automatic generation by a pseudorandom algorithm.* ***The purpose of this article*** *is to increase the number of ensembles of orthogonal sequences by implementing a new algorithm for their formation. It is proposed to automate the process of assigning pseudorandom input data to the diagonal coefficients of the symmetric matrix in the Popenko-Turko function generator by introducing a block of pseudorandom formation of the coefficients of the symmetric matrix. This will provide au-*

tomatic generation of ensembles of pseudorandom orthogonal sequences at the outputs of the generator. ***Methods.*** *The solution of the task is based on the use of the vector synthesis method for ensembles of orthogonal sequences, considering restrictions on the numerical range of pseudorandom input data. As the main indicator of the developed generator, the maximum number of generated structures of ensembles of pseudorandom orthogonal sequences is used.* ***Novelty.*** *Novelty elements consist in obtaining a new algorithm for the formation of ensembles of pseudorandom orthogonal sequences based on the use of the vector synthesis method and the circuit implementation of the generator of ensembles of pseudorandom orthogonal sequences.* ***Results.*** *Using the developed generator and algorithm for forming ensembles of pseudorandom orthogonal sequences allows to form an increased number of ensembles of pseudorandom orthogonal sequences which is necessary for increasing the structural secrecy of information transfer systems with code-division multiple access. The presented implementation of the generator of ensembles of pseudorandom orthogonal sequences and the proposed algorithm for the formation of ensembles of pseudorandom orthogonal sequences provides an increase in the number of generated structures of orthogonal sequences in information transfer systems, and as a result, an increase of the system's structural secrecy. The number of possible structures of orthogonal sequences formed on the basis of the developed algorithm, shows the advantage by 1.5 to 6 times for different dimensions of ensembles of orthogonal sequences in comparison with the number of sequences of the considered class formed on the basis of the more popular De Bruijin algorithm.* ***Practical relevance.*** *The developed generator of ensembles of pseudorandom orthogonal sequences, if used as a component of an information transfer system with code-division multiple access, will increase the time during which the sequence structures used for information exchange will not be repeated because of increasing their quantity. The use of an increased number of ensembles of pseudorandom orthogonal sequences to implement information exchange in information transfer systems with code-division multiple access will increase system's structural secrecy.*

Key words: *information transfer system with code-division multiple access, pseudorandom orthogonal sequence generator, structural secrecy, eigenvector, symmetric matrix.*

Information about Authors

Aleksandr Pavlovich Zhuk – Ph.D. of Engineering Sciences, Professor. Professor at the Department of Organization and Technology of Information Security. Federal State Autonomous Educational Institution of Higher Education «North-Caucasus Federal University». Field of research: development of the theory and methods of information security in wireless telecommunications systems; theory and practice of biometric methods of user identification in information communication systems. E-mail: alekszhuk@mail.ru

Andrei Vladimirovich Studenikin – Doctoral Student. The postgraduate student at the Department of Organization and Technology of Information Security. Federal State Autonomous Educational Institution of Higher Education «North-Caucasus Federal University». Field of research: development of information security methods in wireless telecommunications systems. E-mail: studentstavropol@mail.ru

Elena Pavlovna Zhuk – Ph.D. of Pedagogic Sciences, Associate Professor. Associate Professor at the Department of organization and technology of information security. Federal State Autonomous Educational Institution of Higher Education «North-Caucasus Federal University». Field of research: theory and practice of biometric methods of user identification in information communication systems; development of information security methods in wireless telecommunications systems. E-mail: zhuk1966@yandex.ru

Address: Russia, 355009, Stavropol, Pushkin str. 1.