Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

На правах рукописи

Студеникин Андрей Владимирович

МЕТОД ПРОТИВОДЕЙСТВИЯ УГРОЗЕ ПОДМЕНЫ СООБЩЕНИЙ ДЛЯ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ НА ОСНОВЕ СТОХАСТИЧЕСКОГО ПРИМЕНЕНИЯ АНСАМБЛЕЙ МНОГОФАЗНЫХ ОРТОГОНАЛЬНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Специальность 2.3.6 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
кандидат технических наук, профессор
Жук Александр Павлович

Ставрополь – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Вариантом современного способа информационного обмена является технология многостанционного доступа с кодовым разделением каналов (КРК) (Code Division Multiple Access – CDMA), которая использует канальные сигналы уникальной кодовой структуры, обеспечивающих их передачу одновременно в общей полосе частот, а также эффективное разделение в приемнике. Анализ работ [1-5] показывает, что методы доступа к спектру с несколькими несущими, включая мультиплексирование с ортогональным частотным разделением (OFDM) и множественный доступ с кодовым разделением с несколькими несущими (MC-CDMA), предлагают ряд существенных преимуществ по сравнению с системами с одной несущей в изменчивых средах беспроводных каналов. Технология OFDM по своей сути более устойчива к вредным явлениям межсимвольной интерференции и многолучевого замирания [5]. Кроме того, технология OFDM более эффективно использует отведенный частотный диапазон благодаря плотно расположенным несущим.

Использование технологии MC-CDMA обеспечивает следующие преимущества [6-17]:

– высокую помехозащищенность систем связи;

– эффективную борьбу с искажениями сигналов в канале связи;

– одновременную работу многих абонентов в общей полосе частот за счет кодового разделения каналов;

– более эффективное использование спектра частот на ограниченной территории.

Дополнительным отличием данной технологии передачи информации от других является возможность обеспечения конфиденциальности при обмене информацией между пользователями [18-20].

Известно, что конфиденциальность передачи информации по беспроводным линиям связи может быть обеспечена за счет энергетической и структурной скрытности используемых в системе передачи информации переносчиков информации, а также информационной скрытности передаваемого сообщения [6].

По этим причинам технология OFDM была принята в качестве схемы передачи для ряда современных стандартов беспроводной связи, включая IEEE 802.16 [21] и наземное цифровое видеовещание (DVB-T). OFDM также используется для стандарта IEEE 802.22 когнитивных радиоприемников с динамическим доступом к спектру [1].

Множественный доступ с кодовым разделением с несколькими несущими MC-CDMA является еще одним возможным вариантом для перспективных систем связи с несколькими несущими [2–5, 22] используя гибкость и потенциал, предлагаемые комбинацией OFDM и CDMA.

Системы спутниковой связи (ССС) являются разновидностью беспроводных систем передачи информации, предназначенных для глобального информационного взаимодействия между собой, в которых передача информации осуществляется через искусственные спутники Земли, находящихся на различных орбитах. Системы спутниковой связи играют важнейшую роль в жизни и деятельности людей, поскольку обеспечивают связью, в том числе в тех случаях, когда другие телекоммуникационные системы в силу географической удаленности или сложных метеорологических условий, а также по причине малонаселенности являются недоступными. В настоящее время распространение приобретают многоспутниковые низкоорбитальные ССС, способные обеспечить обменом данными пользователей на всей поверхности Земли, а также организовывать высокоскоростной информационный обмен с низкой задержкой по времени, что является новой концепцией доступа пользователей к ресурсам в сети Интернет. Например, ССС Starlink уже в настоящее время предоставляет доступ к сети Интернет в тех местах Земли, где он был неустойчивым или недоступным.

Анализ показал, что среди многообразия видов множественного доступа в системах спутниковой связи (FDMA (Frequency Division Multiple Access), TDMA

(Time Division Multiple Access), CDMA), доступ с кодовым разделением каналов и прямым расширением спектра CDMA-DS является достаточно распространенным [23-25].

Поскольку система спутниковой связи является беспроводной, то в силу специфики её функционирования существующую угрозу подмены сообщений, передаваемых в ней, можно отнести к угрозе, реализуемой злоумышленниками с высокой степенью вероятности в силу простоты реализации таких угроз и отсутствием необходимости выделения существенных материальных затрат на их реализацию [22-31].

Известно, что большинство коммерческих спутниковых систем спроектированы и используются без защиты данных от угрозы подмены сообщений [27, 32]. Поэтому решение задачи повышения защищённости информационного обмена от указанного вида угроз в системах спутниковой связи имеет важное значение.

Как отмечается в работах Каневского З.М., Сухарева Е.М., Осмоловского С.А., Кандаурова Н.А., Стасева Ю.В, Горбенко И.Д., Макаренко Б.И. и др. в ССС для передачи информации возможно применение кодовых последовательностей, имеющих изменяющуюся структуру для обеспечения их требуемой структурной скрытности. При наличии приемлемого количества ансамблей ортогональных кодовых последовательностей и алгоритма их стохастического применения по мнению упомянутых выше авторов возможно обеспечить защиту информации в системе беспроводной связи с кодовым разделением каналов от угрозы подмены сообщений.

В работе [33] была высказана идея динамической передачи сигналов для решения задачи безопасности информации в системах спутниковой связи, при которой соответствие «информационный символ – сигнал-переносчик» изменяется во времени по псевдослучайному закону. В работе [34] доказано, что режим динамической передачи сигналов позволяет на физическом уровне решить проблему защиты от несанкционированного доступа к информационному тракту, а также обеспечивает повышение информационной скрытности передаваемых

сообщений. Однако вопросы синтеза ансамблей последовательностей для динамического формирования сигналов-переносчиков и практического их применения в процессе передачи информации не рассматривались.

Наибольшую сложность при комплексном решении задачи обеспечения конфиденциальности информации в системах спутниковой связи с кодовым разделением каналов, из всех видов скрытности представляет задача обеспечения структурной скрытности используемых в системе передачи информации сигналов-переносчиков информации. Это связано с тем, что они должны обеспечивать условие ортогональности, а также к ним предъявляются требования по спектральным и корреляционным свойствам. Важно отметить, что количество известных ортогональных кодовых последовательностей требуемой размерности, удовлетворяющих данным требованиям, невелико, поэтому их структура легко обнаруживается после нескольких начальных этапов информационного обмена. Так, например, структурная сложность $M-$последовательностей может быть раскрыта через 2^n символов (где $n-$ число разрядов сдвигового регистра с линейными обратными связями, генерирующего $M-$последовательности длиной 2^n-1 символов) [6]. В работах [11-13] представлены алгоритмы и методы получения ортогональных и квазиортогональных кодовых последовательностей, на основе которых может быть синтезировано количество их структур, превышающее количество кодовых последовательностей, получаемых известными методами. Однако вопросы их формирования не рассматривались. В работах [16, 34, 117, 118] представлены способы информационного обмена на основе применения ансамблей ортогональных и квазиортогональных кодовых последовательностей, тем не менее, вопросы их синтеза детально не рассмотрены.

Учитывая, что в системах спутниковой связи с кодовым разделением каналов при организации трактов передачи и приема наряду с другими используется квадратурная фазовая манипуляция QPSK (Quadrature phase shift keying) и различные виды квадратурной амплитудной модуляции QAM (Quadrature Amplitude Modulation), то по мнению автора в качестве сменяемых последовательностей для достижения требуемого показателя их структурной

скрытности целесообразно использовать ансамбли многофазных ортогональных кодовых последовательностей, поскольку их количество существенно больше, чем количество двоичных ортогональных кодовых последовательностей. Разница в количестве последовательностей и структурной скрытности при их применении достигается тем, что при рассмотрении ансамблей многофазных ортогональных кодовых последовательностей каждый её элемент может иметь более, чем два значения фазы 0° и 180°, которые имеются у двоичных ортогональных кодовых последовательностей.

Поскольку ССС являются неотъемлемой частью глобальной телекоммуникационной инфраструктуры, обеспечивая широкий спектр услуг от телевизионного вещания до подключения к Интернету и глобального позиционирования, возникает логичный вопрос обеспечения информационной безопасности этих систем. Реализация угроз безопасности информации в ССС проводится посредством атак злоумышленника как на систему в целом, так и на ее сегменты, такие как наземный, космический, пользовательский сегменты и сегмент связи. Угроза подмены сообщений в ССС достаточно легко реализуема с использованием стандартного комплекта оборудования спутниковой связи с незначительной модификацией программного обеспечения.

С учетом сказанного можно заключить, что задача разработки метода противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения увеличенного количества ансамблей многофазных ортогональных кодовых последовательностей является **актуальной.**

Таким образом, для решения научной задачи необходимо разработать метод противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения АМФОКП, который должен содержать:

- модель противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП;

- модель АМФОКП и алгоритм их синтеза для стохастического применения в ССС с КРК, обеспечивающие требуемый уровень структурной скрытности;

- принцип и техническое решение по противодействию угрозе подмены сообщений в ССС с КРК.

Целью исследований является повышение защищенности систем спутниковой связи с кодовым разделением каналов по показателю структурной скрытности за счет стохастического применения ансамблей многофазных ортогональных кодовых последовательностей с изменяющейся структурой.

Объектом исследований является система спутниковой связи с кодовым разделением каналов.

Как отмечается в работах Каневского З.М., Сухарева Е.М., Осмоловского С.А., Кандаурова Н.А., Стасева Ю.В, Горбенко И.Д., Макаренко Б.И. и др. в ССС для передачи информации возможно применение кодовых последовательностей, имеющих изменяющуюся структуру для обеспечения структурной скрытности, которые эффективно могут противостоять угрозе подмены сообщений в них.

Для оценки показателя структурной скрытности сигналов S авторами работы Каневским З.М., Литвиненко В.П., Макаровым Г.В. предлагается использовать структурную скрытность, которая определяется мощностью A (числом элементов) множества X возможных сменных параметров сигнала, например, количество фаз, несущих частот, вариантов кодовой структуры. Автор в работе [35, 117] предлагает оценивать структурную скрытность, используя в качестве базовой единицы количество двоичных измерений (ДИЗ), требуемых для расшифровки структуры сигнала.

Оценка структурной скрытности кодовых последовательностей существующих ССС с КРК показала, что они не удовлетворяют требуемому значению $S_{\text{треб.}} \geq 43$ ДИЗ, а используемые в них ансамбли ортогональных кодовых последовательностей, которые определяют этот показатель, не удовлетворяют требованию по их количеству (вариантов кодовой структуры). Также установлено, что по причине применения ограниченного числа известных ансамблей ортогональных кодовых последовательностей, используемых в ССС с КРК, устройства их формирования имеют ограниченные возможности.

В работе Черноусова А.В. и др. [132] отмечено, что свойством ССС с КРК противостоять навязыванию ложного сообщения, его подмене или изменению хранимых данных является имитостойкость, которая является важным показателем защищенности рассматриваемых систем.

В работе Черноусова А.В. и др. [132] отмечено, свойством ССС с КРК противостоять навязыванию ложного сообщения, его подмене или изменению хранимых данных является имитостойкость, которая является важным показателем защищенности рассматриваемых систем.

В исследовании [133] продемонстрировано, что имитостойкость канала связи, обеспечиваемая на уровне сигнала $I_{\text{с}}$, определяется следующими параметрами:

– размерностью пространства сигналов G;

– количеством разрешенных к применению сигналов $G_{\text{р}}$ в заданном временном интервале Δt;

– числом попыток имитации n;

– выбранной стратегией имитации q.

Таким образом, уровень защищенности системы напрямую зависит от перечисленных характеристик и условий их использования.

$$I_{\text{с}} = f\left(G, G_{\text{р}}, n, q\right).$$

В этой же работе отмечено, что в случае многократных попыток навязывания имитостойкость радиоканала может оцениваться безопасным временем $T_{\text{б}}$, определяемым математическим ожиданием времени статистического опробования всевозможных вариантов навязывания противником сигнала с использованием всего пространства $\{Z\}$ сложных сигналов. Безопасное время подразумевает интервал в времени, в течение которого злоумышленник не может осуществить подмену или ввести ложное сообщение.

Также в данной работе был проведен анализ имитостойкости и безопасного времени ССС с КРК на основе модуляции ФМ-2 ШПС с постоянными и

переменными значениями параметрами F_b, F_c. Результат вычислений безопасного времени передачи широкополосного сигнала показывает, что безопасное время ССС с КРК имеют следующие значения [133]:

– Для ФМ-2 при длине ПСП 127, $T_б = 1{,}3 \cdot 10^{-3} = 1{,}3$ мс.

– Для ФМ-2 при длине ПСП 255, $T_б = 2{,}5 \cdot 10^{-3} = 2{,}5$ мс.

Для оценки достаточности времени безопасной работы в данной работе проведен расчет времени, необходимого для передачи пакета данных для SPOT-устройства, которое составляет $T_{\text{сообщ.}} = 15$ мс, что существенно меньше времени безопасной работы, обеспечиваемого существующей ССС с КРК Globalstar на основе модуляции ФМ-2 ШПС.

С учетом того, что имеющееся безопасное время ССС с КРК 1,3 мс и 2,5 мс для соответственно длин ПСП 127 и 255 значительно меньше требуемого $T_{\text{сообщ.}} = 15$ мс для передачи пакета данных для SPOT-устройства длиной 144 бит, то в работе сделан вывод о недостаточности этого показателя в рассматриваемых системах передачи информации.

Поскольку в существующих ССС с КРК чаще всего в качестве расширяющих последовательностей используются последовательности Уолша, то также можно сделать вывод о том, что показатель структурной скрытности последовательностей Уолша является неприемлемым на практике.

По этим причинам выявлено **противоречие в практике**, которое заключается в том, что используемые в настоящее время в ССС с КРК ортогональные кодовые последовательности не позволяют обеспечить требуемый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ, достаточный для противодействия угрозе подмены сообщений.

Для разрешения данного противоречия в работе проанализированы методы синтеза ансамблей ортогональных последовательностей, позволяющие реализовать их стохастическое применение в ССС с КРК, для обеспечения необходимого уровня их структурной скрытности:

1) Методы, основанные на автоматической смене известных структур ансамблей дискретных ортогональных сигналов (АДОС), таких как Уолша, Orthogonal Variable Spreading Factor (OVSF), Стиффлера, Рида-Мюллера, Джеффи, Велти, D-коды, Адамара, Радемахера, Хаара и др.

2) Методы повышения структурной скрытности, заключающиеся в использовании в качестве расширяющих последовательностей нелинейных псевдослучайных последовательностей (ПСП) [75], представленные в работах Сухарева Е.М. [52], Кислицина А.С., Калмыкова В.В., Дмитриева А.С., Панаса А.И. и других исследователей.

3) Методы повышения структурной скрытности, заключающиеся в использовании ансамблей ортогональных последовательностей, полученных на основе векторного синтеза, представленные в работах Попенко В.С., Турко С.А., Самуса М.В., Гайчука Д.В., Сазонова В.В., Трошкова А.М., Жука А.П. и других исследователей [7, 8, 11-13, 17, 68, 72, 73, 77, 79, 81, 82, 88, 87-92, 95].

4) Метод повышения структурной скрытности, основанный на использовании псевдослучайных хаотических последовательностей (ПСХП), представленный в работах Калмыкова В.В., Кислицына А.С., Сухарева Е.М.

5) Метод повышения структурной скрытности, основанный на использовании дискретных ортогональных многоуровневых сигналов (АДОМУС), предложенный в работе Черняка З.В. [57].

Проведенные исследования показали, что существующие подходы к синтезу ансамблей ортогональных кодовых последовательностей (АОКП), направленные на их стохастическое использование в системах ССС с КРК для повышения их структурной скрытности, не устраняют выявленное ранее противоречие. Это обусловлено тем, что объем синтезируемых известными методами АОКП недостаточен для достижения требуемого уровня их структурной скрытности $S_{\text{треб.}}$, который должен составлять не менее 43 ДИЗ.

На основании указанного выше в диссертационной работе выявлено **противоречие в теории**, которое заключается в том, что известные методы синтеза не позволяют получить АОКП в количестве, обеспечивающем требуемое значение

их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ при стохастическом применении в ССС с КРК.

Поскольку из всех известных подходов повышения защищенности ССС с КРК, наибольший эффект в повышении структурной скрытности может обеспечить стохастическое применение псевдослучайных ансамблей многофазных ортогональных кодовых последовательностей (АМФОКП), получаемых на основе векторного синтеза при рассмотрении собственных векторов эрмитовых матриц (ЭМ), данное направление выбрано в качестве основного для разрешения выявленных противоречий.

В этом случае возможно получение множества псевдослучайных АМФОКП, включающее достаточное количество их реализаций для стохастического применения, а также обладающих приемлемыми корреляционными и спектральными характеристиками.

Таким образом, в работе обоснована необходимость усовершенствования метода противодействия угрозе подмены сообщений на основе векторного синтеза увеличенного количества АМФОКП. В связи с этим, **предметом исследования** является метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов.

Из этого следует, что **научная задача исследования** заключается в разработке метода противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения АМФОКП.

Анализ возможных подходов к решению научной задачи показал целесообразность ее декомпозиции на **основные задачи исследования**:

1. Разработать модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП размерностей $N = 128, 256$.

2. Разработать модель и алгоритм синтеза АМФОКП размерностей $N = 128, 256$, в количестве, обеспечивающем при их стохастическом применении в ССС с КРК требуемый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ.

3. Разработать принцип построения и техническое решение стохастического средства защиты информации для ССС с КРК.

Методология и методы исследования работы составляют стохастические методы защиты информации, теории систем сигналов, теории вероятностей и математической статистики, математического моделирования, сравнение и эксперимент.

Положения, выносимые на защиту:

1. Разработанная модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП обеспечивает повышение структурной скрытности выше требуемого значения $S_{\text{треб.}} \geq 43$ ДИЗ, отличается от известных тем, что при передаче каждого информационного бита используется уникальная неповторяющаяся структура многофазной ортогональной кодовой последовательности синхронно изменяемая на приемной и передающей сторонах.

2. Разработанная модель АМФОКП требуемых размерностей $L = 128, 256$ и алгоритм их синтеза, по сравнению с известной моделью АДОМУС, позволяют увеличить выигрыш в структурной скрытности АМФОКП. Получаемые АМФОКП имеют прирост структурной скрытности по отношению к структурной скрытности АДОМУС, который лежит в пределах для порядка матрицы $n = 128$ от 2,5 до 101,31%, для $n = 256$ от 2,32 до 101,02%. Данный выигрыш обеспечивается при условии, что фаза каждого диагонального коэффициента ЭМ изменяется на угол $\Delta\varphi_i = 18^{\circ}$ и, соответственно $\Delta\varphi_i = 1^{\circ}$. Значение структурной скрытности АМФОКП для $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для L=128 и L=256, что позволяет их использовать в существующих ССС с КРК.

3. Полученные принцип построения и техническое решение генератора псевдослучайных АМФОКП для стохастического средства защиты информации ССС с КРК, в отличие от известных, обеспечивают генерацию ансамблей

многофазных ортогональных кодовых последовательностей, описываемых комплексными числами.

Научная новизна полученных результатов диссертационной работы состоит в том, что:

1. Разработанная модель противодействия угрозе подмены сообщений в ССС с КРК, отличающаяся от известных тем, что при передаче каждого информационного бита используется уникальная неповторяющаяся структура ансамбля многофазных ортогональных кодовых последовательностей синхронно изменяемых на приемной и передающей сторонах.

2. Модель АМФОКП требуемых размерностей $N = 128, 256$ и алгоритм их синтеза которые, в отличие от известных, основаны на рассмотрении множества эрмитовых матриц порядка $(n \times n)$, элементы которых являются комплексными числами и задают все возможные ортогональные базисы пространства C^n – комплексных чисел.

3. Принцип построения и техническое решение генератора псевдослучайных АМФОКП для стохастического средства защиты информации системы спутниковой связи с кодовым разделением каналов, позволяющие, в отличие от известных, генерировать псевдослучайные АМФОКП на основе собственных векторов эрмитовых матриц в соответствии с задаваемым набором псевдослучайных комплексных чисел.

Теоретическая значимость работы заключается в развитии стохастических методов защиты информации в ССС с КРК на основе повышения структурной скрытности за счет синтеза, генерации и стохастического применения АМФОКП, описываемых ортогональными базисами пространства комплексных чисел C^n, а также в получении аналитических зависимостей для расчета показателя структурной скрытности для случая стохастического применения АМФОКП, представляемых СВ ЭМ.

Практическая ценность работы состоит в следующем

- Разработанные технические решения по повышению защищённости информации, защищённые патентами на изобретения и свидетельствами на

регистрацию программ для ЭВМ, реализующие предложенные алгоритмы, обеспечивают реализацию модели и алгоритма противодействия угрозе подмены передаваемых в ССС с КРК сообщений на основе формирования и стохастического применения АМФОКП. В случае использования разработанного алгоритма противодействия угрозе подмены сообщений за счет стохастического применения неповторяющихся псевдослучайных АМФОКП происходит преобразование исходной информации и её передача в канал связи с помощью изменяющихся стохастическим образом ансамблей ортогональных кодовых последовательностей для передачи каждого информационного символа, что обеспечивает повышение их структурной скрытности. Получаемые АМФОКП имеют прирост структурной скрытности по отношению к структурной скрытности АДОМУС, который лежит в пределах для порядка матрицы $n = 128$ от 2,5 до 101,31%, для $n = 256$ от 2,32 до 101,02%. Данный выигрыш обеспечивается при условии, что фаза каждого диагонального коэффициента ЭМ изменяется на угол $\Delta\varphi_i = 18^{\circ}$ и, соответственно $\Delta\varphi_i = 1^{\circ}$. Значение структурной скрытности АМФОКП для $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для L=128 и L=256, что позволяет их использовать в существующих ССС с КРК.

- Структура и алгоритм функционирования генератора псевдослучайных АМФОКП, защищённые патентами на изобретения и свидетельствами на регистрацию программ для ЭВМ, позволяют формировать АМФОКП с изменяющейся структурой на основе СВ ЭМ в соответствии с набором псевдослучайных комплексных чисел, поступающих на вход генератора, и могут быть применены для усовершенствования стохастического средства защиты информации в ССС с КРК.

- Разработанное программное обеспечение для ПЭВМ в пакете Matlab SIMULINK, защищённое свидетельством о государственной регистрации программы для ЭВМ позволяет выполнять исследования процесса передачи информации в модели ССС с КРК на основе стохастического применения АМФОКП при изменении отношения сигнал/шум в канале связи.

- Даны рекомендации по использованию компьютерной модели в пакете Matlab SIMULINK ССС с КРК, реализующей модель противодействия угрозе подмены сообщений на основе применения стохастического средства защиты информации.

Степень достоверности результатов диссертационного исследования обеспечивается методологической строгостью применения математического аппарата. Эффективность разработанных методов и алгоритмов подтверждена экспериментально путём компьютерного моделирования в программных средах Matlab и Matlab SIMULINK. Все ключевые положения, гипотезы, ограничения и допущения, использованные в работе, соответствуют опубликованным научным данным в рамках исследуемой тематики. Экспериментальные данные, полученные в ходе исследования, согласуются с частными результатами авторитетных работ в данной области. Техническая новизна генератора АМФОКП и ССС с КРК, использующих стохастическое средство защиты информации, подтверждается имеющимися у автора патентами на изобретения.

Публикации. Основные положения диссертации опубликованы в 14 научных печатных работах в том числе: 5 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК РФ, 9 – в материалах конференций и других изданиях. Получено 4 патента на изобретение, 3 свидетельства о государственной регистрации программ для ЭВМ.

Внедрение результатов исследования проведено в ООО «Инфоком-С» в научно-практических исследованиях по созданию новых и совершенствованию существующих методов и алгоритмов скрытого информационного обмена в беспроводных системах передачи данных в системе комплексной безопасности распределенных объектов на базе программной платформы «Дарвис» с целью повышения скрытности от деструктивных воздействий информации, передаваемых в беспроводных каналах связи; в учебный процесс ФГАОУ ВО «Северо-Кавказский федеральный университет» по дисциплинам «Информационная безопасность телекоммуникационных систем» и «Защита информации в системах беспроводной связи», изучаемых студентами по направлению подготовки 10.03.01

«Информационная безопасность», направленности (профилю) «Организация и технология защиты информации», а также выполнением работ по гранту «Грант-ИБ» № 29/2020 от 14.10.2020 г. РТУ МИРЭА.

Соответствие паспорту научной специальности. Содержание диссертации соответствует паспорту специальности 2.3.6 Методы и системы защиты информации, информационная безопасность (технические науки) по областям исследований:

– **п. 9.** Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности;

– **п. 15.** Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Апробация результатов диссертационного исследования. Основные положения и результаты диссертации обсуждались и получили положительную оценку на: Международной научно-практической конференции «Роль и значение науки и техники для развития современного общества» (Волгоград, 26 ноября 2018 года); Международной научно-практической конференции «Прорывные научные исследования как двигатель науки» (Магнитогорск, 4 декабря 2018 года); IX Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества» (Ставрополь, 19-21 декабря 2018 года); Workshop on computer science and information technologies 21thCSIT’2019 (Vienna, Austria, 2019); VII Международной научной конференции, посвященной памяти С.С. Ефимова «Математическое и компьютерное моделирование» (Омск, 22 ноября 2019 года); Национальной (Всероссийской) научно-практической конференции «Актуальные вопросы развития научных исследований: теоретический и практический взгляд» (Тюмень, 22 декабря 2020 года); II Всероссийской научной конференции (с приглашением зарубежных ученых) «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (Ставрополь, 30 ноября 2020 года); Всероссийской научно-практической

конференции «Инновационные векторы цифровизации экономики и образования в регионах России» (Ставрополь, 10-11 марта 2021 года); Международной научно-практической конференции «Глобальные тенденции и перспективы цифровизации экономики, образования и науки – 2021» (Ставрополь, 19–20 мая 2021 года); Всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий - РЭУС-2020» (Москва, 27-29 мая 2020 года); Всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2021» (Москва, 02-04 июня 2021 года); XI Всероссийской научно-практической конференции «Проблемы передачи информации в инфокоммуникационных системах» (Волгоград, 28 мая 2021 года); Всероссийской научно-теоретической конференции «Теория и практика обеспечения информационной безопасности» (Москва, 3 декабря 2021 года); Всероссийской конференции «Радиоэлектронные устройства и системы для инфокоммуникационных технологий - РЭУС-2022» (Москва, 08-10 июня 2022 года); XLI Всероссийской научно-технической конференции «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» (Серпухов, 23-24 июня 2022 года); IV Всероссийской научно-практическая конференции «Социотехнические и гуманитарные аспекты информационной безопасности» (Пятигорск, 25-27 апреля 2023 года).

Структура и объем работы. Объём диссертационной работы составляет 247 страниц основного содержания. Материал сопровождается 81 иллюстрацией и 15 таблицами. Структура исследования включает введение, четыре раздела, заключение, список из 145 использованных источников, а также три приложения.

Личный вклад автора. Все изложенные в работе результаты исследований получены при непосредственном участии автора. Авторским вкладом являются: 1) разработка модели противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП; 2) разработка модели АМФОКП и алгоритма их синтеза для ССС с КРК; 3) разработка структуры и алгоритма функционирования генератора псевдослучайных АМФОКП для стохастического средства защиты информации (в соавторстве); 4) разработка программной модели

защищённой ССС с КРК со стохастическим применением АМФОКП (в соавторстве).

Во введении проведено обоснование актуальности научного исследования, приведены результаты анализа современных исследований в рассматриваемой предметной области и выявленные противоречия в практике и в теории, обозначены объект и предмет диссертационного исследования, сформулированы цель и задачи диссертационной работы. Детально представлены научная новизна и практическая значимость полученных результатов, а также приведена информация об апробации и внедрении основных результатов диссертационной работы и их публикациях. Изложены ключевые тезисы, формирующие концептуальную основу диссертационной работы, представлены основные положения, выносимые на защиту, приведена общая характеристика диссертационной работы.

В первой главе последовательно проведен анализ функционирования существующих ССС с КРК, проанализированы пути повышения защищенности ССС с КРК, обоснована целесообразность решения вопроса повышения защищенности информации в ССС с КРК от угрозы подмены сообщений на основе увеличения структурной скрытности ансамблей ортогональных кодовых последовательностей с изменяющейся структурой и определены научная задача исследования и основные задачи исследования. Обоснована необходимость разработки метода противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения АМФОКП.

Во второй главе решена первая основная задача исследования. В ней разработана модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП размерностей N =128, 256, которая позволяет повысить показатель структурной скрытности, что в свою очередь обеспечивает противодействие угрозе подмены сообщений в ССС с КРК. Модель противодействия угрозе подмены сообщений позволяет в процессе передачи информации реализовать стохастическое применение АМФОКП синхронно на передающей и приемной сторонах.

В третьей главе решена вторая основная задача исследования – разработана модель АМФОКП и алгоритм их синтеза для ССС с КРК, обеспечивающие повышение их количества до требуемого значения $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$ по сравнению с известными.

Разработанные модель и алгоритм синтеза псевдослучайных АМФОКП основаны на рассмотрении СВ ЭМ, которые удовлетворяют условию ортогональности. В главе показано, что, используя различные наборы диагональных коэффициентов ЭМ, можно получать различные по своей структуре ансамбли ортогональных кодовых последовательностей. Аналитически и экспериментально доказана взаимосвязь между модулями и аргументами диагональных коэффициентов ЭМ и координатами их СВ, выступающими в качестве моделей псевдослучайных АМФОКП. В данной главе проведено сравнение количества уникальных последовательностей АМФОКП, полученных разработанным методом синтеза, с количеством известных АДОМУС. Повышение уровня структурной скрытности до требуемого значения $S_{\text{треб.}} \geq 43$ ДИЗ возможно при условии, что дискретность изменения угла фаз в составе получаемых АМФОКП будет от $\Delta\varphi \leq 90°$. Выявленные преимущества АМФОКП, получаемых на основе СВ бидиагональных ЭМ, по показателю структурной скрытности по сравнению с известными ансамблями ортогональных кодовых последовательностей обосновывают целесообразность их стохастического применения в современных ССС с КРК для обеспечения требуемого уровня их структурной скрытности.

В четвертой главе решена третья основная задача исследования – разработаны принцип построения и техническое решение стохастического средства защиты информации для ССС с КРК, предназначенного для противодействия угрозе подмены сообщений в ССС с КРК в виде структуры универсального формирователя АМФОКП и алгоритма формирования АМФОКП. Также в данной главе осуществлена разработка программной модели ССС с КРК в виде структуры и алгоритма функционирования генератора псевдослучайных

АМФОКП для стохастического средства защиты информации, а также программной модели ССС с КРК на основе стохастического применения АМФОКП в среде Matlab SIMULINK.

В заключении приведены основные научные и практические результаты исследований, а также предложены возможные направления дальнейших исследований, сформулированы выводы по диссертации.

Автор выражает огромную признательность научному руководителю, кандидату технических наук, профессору Жук Александру Павловичу за помощь в решении частных научных задач и подготовке к защите диссертации.

1 АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ И УГРОЗ НАРУШЕНИЯ ИХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Исследование принципов построения и функционирования систем спутниковой связи

Оценка требуемых характеристик будущей усовершенствованной с точки зрения защищённости системы передачи информации основывается на выборе системы передачи, выбранной в качестве прототипа. Рассмотрев параметры и характеристики системы передачи информации-прототипа, можно будет определить исходные данные для разработки предложений по синтезу и применению новых сигнально-кодовых конструкций.

В данной работе за прототип выбирается система спутниковой связи с кодовым разделением каналов. Данный выбор объясняется следующими причинами:

– ССС в последние десятилетия находят широкое применение для глобальных коммуникаций в различных целях;

– ССС имеют тенденцию к повышению пропускной способности информационных трактов и снижению стоимости за её использование;

– ССС подвержены различным угрозам, характерным для беспроводных систем передачи информации, что предопределяет необходимость развития защитных механизмов для предотвращения угроз передаваемой информации.

Как известно, системы спутниковой связи являются разновидностью беспроводных систем передачи информации, предназначенных для глобального информационного взаимодействия между собой, в которых передача информации осуществляется через искусственные спутники Земли, находящихся на различных орбитах [1-4].

ССС играют важнейшую роль в жизни и деятельности людей, поскольку обеспечивают связью, в том числе в тех случаях, когда другие телекоммуникационные системы в силу географической удаленности или сложных метеорологических условий, а также по причине малонаселенности являются недоступными [38, 74].

Увеличение спутниковой емкости за последние годы привело к снижению стоимости одного телефонного канала в новейшей истории и теперь рассчитывается как снижение стоимости бита в цифровую эпоху. Помимо снижения стоимости связи, наиболее значимой особенностью ССС является разнообразие услуг, предлагаемых ими [39].

ССС является сложной в исполнении и имеет высокую стоимость создания и обслуживания. Для передачи информации комплекс оборудования ССС включает наземную станцию, антенну и спутник-ретранслятор. Наиболее дорогостоящим устройством ССС является спутник-ретранслятор.

Оборудование наземной станции состоит из устройств, формирующих сигнал, устройств приема и передачи сигнала на требуемой частоте и антенну или антенную систему.

Варианты наземных станций спутниковой системы связи представлены на рисунке 1.1

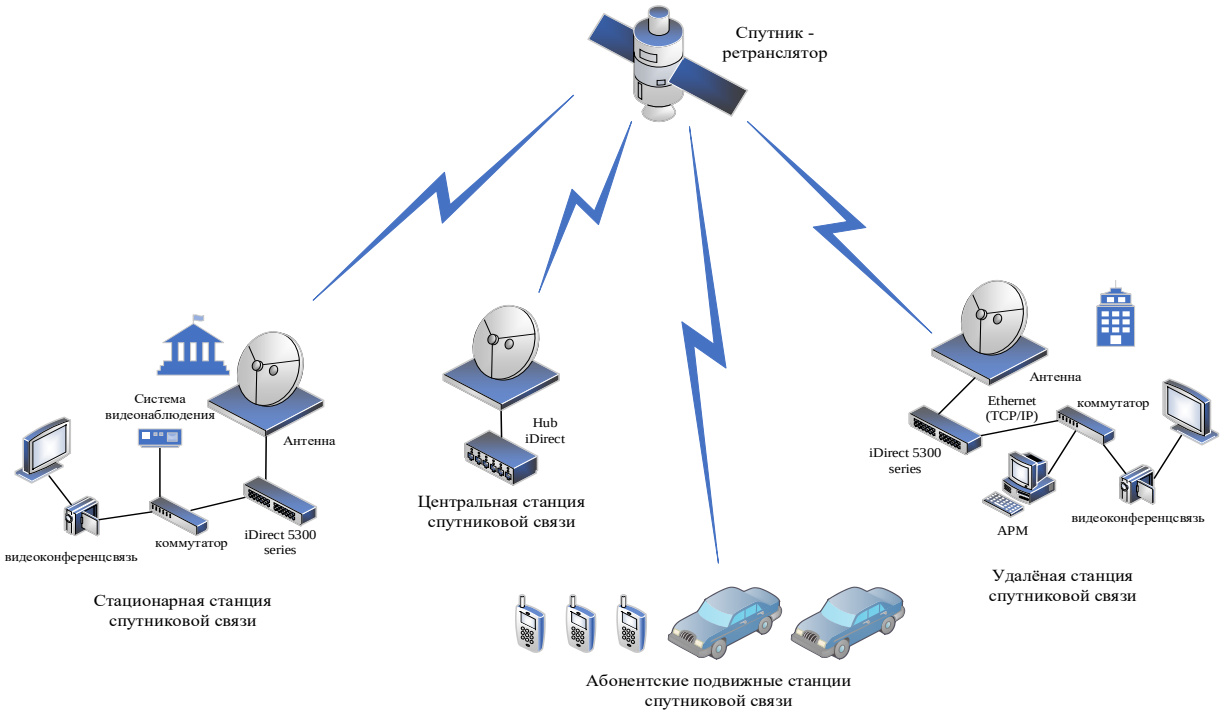


Рисунок 1.1 – Варианты наземных станций спутниковой системы связи

Наземные станции различают по следующим основным параметрам [1-4, 40]:

– диаметр антенны;

– мощность передатчика;

– качество приемника;

Диаметр антенны ССС может составлять от 0,5 м до 30 м. Больший диаметр антенны обеспечивает лучший прием. У переносных наземных станций антенна может быть складной. Ее диаметр составляет порядка 1 м.

Для современных ССС характерно быстрое увеличение объема передаваемой информации. Для лучшего покрытия поверхности Земли и увеличения пропускной способности ССС увеличивается количество спутников на геостационарной орбите, что сокращает расстояние между ними. Опыт эксплуатации ССС показывает, что при уменьшении углового расстояния менее 5° между спутниками на орбите появляются взаимные помехи, что может создать проблемы в приеме сигналов от спутников-ретрансляторов для наземных станций.

Указанная проблема может решаться путем перехода в более высокий диапазон частот с целью создания узконаправленного изучения. Другим путем

решения данной проблемы является создание сигналов на основе ортогональной поляризации радиоволн.

Частота, с которой сигнал отправляется в космос, называется частотой восходящей линии связи, а частота, с которой он отправляется транспондером, называется частотой нисходящей линии связи. Иллюстрация восходящих и нисходящих линий спутниковой связи представлена на рисунке 1.2.

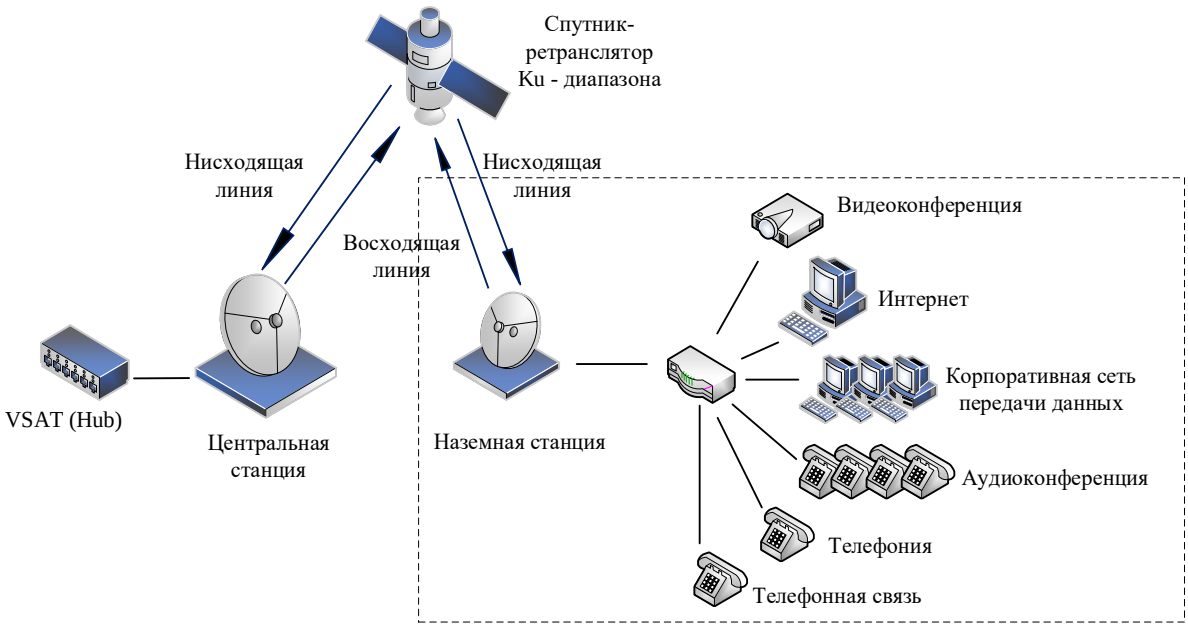


Рисунок 1.2 – Иллюстрация нисходящей и восходящей линий спутниковой связи

Сигналы ССС различают по форме, частоте, в пространстве, по времени. При передаче сигналы кодируют различными способами.

Существует множество преимуществ спутниковой связи, таких как:

– гибкость;
– простота установки новых схем;
– легкость преодоления больших расстояний при низкой стоимости;
– возможность вещания на определенную территорию;
– высокая плотность покрытия Земли;
– возможность управлять сетью со стороны пользователя.

Спутниковая связь также имеет следующие недостатки:

– первоначальные затраты слишком высоки;

– перегруженность частотного диапазона;

– высокая чувствительность системы к помехам и условиям распространения радиоволн.

В работах [1-4, 26-30, 38-40, 45-47, 50, 56,58, 67, 134, 135] приведены подробное описание состава ССС и архитектуры спутниковых группировок, характеристика спутниковых орбит, диапазонов частот и проведен сравнительный анализ различных ССС.

Одним из ключевых вопросов, влияющих на эффективность функционирования ССС, является тип многостанционного доступа. Он подразумевает под собой возможность для любой наземной станции системы независимо от других наземных станций системы использовать спутник-ретранслятор для передачи своих сигналов, а также устанавливать связь через спутник-ретранслятор с каждой наземной станцией системы [1-4].

Многостанционный доступ обеспечивает системе необходимую гибкость, но при этом усложняет функции спутника-ретранслятора [41, 42].

Организация многостанционного доступа позволяет закрепить линию связи между двумя станциями или последовательно использовать линию связи между наземными станциями при ее освобождении.

В ССС используют следующие виды многостанционного доступа, отличающиеся по принципу разделения сигналов:

1. Частотный многостанционный доступ FDMA (Frequency-division multiple access).

2. Временной многостанционный доступ TDMA (Time-division multiple access).

3. Пространственный многостанционный доступ SDMA (Space-division multiple access).

4. Кодовый многостанционный доступ CDMA (Code-division multiple access).

В таблице 1.1 показаны ССС, использующие указанные виды многостанционного доступа.

Таблица 1.1 – Характеристики современных ССС

Наименование ССС	Высота, км	Многостанционный доступ	Предоставляемые услуги	Год начала работы
Globalstar	1389	CDMA/FDMA	Глобальный роуминг, подключение к наземным сетям сотовой связи	1999
Iridium	765	TDMA	Передача голоса, данных и пейджинг на портативные терминалы	1998
Odyssey	10355	CDMA	Передача голоса, данных и пейджинг на портативные терминалы	1997
Ellipso	429/2903	CDMA	Дополняет и расширяет существующие сотовые системы	1996
Starlink	335,9 -570	TDMA FDMA	Высокоскоростной доступ в сеть Интернет	2020

Среди многообразия видов доступа в ССС с КРК доступ типа CDMA является достаточно распространенным, в частности используется в Globalstar для предоставления пользователям услуг связи по передаче речи и данных.

Анализ источников [43-49] показывает, что ССС с КРК имеют следующие преимущества:

1. Имеют повышенную пропускную способность.

2. За счет применения ортогональных последовательностей в канале связи отмечается более низкий уровень помех со стороны других мобильных устройств, что обеспечивает более простое совместное использование частотных ресурсов по сравнению с FDMA.

3. Облегчает совместное использование частотных ресурсов при наличии больших доплеровских сдвигов частоты.

4. Общее использование системой одной частотной полосы пропускания приводит к возможности использования более узкополосных антенн, что в свою очередь уменьшает размеры антенны и тем самым позволяет с одной стороны защититься от помех соседних спутниковых систем, включая средства

радоэлектронной борьбы (РЭБ), с другой стороны уменьшить массогабаритные показатели портативного и переносного оборудования.

В силу преимуществ система спутниковой связи с кодовым разделением каналов выбрана в качестве **объекта исследования** в данной диссертационной работе.

Следует отметить, что в ССС с КРК используется в линиях вверх и вниз несколько видов кодовых последовательностей. Для расширения спектра используется короткий код, обычно на основе последовательностей Уолша, для скремблирования используется длинный код, обычно на основе M-последовательностей, кодов Голда [50]. Для начального взаимодействия в ССС с КРК также используются код преамбулы на основе кодов Адамара.

Также отметим, что при организации трактов передачи и приема используется квадратурная фазовая манипуляция QPSK (Quadrature phase shift keying), которая строится на основе кодирования двух бит передаваемой информации одним символом (рисунок 1.3). При этом символьная скорость в два раза ниже скорости передачи информации.

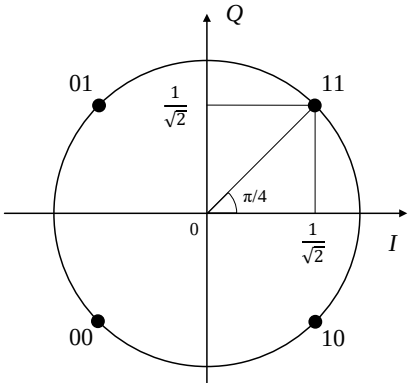


Рисунок 1.3 – Иллюстрация модуляции QPSK

Также в работе [145] отмечается, что в ССС с КРК может использоваться квадратурная амплитудная модуляция (КАМ), или как указано в англоязычных источниках Quadrature Amplitude Modulation (QAM). При данном виде модуляции изменению подвергается и амплитуда и фаза несущего сигнала. У модуляции 16-

QAM используется четыре уровня в каждом квадратурном канале. В методе 16-позиционной квадратурной амплитудной модуляции (16-QAM) каждая из квадратурных составляющих — синфазная (I) и квадратурная (Q) — может принимать четыре различных уровня сигнала. Комбинируя эти уровни, формируется 16 уникальных состояний результирующего сигнала, как показано на рисунке 1.4, что повышает эффективность передачи данных [145].

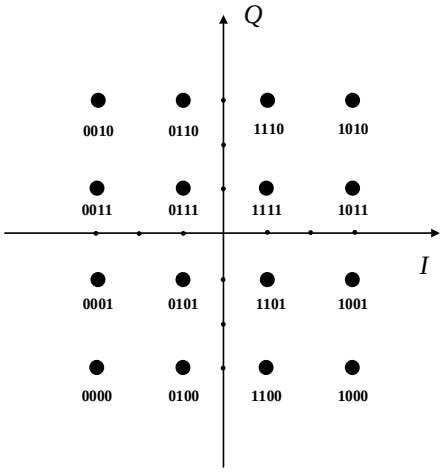


Рисунок 1.4 – Иллюстрация модуляции 16-QAM

Таким образом, системы спутниковой связи приобретают все более значимую роль в процессе организации коммуникаций пользователей в глобальном мировом масштабе и за его пределами.

1.2 Анализ угроз информационной безопасности систем спутниковой связи

В силу того, что ССС стали неотъемлемой частью глобальной телекоммуникационной инфраструктуры, обеспечивая широкий спектр услуг от

телевизионного вещания до подключения к Интернету и глобального позиционирования, возникает логичный вопрос обеспечения информационной безопасности в этих системах.

Анализ источников показывает, что в отношении ССС существуют угрозы безопасности информации. Эти угрозы можно классифицировать на физические угрозы, кибернетические угрозы (киберугрозы) и электронные угрозы телекоммуникационной системе (рисунок 1.5) [27-30].

Рисунок 1.5 – Классификация угроз ССС

К физическим угрозам относятся стихийные бедствия, такие как космический мусор, солнечные вспышки и метеориты, которые могут повредить или уничтожить спутники. Космический мусор, в частности, стал серьезной проблемой из-за увеличения числа спутников, выводимых на орбиту. Еще одна физическая угроза исходит от противоспутникового оружия, представляющего собой устройства, предназначенные для вывода из строя или уничтожения спутников в стратегических военных целях. В свою очередь, физические угрозы могут быть кинетическим и некинетическими.

Вторая категория угроз – это кибернетические угрозы или киберугрозы. Системы спутниковой связи используют сложное программное обеспечение и цифровые протоколы связи, которые могут быть уязвимы для взлома и других форм кибератак. Реализация киберугроз может нарушить работу сервисов ССС, осуществить утечку конфиденциальных данных или взятие под контроль злоумышленников управление спутниками. К кибернетическим угрозам относятся [51] угрозы от:

– сетевой атаки методом грубой силы;
– сетевой атаки на основе электронной почты;
– атаки через внешний/съемный носитель;
– сетевой атаки, путем маскировки под авторизованного пользователя;
– неквалифицированной эксплуатации оборудования;
– утери/кражи оборудования;
– сетевой атаки через Интернет;
– других типов атак.

К электронным угрозам относятся угрозы нарушения функционирования сегментов ССС путем воздействия на линии связи, указанные на рисунке 4.

Функционирование спутниковой группировки зависит от надежности функционирования линий связи между космическим сегментом и наземным сегментом в обоих направлениях. Если восходящий канал, такой как канал телеуправления, будет атакован, то спутник выйдет из-под контроля и не сможет корректно функционировать. Если нисходящая линия связи будет атакована, то данные, отправленные со спутника, не будут приниматься наземными станциями [31].

Электронные угрозы ССС разделяют на угрозы линям ССС, включающие в себя:

– подавление (глушение) линий спутниковой связи (угрозы орбитального глушения системы спутниковой связи, угроза наземного глушения сигналов спутниковой связи, угроза глушения восходящей и нисходящей линий спутниковой связи);
– подмена сообщений (англ. spoofing – подмена);
– подслушивание (от англ. sniff – нюхать).

Классификация электронных угроз ССС представлена на рисунке 1.6.

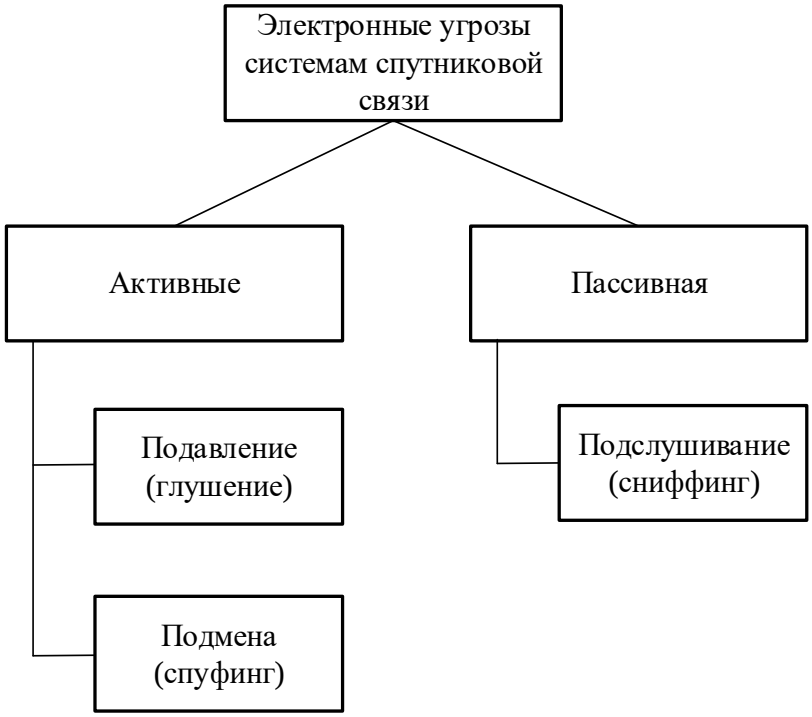


Рисунок 1.6 – Классификация электронных угроз ССС

Электронные угрозы ССС делятся на активные, такие как подавление (глушение) и подмена и пассивную – подслушивание [72].

Подавление (глушение) является самым известным методом воздействия на системы спутниковой связи. В этом случае злоумышленник излучает ложный сигнал в сторону приемника или подавляет (глушит) полезный сигнал передатчика, препятствуя штатному функционированию системы спутниковой связи. Создаваемые таким образом помехи стали являются основной причиной износа и деградации спутников.

Злоумышленники используют направленную антенну для создания помех, обычно специально созданного сигнала, который имеет достаточную мощность, чтобы он был воспринят за исходный передаваемый сигнал. Глушение спутников – это угроза, которая часто реализуется для вмешательства в коммуникации для предотвращения распространения информации. Часто используется в отношении средств массовой в целях цензуры.

Существует две формы глушения спутников: орбитальная и наземная.

При орбитальном глушении злоумышленник посылает луч подавляющих сигналов непосредственно на спутник через ложную станцию восходящей линии связи (рисунок 1.7). Сигналы помех смешиваются с полезными сигналами, тем самым создавая для них помехи.

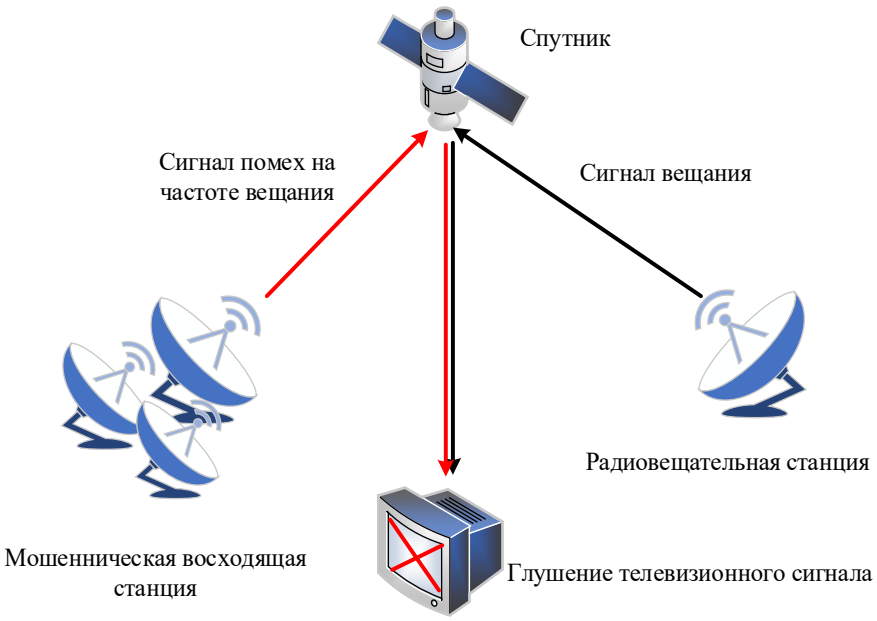


Рисунок 1.7 – Иллюстрация угрозы орбитального глушения ССС

При наземном глушении атакующий злоумышленник передает подавляющие сигналы на блуждающих частотах в направлении наземных спутниковых станций (приемных антенн). В данном случае наземные помехи воздействуют в направлении рядом расположенных спутниковых антенн потребителей. Подавление помех в этом случае ограничивается определенной областью, т.е. помехи создаются только сигналам на частоте излучения, исходящим от спутника в ограниченном пространстве.

Устройства наземного глушения имеют небольшой радиус действия порядка 3-20 километров. Иллюстрация процесса наземного глушения сигналов спутниковой связи представлена на рисунке 1.8.

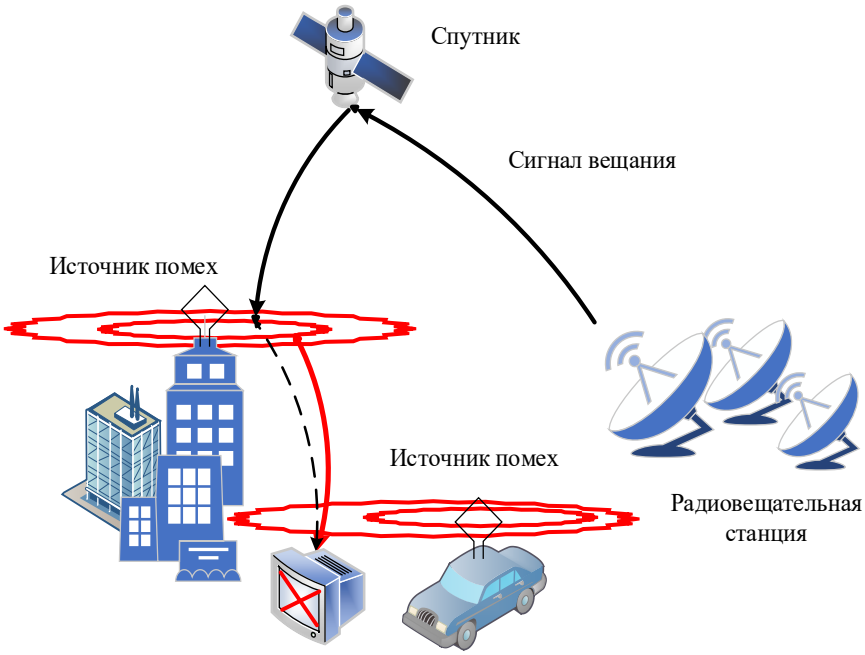


Рисунок 1.8 – Иллюстрация угрозы наземного глушения сигналов спутниковой связи

Угроза подмены сообщений в линиях спутниковой связи реализуется с помощью спуфинг-атаки – такого вида атаки, при которой с использованием специального устройства на частотах ССС приемному устройству отправляются ложные сообщения под видом истинных. Уровень сигнала устройства, отправляющего ложные данные, должен быть выше уровня сигнала в ССС. На входе приемника происходит подмена сообщения и ССС получает ложные данные.

Угроза подмены сообщения (спуфинг) опасна тем, что может внести незаметные для системы (пользователя) искажения в данные, в интересах злоумышленника.

Реализация угроз ССС проводится посредством атак злоумышленника как на систему в целом, так и на ее сегменты, такие как наземный, космический, пользовательский сегменты и сегмент связи.

Физические атаки легко обнаруживаются. Кинетическое оружие наносит удар по наземной станции и спутнику-ретранслятору напрямую. Некинетическое оружие включает в свой состав электромагнитные импульсы, лазеры, микроволновое излучение большой мощности и наносит поражение без

непосредственного физического контакта с объектом воздействия. Атаки некинетическим оружием незаметны и наносятся практически со скоростью света.

Электронная атака глушение сигналов производится путем подавления радиочастотных сигналов, используемых для передачи данных ССС. Такую атаку обнаружить легко. Глушение с одной стороны является достаточно легко реализуемым и не дорогим в исполнении видом атаки, с другой стороны глушение является одной из самых легких форм взломов, так как сигнал после прекращения такого воздействия достаточно быстро восстанавливается в исходное состояние.

Электронную атаку подмены обнаружить сложно. Такая атака может внести незаметные для системы (пользователя) искажения в данные, в интересах злоумышленника.

Электронную атаку подслушивание обнаружить невозможно, ввиду того что отсутствуют признаки воздействия на ССС, однако именно подслушивание злоумышленником сигналов атакуемой ССС, может указывать на сбор данных для последующих атак на систему, в том числе таких как кибернетические атаки.

Защитить открытые данные от такого вида атак достаточно сложная задача, которая может решаться путем шифрования (кодирования) данных или изобретением специальных алгоритмов обнаружения ложных данных и их отбрасывания. Во многих ССС данные передаются при отсутствии шифрования или кодирования, поэтому их легко перехватить и исказить.

Одним из самых популярных технических решений в виде кейсов спутникового прослушивания является готовое программное обеспечение SkyGrabber, производимое российской фирмой Sky Software.

Это программное обеспечение использовалось хакерами в Ираке и Афганистане для захвата незашифрованных видеопотоков беспилотных летательных аппаратов (БЛА) Predator. Повстанцы в этих районах не могли контролировать или нарушать работу БПЛА, но они использовали программу SkyGrabber от компании SkySoftware для подслушивания посылаемых сигналов.

Кибернетические атаки обнаружить сложнее других видов атак. В настоящее время это одна из самых изощренных видов атак на ССС. Она способна привести к

отключениям, манипуляции данными и их модификации. В таблице 1.2 приведена открытая статистика NASA по количеству реализованных кибернетических атак ССС [51].

Таблица 1.2 – Количество реализованных кибернетических атак ССС по данным NASA

№ п/п	Типы реализованных атак	Количество реализованных атак			
		2017 г.	2018 г.	2019 г.	2020 г.
1	Сетевая атака методом грубой силы	9	10	0	2
2	Сетевая атака на основе электронной почты	149	97	510	110
3	Атака через внешний/съемный носитель	6	0	6	30
4	Сетевая атака, путем маскировки под авторизованного пользователя	0	1	0	4
5	Неквалифицированная эксплуатация оборудования	249	267	805	1103
6	Утеря/кража оборудования	430	392	346	274
7	Сетевая атака через Интернет	391	287	95	219
8	Другие типы атак	50	83	126	43
	Всего:	1284	1137	1888	1785

Статистика показывает увеличение следующих кибератак: сетевая атака, путем маскировки под авторизованного пользователя и неквалифицированная эксплуатация оборудования, которые способны нанести вред и привести к утечке конфиденциальных данных.

С учетом того, что неквалифицированная эксплуатация оборудования зависит от правильности действий персонала, то основной атакой со стороны злоумышленника можно считать сетевую атаку, путем маскировки под авторизованного пользователя. Такая атака требует небольших затрат злоумышленнику на оборудование в сравнении с потенциальным вредом, который он может нанести, при ее реализации.

Таким образом, спутники на орбите зависят от линий связи между космическим сегментом и наземными станциями в обоих направлениях. Если восходящий канал, такой как канал телеуправления, будет атакован, спутник

выйдет из-под контроля и не сможет предоставлять запланированные услуги. Если нисходящая линия связи будет атакована, то данные, отправленные со спутника, не будут приниматься наземными станциями.

Угрозы ССС со стороны злоумышленника направлены как на систему в целом, так и на ее сегменты.

Угрозы ССС можно классифицировать на физические угрозы, электронные угрозы телекоммуникационной системе и кибернетические угрозы (киберугрозы).

Электронные угрозы ССС наиболее просто могут быть реализованы злоумышленниками, а также могут быть активными и пассивной. Они направлены на линии и сигналы ССС с целью подавления (глушения) линий, подслушивания и подмены сообщений в линиях спутниковой связи.

Для реализации угрозы глушения линии спутниковой связи злоумышленнику необходимо специальное оборудование, позволяющее сначала ему обнаружить, а затем блокировать (подавить) необходимую радиолинию. Применительно к рассматриваемым системам спутниковой связи устройство блокирования помимо всего прочего должно иметь направленную антенну для обеспечения высокой эффективности глушения линии спутниковой связи. С учетом сказанного можно сделать вывод о том, что для реализации угрозы глушения линии спутниковой связи требуются существенные материальные затраты на приобретение оборудования и его использование подготовленными специалистами, поэтому реализация данной угрозы возможна тогда, когда существует объективная необходимость блокирования процесса информационного обмена между корреспондентами ССС.

Кроме того, угроза подслушивания в ССС может быть предварительным этапом реализации угрозы глушения линии спутниковой связи, поскольку прежде, чем подавлять конкретную радиолинию ССС, необходимо быть уверенным в том, что это именно она.

По причинам наличия объективной необходимости глушения конкретной линии ССС и необходимости выделения существенных материальных затрат на

приобретение оборудования и его использование подготовленными специалистами при реализации угрозы глушения ССС её можно отнести к маловероятным угрозам.

Угрозу подмены сообщений в ССС достаточно легко реализовать с использованием стандартного комплекта оборудования спутниковой связи с незначительной модификацией программного обеспечения.

По этой причине угроза подмены сообщений можно отнести к угрозе, реализуемой злоумышленниками с высокой степенью вероятности в силу простоты ее реализации и отсутствием необходимости выделения существенных материальных затрат на ее реализацию. В силу выявленных обстоятельств в данной диссертационной работе основное внимание будет уделено противодействию угрозы подмены сообщений в ССС.

Рассмотрим угрозу подмены сообщений сети передачи данных на примере ССС с КРК Globalstar.

Система спутниковой связи (ССС) с использованием кодового разделения каналов (КРК) Globalstar была создана в 1991 году с целью обеспечения широкого доступа к услугам спутниковой связи. Основной функционал системы включает телефонную связь, передачу данных на скорости до 9,6 кбит/с, обмен SMS-сообщениями, голосовую почту, глобальный роуминг, экстренный вызов служб спасения и определение геолокации [32, 56, 34, 135].

К дополнительным возможностям ССС с КРК Globalstar относятся: переадресация звонков, функция удержания и блокировки вызовов, идентификация и скрытие номера, а также организация трехсторонней связи [32, 56, 34, 135].

Изначально система ССС с КРК Globalstar создавалась для обеспечения взаимодействия с существующими сотовыми системами связи за пределами их зон покрытия.

В настоящее время ССС с КРК Globalstar предоставляет спутниковую связь высокого качества на более чем 80% поверхности Земли и имеет высокий потенциал развития, в частности в 2024 году Федеральная комиссия по связи (FCC) США дала частичное разрешение компании Globalstar, предоставляющую связь

для iPhone, на запуск 26 спутников для обновления и расширения своей существующей сети мобильной связи.

ССС с КРК Globalstar разрабатывает новые системы и устройства с целью расширения возможностей по предоставлению услуг связи. Таким устройством является спутниковый приемопередатчик SPOT и система для телеметрического контроля и сбора данных (SCADA).

SPOT позволяет отслеживать местоположение пользователя и отправлять текстовые сообщения, в том числе сигнал о бедствии.

SCADA использует модем GSP-1620 который является полно дуплексным спутниковым модемом на 9600 бит/сек. Модем GSP-1620 функционирует как «узел» Интернет, и, имея свой фиксированный или динамически присваиваемый IP-адрес, может адресоваться в режиме реального времени с необходимой частотой для поддержания контроля приложения за удалёнными устройствами.

OEMs обеспечивают приложение хоста (сервер), который использует модем GSP-1620 для собственного приложения SCADA на оконечном оборудовании данных (DTE) на удалённой площадке/объекте. Приложение хоста управляет обработкой данных на месте и выдаёт уведомления о нештатных процессах, отчёты о работе, аварийные состояния т.е. все данные, которые необходимо получить с удалённого объекта.

1.3 Анализ известных методов противодействия угрозам в системах спутниковой связи с кодовым разделением каналов

Как было установлено выше, информация, передаваемая в ССС, в наибольшей степени подвержена электронной угрозе подмены сообщений. Для

анализа возможных вариантов защиты информации от данного вида угрозы исследуем способы защиты информации в ССС.

В работах Сухарева Е.М., Гришенцева А.Ю. и др. [31, 52] указывается, что конфиденциальность передачи сообщений в беспроводных системах связи может быть обеспечена за счет информационной, энергетической и структурной скрытности.

Информационная скрытность подразумевает скрытие смыслового содержания передаваемой информации и достигается, как правило, за счет применения криптографических методов защиты информации в виде шифрования и расшифрования [138, 139].

Энергетическая скрытность подразумевает под собой свойство системы передачи информации противостоять мероприятиям по обнаружению полезного сигнала злоумышленником на фоне помех. Чем менее заметным является полезный сигнал в анализируемом частотном диапазоне, тем выше его энергетическая скрытность.

Структурная скрытность характеризуется сложностью распознавания злоумышленником структуры информационного сигнала. Данное свойство достигается за счет использования сигнала, который по своей структуре максимально приближен к характеристикам фонового шума.

Реализация защиты информации способом обеспечения информационной скрытности осуществляется как правило шифрованием, которое включает в себя преобразование открытого текста в зашифрованный (закрытый) текст с использованием алгоритма шифрования и секретного ключа. Зашифрованный текст может быть расшифрован при использовании симметричных криптоалгоритмов только с использованием одного и того же секретного ключа, гарантируя, что только авторизованные пользователи могут получить доступ к передаваемой информации [138, 139].

Шифрование пользовательской информации, передаваемой в ССС, имеет важное значение для обеспечения безопасности и целостности конфиденциальной информации, передаваемой посредством системы спутниковой связи. Без

шифрования данные могут быть перехвачены и скомпрометированы посторонними лицами, что приведет к серьезным последствиям, таким как нарушения информационной безопасности и/или финансовые потери.

Шифрование имеет решающее значение для защиты данных от спуфинговых атак, а также используется для взаимной аутентификации собеседников. Шифрование в ССС не является окончательным решением, оно добавляет дополнительный уровень защиты, например, за счет использования криптографических алгоритмов.

В ССС кроме шифрования пользовательской информации реализуется шифрование служебной информации в трактах передачи между модулями спутниковой структуры. В некоторых ССС могут быть зашифрованы, например, данные телеуправления-телесигнализации (TT&C), восходящие линии связи или доступ между наземными сетями и наземными станциями.

Анализ источников [27, 32] показывает, что большинство коммерческих спутниковых систем спроектированы и используются без шифрования данных. Каждая передача имеет «открытый доступ» и передается без какой-либо защиты.

Например, ССС с КРК Globalstar [32] не используют шифрование при передаче сообщений, что позволяет злоумышленнику без труда получать доступ к информации в ССС.

Такой недостаток может быть устранен, например, с помощью комплекса «Застава» компании ЭЛВИС-ПЛЮС, с помощью которого обеспечивается криптографическое преобразование пользовательских данных при организации защищенного удаленного доступа с помощью ССС.

Наряду с очевидным достоинством обеспечения информационной скрытности передаваемой информации путем её шифрования, существует ряд существенных его недостатков, а именно:

1. Шифрование может быть обеспечено увеличением вычислительной мощности процессоров систем передатчика и приемника ССС, что приведет к увеличению затрат на их реализацию, что влияет на общую стоимость системы, на производительность и глобальную безопасность системы.

2. Шифрование информации приводит к дополнительным неизбежным временным задержкам в процессе его реализации, помимо задержек сигнала, возникающих в силу большой протяженности космических линий, что, в свою очередь, имеет значение для передачи сообщений, критичных к времени их доставки до получателя.

3. Для организации криптографической защиты данных в ССС первостепенной задачей является решение вопроса распределения ключей, используемых для шифрования данных.

Анализ работы [52] показывает, что энергетическая скрытность систем спутниковой связи, использующей широкополосные сигналы (ШПС) тем выше, чем большее значение имеет ширина спектра ШПС, что в свою очередь, увеличивает время анализа сигнала в обнаружителе злоумышленника до момента его обнаружения. Однако ширина спектра ШПС не может увеличиваться до бесконечности в силу ограниченного частотного диапазона ССС. Известно [1-4], что ССС характеризуются применением ШПС с достаточно большой базой, что предопределяет наличие у них определенной энергетической скрытности, которая дальнейшим расширением спектра ШПС далее увеличивать невозможно. Поэтому рассматривать дальнейшее совершенствование системы защиты информации ССС на основе увеличения энергетической скрытности является нецелесообразным.

Вопросы обеспечения информационной и энергетической скрытности в ССС решены достаточно полно, поэтому в данной диссертационной работе для решения вопроса повышения защищенности информации в рассматриваемых системах предлагается совершенствование процесса защиты информации в ССС с КРК на основе увеличения арсенала используемых ансамблей ортогональных кодовых последовательностей, обеспечивающих повышение их структурной скрытности.

В системе спутниковой связи с КРК Globalstar, в настоящее время доступны следующие услуги: мобильная и фиксированная телефонная связь, передача данных (SCADA), передача факсимильных сообщений, отправка и прием коротких сообщений, международный роуминг, голосовая почта, экстренный вызов служб

спасения, определение координат объектов (SPOT), а также другие сервисы [32, 56, 34, 135].

В работе Черноусова А.В. и др. [132] отмечено, свойством ССС с КРК противостоять навязыванию ложного сообщения, его подмене или изменению хранимых данных является имитостойкость, которая является важным показателем защищенности рассматриваемых систем.

В исследовании [133] продемонстрировано, что имитостойкость канала связи, обеспечиваемая на уровне сигнала $I_{\text{с}}$, определяется следующими параметрами:

– размерностью пространства сигналов G;

– количеством разрешенных к применению сигналов $G_{\text{р}}$ в заданном временном интервале Δt;

– числом попыток имитации n;

– выбранной стратегией имитации q.

$$I_{\text{с}} = f\left(G, G_{\text{р}}, n, q\right). \tag{1.1}$$

В этой же работе отмечено, что в случае многократных попыток навязывания имитостойкость радиоканала может оцениваться безопасным временем $T_{\text{б}}$, определяемым математическим ожиданием времени статистического опробования всевозможных вариантов навязывания противником сигнала с использованием всего пространства $\{Z\}$ сложных сигналов. Безопасное время подразумевает интервал в времени, в течение которого злоумышленник не может осуществить подмену или ввести ложное сообщение.

Величина $T_{\text{б}}$ определяется из соотношения:

$$T_{\text{б}} = \frac{1}{2} \cdot Z \cdot t_{\text{опр.}}, \tag{1.2}$$

где $t_{\text{опр.}}$ – время передачи имитационного сигнала.

Очевидно, что

$$t_{\text{опр.}} = \frac{1}{R_n}, \tag{1.3}$$

где R_n – скорость имитационных воздействий противника.

Анализ выражения (1.2) показывает, что безопасное время $T_б$ зависит от размерности пространства сложных сигналов $\{Z\}$ и времени передачи имитационного сигнала $t_{\text{опр.}}$

Также в данной работе был проведен анализ имитостойкости и безопасного времени ССС с КРК на основе модуляции ФМ-2 ШПС с постоянными и переменными значениями параметрами F_b, F_c. Результат вычислений безопасного времени передачи широкополосного сигнала, представленный в работе [133], приведен в таблице 1.3.

Таблица 1.3 – Безопасное время передачи ШПС

Тип формирования	Длина ШПС					
	31	63	127	255	511	1023
ФМ-2 ШПС	$3{,}1\cdot10^{-4}$	$6{,}3\cdot10^{-4}$	$1{,}3\cdot10^{-3}$	$2{,}5\cdot10^{-3}$	$5\cdot10^{-3}$	$1\cdot10^{-2}$

Анализ таблицы 1.3 показывает, что безопасное время ССС с КРК имеют следующие значения

Для ФМ-2 при длине ПСП 127, $T_б = 1{,}3 \cdot 10^{-3} = 1{,}3$ мс.

Для ФМ-2 при длине ПСП 255, $T_б = 2{,}5 \cdot 10^{-3} = 2{,}5$ мс.

Для оценки достаточности времени безопасной работы рассчитаем время, необходимое для передачи пакета данных для SPOT-устройства. Так как скорость передачи информации в ССС с КРК Globalstar составляет 9600 бит/с, а размеры пакета данных для SPOT-устройства $Length = 144$ бит, то для передачи пакета данных потребуется время, равное $T_{\text{сообщ.}} = \frac{\text{Length}}{R} = 15$ мс.

С учетом того, что имеющееся безопасное время ССС с КРК значительно меньше требуемого для передачи пакета данных для SPOT 144 бит, а для SCADA–

устройств, то можно сделать вывод о недостаточности этого показателя в существующих ССС с КРК.

Поскольку в существующих ССС с КРК чаще всего в качестве расширяющих последовательностей используются последовательности Уолша, то можно сделать вывод о том, что их использование не обеспечивает безопасное время ССС в с КРК.

Как отмечается в работах Каневского З.М., Сухарева Е.М., Осмоловского С.А., Кандаурова Н.А., Стасева Ю.В, Горбенко И.Д., Макаренко Б.И. и др. в ССС для передачи информации возможно применение кодовых последовательностей, имеющих изменяющуюся структуру для обеспечения их структурной скрытности и безопасного времени ССС с КРК [35, 37, 48, 52, 53].

Для оценки показателя структурной скрытности сигналов Каневским З.М., Литвиненко В.П. [35, 117] предлагается использовать структурную скрытность, которая определяется мощностью A (числом элементов) множества X возможных сменных параметров сигнала, например, количество фаз, несущих частот, вариантов кодовой структуры. Авторами данных работ предлагается элементарная единица оценки скрытности в виде ДИЗ.

При оценке скрытности объекта (ансамбля кодовых последовательностей) предполагается оценивать затраты на выявление его состояния с заданной достоверностью (вероятностью правильного решения). Каждый этап поиска состояния объекта в данном подходе сопровождается одним ДИЗ.

Под структурной скрытностью подразумевается скрытность, определяемая мощностью A (числом элементов) множества X возможных сменных параметров сигнала, например вариантов кодовой структуры или несущих частот. Рабочие параметры передаваемого сигнала выбираются из этого множества случайно для злоумышленника.

Для оценки показателя структурной скрытности ортогональных кодовых последовательностей для ССС с КРК в данной диссертационной работе предлагается использовать показатель структурной скрытности, предложенный Каневским З.М. [35, 117]

$$S = \log_2 A \qquad (1.4)$$

При этом, как будет показано ниже, множество X возможных сменных параметров последовательностей, от которых будет зависеть показатель структурной скрытности, будет определяться количеством фаз элементов рассматриваемых последовательностей.

С учетом того, что максимальная скорость в прямом информационном канале 9600 Бит/с, а срок активной эксплуатации спутника ССС Globalstar до 15 лет, можно определить количество неповторяющихся структур АМФОКП (арсенал значений кодовых последовательностей), которые позволят обеспечить непрерывный информационный обмен ССС с КРК Globalstar без возвращения, то есть без повторного применения ранее использованных кодовых последовательностей.

Можно полагать, что в 15 годах содержится время $T_{\text{сущ. ССС}} = 473\,040\,000$ с. При скорости 9600 Бит/с за 15 лет может быть непрерывно передано $Length = T_{\text{сущ. ССС}} \cdot R$ =4 541 184 000 000 или $4{,}54 \cdot 10^{12}$ информационных символов.

В данном случае полученное число информационных символов, которые позволят обеспечить непрерывный информационный обмен ССС с КРК Globalstar за 15 лет неповторяющимися структурами кодовых последовательностей может принят за минимально допустимый арсенал АМФОКП $A_{\text{треб.}}$.

$$A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}.$$

Тогда по формуле для определения структурной скрытности $S = log_2 A$ можно определить минимально-допустимую структурную скрытность, которой должны обладать АМФОКП $S_{\text{треб.}} \geq log_2 A_{\text{треб.}}$, по результатам вычислений получим

$$S_{\text{треб.}} \geq 43 \text{ ДИЗ}.$$

Как известно в ССС с КРК, для расширения спектра используется короткий код, обычно на основе последовательностей Уолша, для скремблирования используется длинный код, обычно на основе M- последовательностей и кодов Голда [50]. Поэтому для оценки показателя структурной скрытности используемых в настоящее время ортогональных кодовых последовательностей определим значение этого показателя для последовательностей Уолша, M-последовательностей и кодов Голда.

В работе [37] приведена оценка численных значений структурной скрытности последовательностей Голда при длинах последовательностей равных 127, 255, 2047, 8191 и 16383, которая представлена в таблице 1.4.

Таблица 1.4 – Структурная скрытность последовательностей Голда

Длина последовательности Голда	Значение структурной скрытности последовательности Голда, ДИЗ
127(128)	≈7
255(256)	≈8
2047(2048)	≈11
8191(8192)	≈13
16383(16384)	≈14

Анализ таблицы 1.4 показывает, что при рассматриваемых ограничениях на длину последовательности, коды Голда имеют низкое значение структурной скрытности, значительно ниже 43 ДИЗ.

Поскольку в качестве длинного кода в рассматриваемой ССС с КРК используются ШПС на базе M-последовательностей, оценим их структурную скрытность.

Арсенал M-последовательностей равен базе ШПС и определяется выражением

$$S_M = S_0 = \log_2 B. \qquad (1.5)$$

График зависимости структурной скрытности ШПС M-последовательностей S_M от базы B имеет следующий вид (рисунок 1.9).

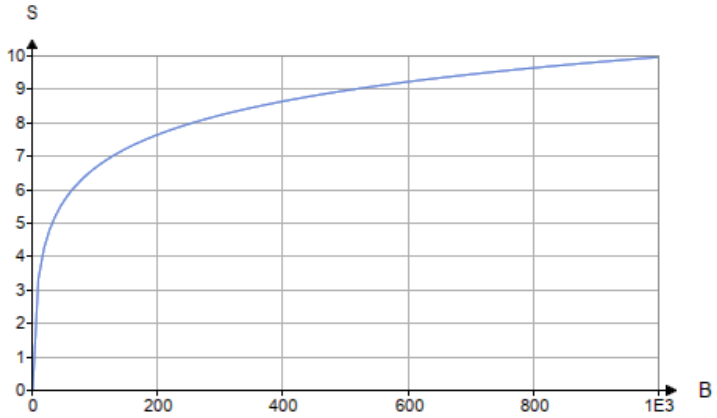


Рисунок 1.9 – График зависимости структурной скрытности ШПС M-последовательностей S_M от базы B

Анализ рисунка 1.9 показывает, что M-последовательностей обладают низкой структурной скрытностью, которая значительно ниже $S_{\text{треб.}} \geq 43$ ДИЗ.

Проведем расчеты показателя структурной скрытности для известных ансамблей ортогональных кодовых последовательностей, которые используются или могут использоваться в качестве короткого кода.

Рассмотрим наиболее широко используемые в настоящее время ансамбли ортогональных кодовых последовательностей Уолша с длиной L =128 или L =256 символов. Известно из [35], что для ШПС, в качестве которых в данном случае выступают последовательности Уолша структурная скрытность может быть определена по следующей формуле

$$S_{\text{Уолша}}(B) = \log_2 B, \tag{1.6}$$

где B является базой последовательностей Уолша.

График зависимости структурной скрытности последовательностей Уолша $S_{\text{Уолша}}$ от базы B имеет следующий вид (рисунок 1.10).

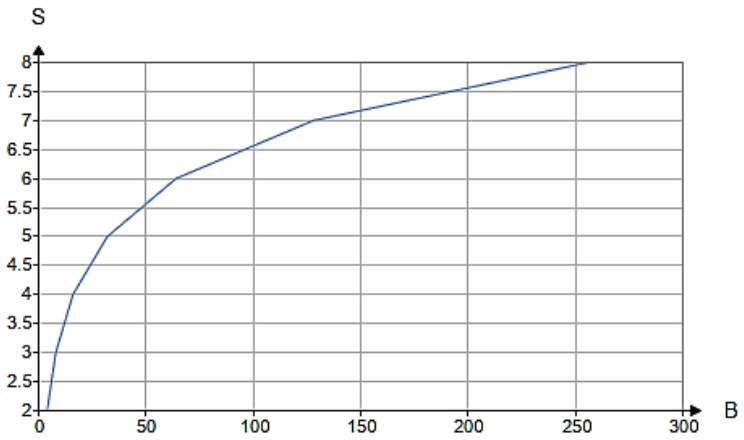


Рисунок 1.10 – График зависимости структурной скрытности последовательностей Уолша $S_{\text{Уолша}}$ от базы B

Анализ результатов расчетов показывает, что последовательности Уолша обладают низкой структурной скрытностью, которая значительно ниже $S_{\text{треб.}} \geq 43$ ДИЗ.

Таким образом, анализ значения структурной скрытности используемых в ССС с КРК Globalstar ортогональных кодовых последовательностей Уолша и псевдослучайных последовательностей Голда и M-последовательностей имеют низкую структурную скрытность, поскольку не удовлетворяют требуемому показателю структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ.

С учетом проведенного анализа структурной скрытности используемых в ССС с КРК ортогональных кодовых последовательностей выявлено **противоречие в практике**, которое заключается в том, что используемые в настоящее время в ССС с КРК ортогональные кодовые последовательности не позволяют обеспечить требуемый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ, достаточный для противодействия угрозе подмены сообщений.

1.4 Исследование известных методов построения ортогональных кодовых последовательностей по показателю структурной скрытности

В связи с тем, что используемые в настоящее время в ССС с КРК ортогональные кодовые последовательности не обеспечивают требуемое значение показателя структурной скрытности, существует необходимость проведения исследования известных методов построения ортогональных кодовых последовательностей по показателю структурной скрытности. В случае, если известные методы позволят получить последовательности с показателем структурной скрытности более 43 ДИЗ при длинах последовательностей равных L=128 и L=256, можно предположить их стохастическое применение в ССС с КРК для обеспечения защиты информации.

Проведем анализ известных методов построения ортогональных кодовых последовательностей по показателю структурной скрытности для выявления возможности их применения в ССС с КРК.

С учетом мнения авторов L. Schiff, A. Chockalingam, А.З. Айтмагамбетова, также с учетом данных, представленных в рекомендациях Международного союза электросвязи (МСЭ) [32, 39, 50] «Подвижная спутниковая служба, спутниковая служба радиоопределения, любительская спутниковая служба и относящиеся к ним спутниковые службы» МСЭ-R M.1850 длина кода L Уолша-Адамара используемого в ССС с КРК, имеет два значения L=128 и L=256 (битов, чипов). С учетом этого обстоятельства рассчитаем значение структурной скрытности известных АОКП и проведем их сравнительный анализ при длине кода L=128 и L=256 [142].

По мнению ряда авторов [32, 35, 37, 54], в том числе Л.Е. Варакина, длина кодовой последовательности и база сигналов, построенных на их основе, могут отождествляться. Поскольку для расчета показателя структурной скрытности

различных последовательностей используется понятие базы сигнала, то будем отождествлять понятия длины кодовой последовательности L и базы сигнала B.

В этой связи проведем анализ показателя структурной скрытности для рассматриваемых последовательностей на предмет их соответствия указанному требованию.

Анализ источников [35, 37, 48, 52] показывает, что в ССС с КРК кроме ортогональных функций Уолша-Адамара, могут использоваться в качестве расширяющих последовательностей сигналы с линейной частотной модуляцией, импульсные последовательности на основе реализации шума, последовательности ПСХП-1, ПСХП-2, ПСХП-3, производные АОКП, АДОМУС, другие.

Сигналы с линейной частотной модуляцией (ЛЧМ) получают при формировании аналогового ШПС с помощью частотной модуляции по линейному закону гармонической несущей с частотой f_0 [55].

Сигналы с ЛЧМ используются в радиолокации, защищенной связи, наблюдении в плотных средах (геолокация), медицине и гидролокации [49].

ЛЧМ-сигналы подходят для каналов с низким отношением мощности сигнала к мощности шума и для точного измерения параметров объектов, которые ими облучаются.

Скрытность ШПС с ЛЧМ определяется по формуле [35]

$$S_{\text{ЛЧМ}} = log_2 FT, \tag{1.7}$$

что соответствует скрытности узкополосных сигналов.

График зависимости структурной скрытности ШПС ЛЧМ $S_{\text{ЛЧМ}}$ от базы B имеет следующий вид (рисунок 1.11).

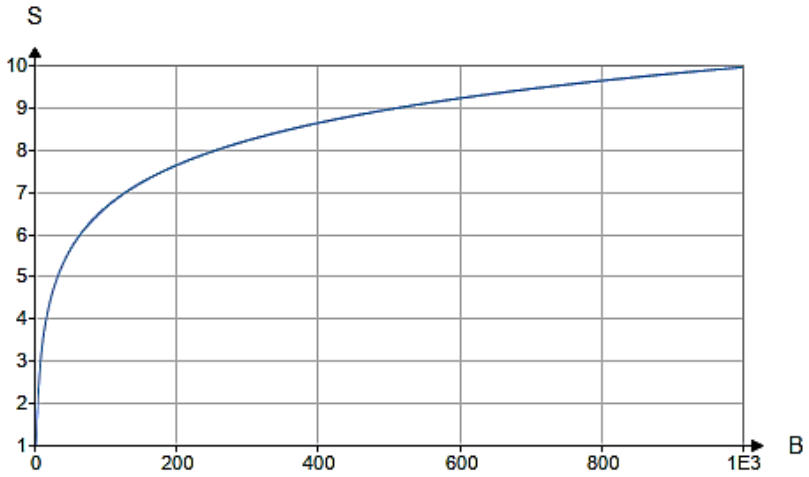


Рисунок 1.11 – График зависимости структурной скрытности ШПС ЛЧМ $S_{ЛЧМ}$ от базы B

Рассмотрим скрытность квантованной реализации случайного процесса, которая определяется следующей формулой [35]

$$S_{Ш} = FT \cdot log_2\left(2\pi e \frac{\sigma_E^2}{(\Delta e)^2}\right) = B \cdot log_2\left(2\pi e \frac{\sigma_E^2}{(\Delta e)^2}\right). \quad (1.8)$$

График зависимости структурной скрытности многопозиционной импульсной последовательности на основе реализации шума $S_{Ш}$ от базы B имеет следующий вид (рисунок 1.12).

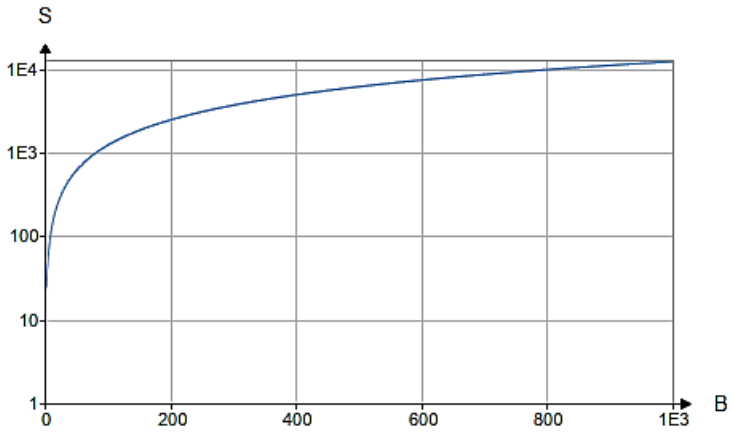


Рисунок 1.12 – График зависимости структурной скрытности многопозиционной импульсной последовательности на основе реализации шума $S_{Ш}$ от базы B

В работе Е.М. Сухарева [52] для повышения структурной скрытности в СПИ с КРК предложено использовать псевдослучайные хаотические последовательности (ПСХП). В работе Е.М. Сухарева рассматривается три вида ПСХП [52].

Проведем расчеты показателя структурной скрытности для последовательностей ПСХП-1, ПСХП-2 и ПСХП-3. Известно из [35], что для ШПС, в качестве которых в данном случае выступают последовательности ПСХП-1, ПСХП-2 и ПСХП-3 структурная скрытность может быть определена следующим образом.

ПСХП-1 основана на описании хаотического поведения нелинейной динамической системы логистическим правилом на основе квадратической параболы [52]

$$x_{n+1} = rx_n(1 - x_n), \tag{1.9}$$

где r – параметр бифуркации, x_n, x_{n+1} - текущее и последующее состояние системы.

Арсенал последовательности ПСХП-1 описывается следующей формулой [52]

$$A = 0{,}9B^{1,2}. \tag{1.10}$$

Структурная скрытность ПСХП-1 рассчитывается по формуле [52]

$$log_2 A = log_2(0{,}9B^{1,2}). \tag{1.11}$$

ПСХП-2 описывается хаотическим поведением нелинейной динамической системы логистическим правилом на основе кубической параболы [52]

$$x_{n+1} = rx_n(1 - x_n^2). \quad (1.12)$$

Значения начального условия и параметра бифуркации выбирают из диапазонов $0 < x_0 < 1{,}16$, $2{,}7 < r < 3{,}0$.

Арсенал последовательности ПСХП-2 описывается следующей формулой [52]

$$A = 1{,}05B^{1{,}02}. \quad (1.13)$$

Структурная скрытность ПСХП-2 рассчитывается по формуле [52]

$$log_2 A = log_2(1{,}05B^{1{,}02}). \quad (1.14)$$

ПСХП-3 описывается хаотическим поведением нелинейной динамической системы логистическим правилом на основе преобразования Tent Map [52]

$$x_{n+1} = 0{,}5 - 2x_n, x_n \geq 0;\ x_{n+1} = 0{,}5 + 1{,}8x_n, x_n < 0\,. \quad (1.15)$$

Арсенал последовательности ПСХП-3 описывается следующей формулой [52]

$$A = 0{,}1B^{1{,}7}. \quad (1.16)$$

Структурная скрытность ПСХП-3 рассчитывается по формуле [52]

$$Log_2 A = Log_2(0{,}1B^{1{,}7}). \quad (1.17)$$

В этой же работе описаны характеристики ПСХП и их корреляционно-структурные свойства.

График зависимости структурной скрытности последовательностей ПСХП-1 $S_{\text{ПСХП}-1}$, ПСХП-2 $S_{\text{ПСХП}-2}$ и ПСХП-3 $S_{\text{ПСХП}-3}$от базы B имеет следующий вид (рисунок 1.13).

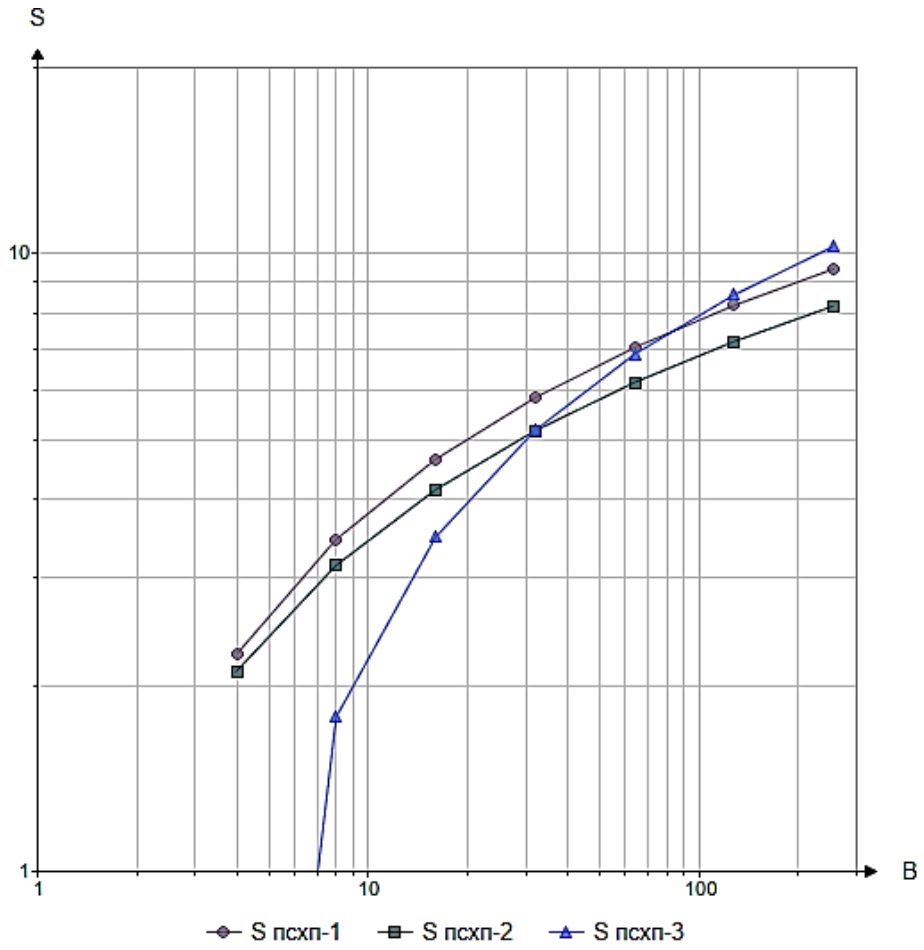


Рисунок 1.13 – График зависимости структурной скрытности последовательностей ПСХП-1 $S_{\text{ПСХП}-1}$, ПСХП-2 $S_{\text{ПСХП}-2}$ и ПСХП-3 $S_{\text{ПСХП}-3}$ от базы B

В силу того, что рассматриваемые ПСХП имеют приемлемые автокорреляционные и взаимокорреляционные свойства, они могут использоваться в СПИ с КРК.

В работах [9, 10, 13, 18, 54]. отмечено, что производный ансамбль ортогональных кодовых последовательностей получается путем посимвольного (поэлементного) перемножения каждой его последовательности на выбранную по

определенным критериям производящую кодовую последовательность. В качестве исходного очень часто используют ансамбль кодовых последовательностей Уолша, а в качестве производящего кодовую последовательность, как правило, имеющую хорошую функцию автокорреляции с количеством элементов, равным количеству элементов исходных последовательностей.

Среди известных производных ансамблей ортогональных кодовых последовательностей являются ансамбли Рида-Мюллера, Сандерса, Джеффи, Стиффлера, Л.Е. Варакина и др., которые подробно описаны в [9, 10, 13, 18, 54].

Структурная скрытность ансамблей ортогональных кодовых последовательностей будет зависеть от базы кодовых последовательностей, поэтому для определения ее значения воспользуемся следующим выражением для определения структурной скрытности ШПС, известным из [35]

$$S_{\text{Пр.}}(B) = \log_2 B, \tag{1.18}$$

График зависимости структурной скрытности производного ансамбля АОКП $S_{\text{Пр.}}$ имеет следующий вид (рисунок 1.14).

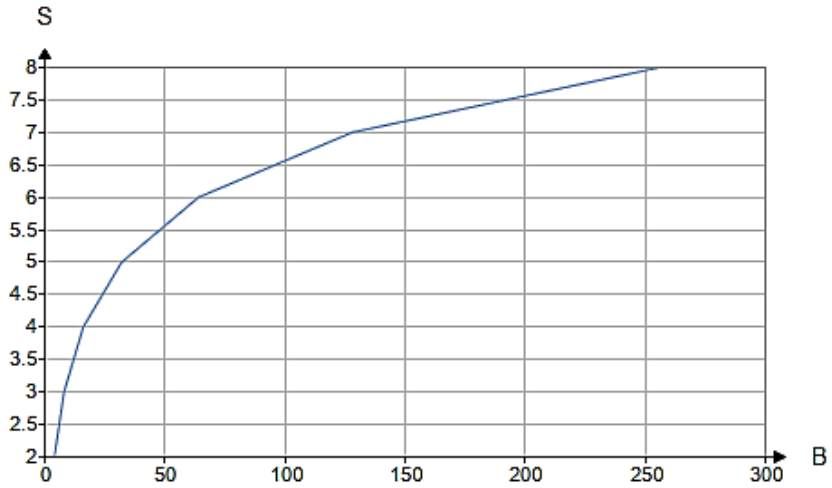


Рисунок 1.14 – График зависимости структурной скрытности производного ансамбля АОКП $S_{\text{Пр.}}$ от базы B

В работе З.В. Черняка предложен метод повышения скрытности СПИ с КРК на основе стохастического применения АДОМУС [57]. Описанный метод базируется на использовании ансамблей ортогональных кодовых последовательностей, которые относятся к классу многопозиционных, поскольку они являются многоуровневыми.

Поскольку в работе представлены расчеты количества сигналов только для размерностей $N = 4, 8, 16, 32$ и 64, а в данном случае нас интересуют размерности L=128 и L=256, то проведем расчеты количества ансамблей и показателя структурной скрытности для ансамблей дискретных ортогональных многоуровневых сигналов с учетом аппроксимации представленных в диссертации З.В. Черняка зависимостей количества получаемых ансамблей сигналов в зависимости от их размерности до требуемых размерностей L=128 и L=256.

Структурная скрытность $S_{\text{АДОМУС}}$ рассчитывается по формуле [57]

$$S_Q = \log_2 M \cdot 2^{N-1} = (N-1) \cdot \log_2 M, \qquad (1.19)$$

где M – количество различных наборов значений амплитуд, N – порядок используемой матрицы.

В соответствии с [57] количество ансамблей $Q_{\text{АДОМУС}}$ и структурную скрытность $S_{\text{АДОМУС}}$ для порядков $N = 4, 8, 16, 32, 64, 128, 256$ приведем в таблице 1.5

Таблица 1.5 – Количество ансамблей $Q_{\text{АДОМУС}}$ и структурная скрытность $S_{\text{АДОМУС}}$

Порядок матрицы, N	Количество АДОМУС, Q	Структурная скрытность АДОМУС, $S_{\text{АДОМУС}}$
4	$2{,}02 \cdot 10^{3}$	10,98
8	$2{,}51 \cdot 10^{8}$	27,90
16	$3{,}85 \cdot 10^{18}$	61,74
32	$9{,}11 \cdot 10^{38}$	129,42
64	$5{,}10 \cdot 10^{79}$	264,78
128	$1{,}59 \cdot 10^{161}$	535,50
256	$1{,}62 \cdot 10^{324}$	1077

График зависимости структурной скрытности АДОМУС имеет следующий вид (рисунок 1.15).

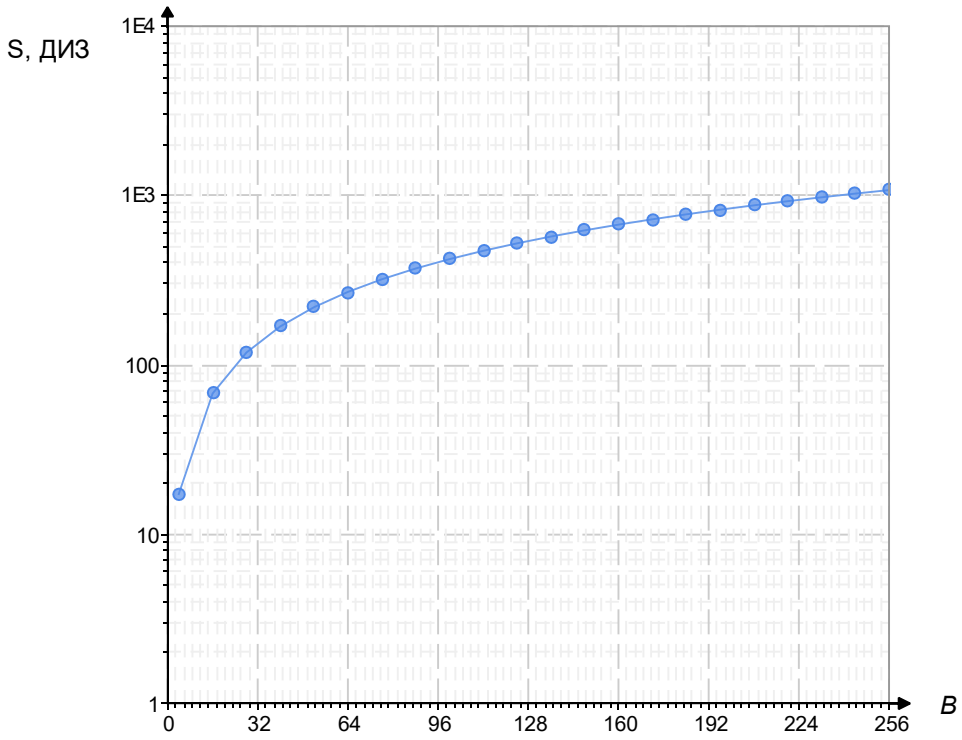


Рисунок 1.15 – График зависимости структурной скрытности АДОМУС $S_{\text{АДОМУС}}$ от базы B

На рисунке 1.16 приведены зависимости структурной скрытности S от базы B последовательностей квантованной реализации случайного процесса $S_{\text{Ш}}$, производные АОКП $S_{\text{Пр.}}$, ансамблей дискретных ортогональных многоуровневых сигналов $S_{\text{АДОМУС}}$, ансамблей с линейной частотной модуляцией $S_{\text{ЛЧМ}}$, последовательностей ПСХП-1 $S_{\text{ПСХП}-1}$, ПСХП-2 $S_{\text{ПСХП}-2}$ и ПСХП-3 $S_{\text{ПСХП}-3}$, последовательностей Уолша $S_{\text{Уолша}}$.

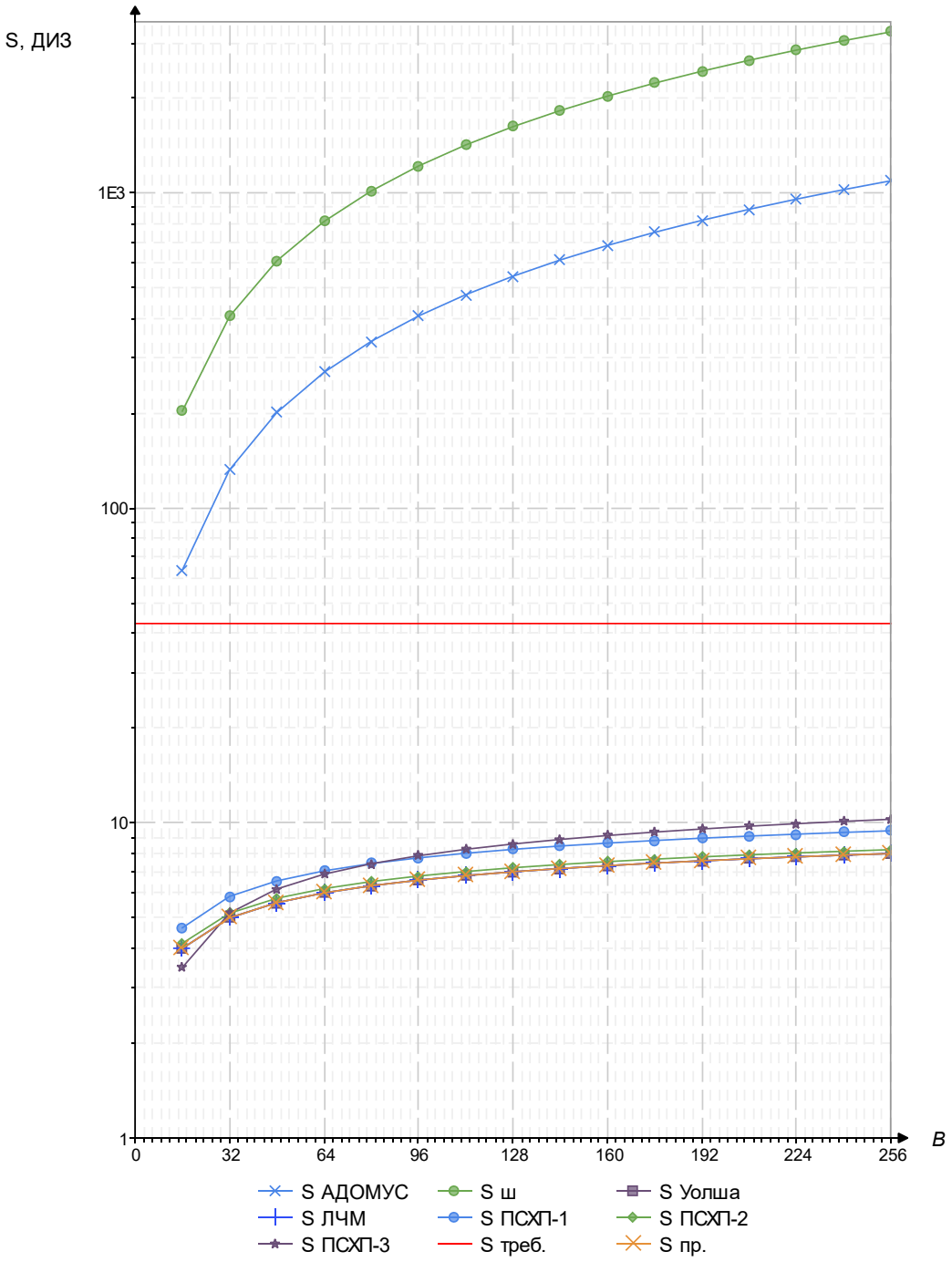


Рисунок 1.16 – Сравнительный анализ графиков зависимости структурной скрытности S известных ортогональных кодовых последовательностей от базы сигнала B

Сравнительный анализ графиков зависимости структурной скрытности S известных ШПС от базы B, представленных на рисунке 1.19 показывает, что:

- скрытность сигналов, получаемых на базе последовательностей Уолша $S_{\text{Уолша}}$, ПСХП-1 $S_{\text{ПСХП}-1}$, ПСХП-2 $S_{\text{ПСХП}-2}$, ПСХП-3 $S_{\text{ПСХП}-3}$, ЛЧМ $S_{\text{ЛЧМ}}$ при увеличении базы сигнала находится значительно ниже целевого показателя $S_{\text{треб.}} \geq 43$ ДИЗ для 128 и 256 элементных последовательностей;

- скрытность многопозиционных АДОМУС $S_{\text{АДОМУС}}$ при базе сигнала $B > 128$ достигает целевого показателя $S_{\text{треб.}} \geq 43$ ДИЗ при базе сигнала $B > 10$. Отметим, что многопозиционные АДОМУС использоваться в ССС с КРК не могут, поскольку они являются многоуровневыми и обладают низкой помехоустойчивостью, что неприемлемо для спутниковых радиолиний;

- скрытность многопозиционной импульсной последовательности на основе реализации шума при базе сигнала $B > 4$ находится выше целевого показателя $S_{\text{треб.}} \geq 43$ ДИЗ, которая растет при увеличении длины последовательности. Однако практическая реализация информационного обмена на базе случайного процесса затруднительна, ввиду невозможности обеспечения устойчивой синхронизации приемной и передающей частей аппаратуры, поскольку соседние по времени отсчеты такого сигнала статистически независимы. Также существует сложность идентичной генерации кодовых последовательностей в цифровом виде на основе аналогового шумового процесса на приемной и передающей сторонах.

Таким образом, исследованные известные методы синтеза ансамблей ортогональных кодовых последовательностей по показателю структурной скрытности не позволяют обеспечить требуемое значение структурной скрытности ССС с КРК $S_{\text{треб.}} \geq 43$ ДИЗ, либо не могут быть применены в ССС с КРК в качестве расширяющих последовательностей по причине ограничений на их использование, и тем самым не обеспечивают разрешение выявленного ранее противоречия в практике.

В связи с этим выявлено **противоречие в теории**, заключающееся в том, что известные методы синтеза не позволяют получить АОКП в количестве, обеспечивающем требуемое значение их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ при их стохастическом применении в ССС с КРК.

Следует отметить, что в соответствии с рисунком 1.19 структурная скрытность рассмотренных двоичных кодовых последовательностей существенно ниже структурной скрытности известных многопозиционных последовательностей (АДОМУС и последовательностей на основе реализации шума), поэтому многопозиционные последовательности в этом плане имеют преимущество.

В работе Быховского М.А. [58] показана целесообразность применения многомерных (многозначных) последовательностей в ССС, которые по сравнению с двоичными последовательностями имеют большее количество сменных параметров. При этом отмечается, что по своим характеристикам ССС, использующие многомерные последовательности существенно превосходят аналогичные системы с двоичными последовательностями. Поэтому можно предположить, что многопозиционные последовательности имеют большее количество сменяемых параметров по сравнению с двоичными, а следовательно, большую арсенальную и структурную скрытности.

Как полагает автор, максимального повышения структурной скрытности в системах с кодовым разделением каналов можно достичь за счёт стохастического использования ансамблей многопозиционных ортогональных кодов, получаемых методом векторного синтеза.

В работе показано, что в ССС с КРК для увеличения количества сменяемых параметров сигналов и повышения их структурной скрытности целесообразно рассматривать ансамбли многофазных ортогональных кодовых последовательностей. Стохастическое применение АМФОКП в ССС с КРК осуществимо, поскольку на их основе возможно легко реализовать информационный обмен в линиях вверх и вниз, используя применяемые в настоящее время такие виды модуляции, как QPSK, 16-QAM.

Следовательно, обоснована необходимость разработки усовершенствованного метода векторного синтеза для получения АМФОКП, обеспечивающих достижение ими целевого показателя структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ, как одного из наиболее перспективных подходов противодействия угрозе подмены сообщений.

В связи с этим, **предметом исследования** является метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов.

В данной работе автором предлагается для решения задачи противодействия угрозе подмены сообщений в рассматриваемых системах связи разработать метод противодействия угрозе подмены сообщений для ССС с КРК на основе стохастического применения ансамблей ортогональных кодовых последовательностей.

Из этого следует, что **научная задача исследования** заключается в разработке метода противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения АМФОКП.

В [137] под понятием «метод» понимается «способ, порядок, основания; принятый путь для хода, достижения чего-либо, в виде общих правил».

Для решения поставленной задачи требуется разработать метод противодействия угрозе подмены сообщений в системе спутниковой связи с кодовым разделением каналов, который предполагает получение и случайное использование АМФОКП и включает в себя:

- модель противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП;

- модель АМФОКП и алгоритм их синтеза для стохастического применения в ССС с КРК, обеспечивающие требуемый уровень их структурной скрытности;

- разработку принципа и технического решения по противодействию угрозе подмены сообщений в ССС с КРК.

Анализ возможных подходов к решению научной задачи показал целесообразность ее декомпозиции **основные задачи исследования**:

1. Разработать модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП размерностей $N = 128, 256$.

2. Разработать модель и алгоритм синтеза АМФОКП размерностей $N = 128, 256$, в количестве, обеспечивающем при их стохастическом применении в ССС с КРК требуемый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ.

3. Разработать принцип построения и техническое решение стохастического средства защиты информации для ССС с КРК.

1.5 Выводы по главе

1. Проведенный анализ показал, что ССС с множественным доступом и КРК имеют преимущества по сравнению с ССС с другими видами множественного доступа по эффективности использования частотного диапазона, меньшего уровня канальных помех, меньших габаритов спутниковых антенн и повышенной пропускной способности, поэтому в данной диссертационной работе система спутниковой связи с кодовым разделением каналов выбрана в качестве **объекта исследования**.

2. Анализ существующих угроз ССС показывает, что они подразделяются на физические угрозы, электронные угрозы телекоммуникационной системе и кибернетические угрозы (киберугрозы). Электронные угрозы ССС наиболее доступны для реализации злоумышленниками и направлены на линии и сигналы ССС с целью подавления (глушения) линий, подслушивания и подмены сообщений в линиях спутниковой связи.

3. Угроза подмены сообщений можно отнести к угрозе, реализуемой злоумышленниками с высокой степенью вероятности в силу простоты ее реализации и отсутствием необходимости выделения существенных материальных

затрат на ее реализацию. Поэтому в данной диссертационной работе основное внимание уделяется противодействию угрозе подмены сообщений в ССС с КРК.

4. Известно, что способность ССС с КРК противостоять навязыванию ложного сообщения, его подмене или изменению хранимых данных называется имитостойкость, которая оценивается безопасным временем $T_б$. Анализ показал, что безопасное время известных ССС с КРК имеет значения $T_б = 1{,}3 - 2{,}5$ мс. Проведенный расчет показал, что в ССС с КРК Globalstar при передаче пакета данных потребуется время, равное $T_{\text{сообщ.}} = 15$ мс. Исходя из этого сделан вывод о недостаточности показателя безопасное время у существующих ССС с КРК у которых в качестве расширяющих последовательностей используются последовательности Уолша.

5. Обоснована целесообразность решения вопроса повышения защищенности информации в ССС с КРК за счет применения увеличенного количества ансамблей ортогональных кодовых последовательностей с изменяющейся структурой.

6. Для численной оценки показателя структурной скрытности в данном разделе используется подход, изложенный в [37], зависящий от арсенала возможных сменяемых параметров кодовой последовательности, определяемый согласно формуле 1.4. В данном разделе определена минимально-допустимая структурная скрытность, которую должны обеспечивать применяемые в ССС с КРК АМФОКП $S_{\text{треб.}} \geq 43$ ДИЗ с учетом обеспечения непрерывного информационного в течение среднего времени эксплуатации спутника в течение 15 лет неповторяющимися структурами кодовых последовательностей.

7. С учетом проведенного анализа структурной скрытности, обеспечиваемой, используемыми в ССС с КРК ортогональными кодовыми последовательностями выявлено **противоречие в практике**, которое заключается в том, что используемые в настоящее время в ССС с КРК ортогональные кодовые последовательности не позволяют обеспечить требуемый уровень их структурной

скрытности $S_{\text{треб.}} \geq 43$ ДИЗ, достаточный для противодействия угрозе подмены сообщений.

8. Возможности известных методов синтеза ансамблей ортогональных последовательностей и последующего их применения не позволяют получить ансамбли ортогональных кодовых последовательностей в требуемом количестве $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$.

9. Анализ известных методов синтеза ансамблей ортогональных кодовых последовательностей по показателю структурной скрытности позволил выявить **противоречие в теории**, заключающееся в том, что известные методы синтеза не позволяют получить АОКП в количестве, обеспечивающем требуемое значение их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ при их стохастическом применении в ССС с КРК.

10. Наиболее эффективное повышение структурной скрытности АОКП, описываемых собственными векторами ЭМ, предполагает их стохастическое применение в ССС с КРК. Этот подход предполагает генерацию достаточного количества последовательностей с приемлемыми корреляционными характеристиками, что необходимо для их практического стохастического использования.

В связи с этим определены **основные задачи исследования**, решаемые в данной работе:

1. Разработать модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП размерностей $N = 128, 256$.

2. Разработать модель и алгоритм синтеза АМФОКП размерностей $N = 128, 256$, в количестве, обеспечивающем при их стохастическом применении в ССС с КРК требуемый уровень структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ.

3. Разработать принцип построения и техническое решение стохастического средства защиты информации для ССС с КРК.

2 РАЗРАБОТКА МОДЕЛИ ПРОТИВОДЕЙСТВИЯ УГРОЗЕ ПОДМЕНЫ СООБЩЕНИЙ В СИСТЕМЕ СПУТНИКОВОЙ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

2.1 Обоснование необходимости стохастического применения псевдослучайных ортогональных кодовых последовательностей для противодействия угрозе подмены сообщений в системе спутниковой связи с кодовым разделением каналов

Рассмотрим концепцию защиты информации на основе повышения структурной скрытности при использовании стохастических кодов, рассмотренную такими авторами, как Варакин Л.Е., Осмоловский С.А., Сухарев Е.М., Воронин Е.И., Кандауров Н.А., Черняк З.В., Быховский М.А. и другими.

В работе [53] рассматривается следующая структура участников информационного процесса:

– источники сообщения,

– получатели сообщения;

– телекоммуникационная сеть;

– злоумышленник, реализующий одну или несколько своих стратегий для противодействия информационному обмену;

– само сообщение, которое должно быть доставлено от источника к его получателю за установленное время [53].

Структура участников информационного процесса представлена на рисунке 2.1.

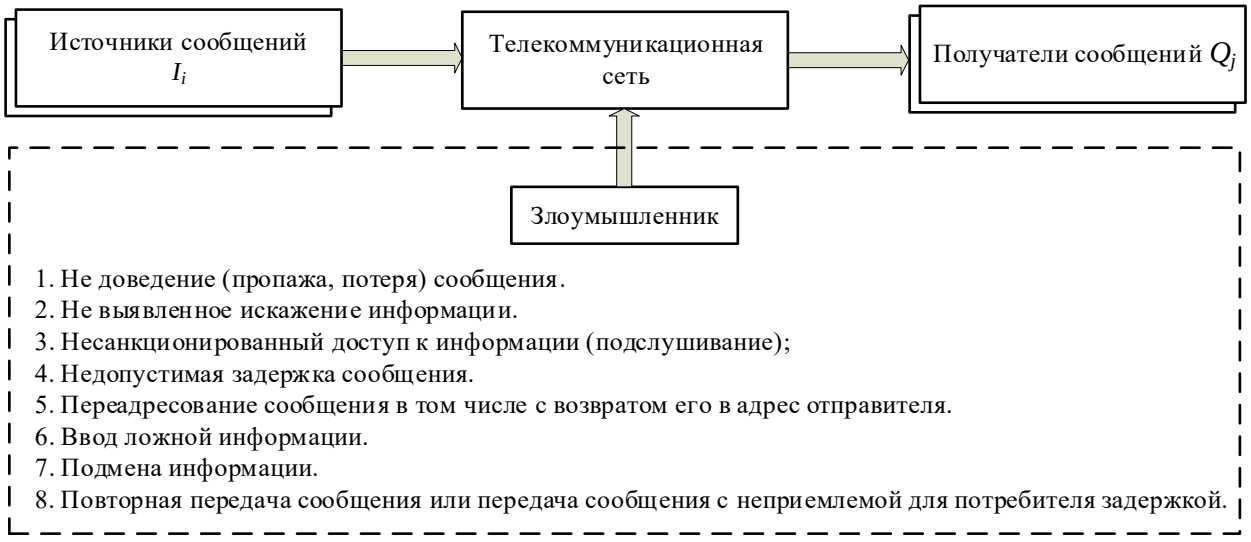


Рисунок 2.1 – Структура участников информационного процесса

Целью отправителя и получателя сообщений является устойчивый, достоверный и конфиденциальный информационный обмен.

В исследовании под номером [53] автор обозначил ключевые угрозы информационной безопасности, характерные для рассматриваемой структуры. Среди них выделяются: утрата или потеря сообщений, необнаруженные искажения данных, несанкционированный доступ к информации (включая перехват), неприемлемые задержки при доставке сообщений, их перенаправление (в том числе возврат отправителю), внедрение ложных сведений, подмена содержимого, повторная отправка сообщений или их передача с задержкой, критичной для получателя.

Поэтому целью злоумышленника в информационном процессе в зависимости от выбранной стратегии может быть ознакомление с содержанием передаваемых отправителем сообщений (нарушение конфиденциальности сообщения), препятствование процессу информационного обмена между отправителем и получателем сообщений (подавление, искажение, задержка и др.), подмена передаваемых сообщений и прочие деструктивные воздействия.

Применительно к ССС с КРК, рассматриваемым в данной диссертационной работе, ранее было установлено, что для них характерными из всех вышеперечисленных угроз безопасности информации является угроза подмены

сообщений. Поэтому вопросы защиты информации в ССС с КРК, решаемые в данной работе, учитывают противодействие угрозе подмены сообщений.

В классической формулировке Клода Шеннона проблема защиты информации рассматривается как обеспечение передачи данных с устойчивостью к помехам, гарантируя при этом заданную точность и конфиденциальность [62, 63]. С учетом этого в данной работе предлагается использовать ортогональные кодовые последовательности, формируемые на основе принципа случайности, что позволяет повысить помехоустойчивость и безопасность коммуникации.

В работах Клода Шеннона [62, 63] показано, что абсолютная секретность системы может быть обеспечена при выполнении следующих условий:

– каждое сообщение M связывается с каждым значением криптограммы E только одной линией;

– все ключи равновероятны.

Теория использования случайного кодирования Клода Шеннона в дальнейшем получила практическую реализацию в работах Финка Л.М., Мухаметшина С.А., Осмоловского С.А. и др. Решение задачи сводилась к технической реализации случайного кодирования [53, 64, 65].

С.А. Осмоловским решена задача синтеза помехоустойчивого кода и его стохастического применения для дискретного канала связи [53, 144]. При этом используется помехоустойчивый код, обеспечивающий требуемую достоверность передачи информации, а случайность выбора разрешенных к использованию кодовых последовательностей обеспечивает защиту информации от угроз.

Согласно исследованиям Осмоловского С.А., стохастическое кодирование представляет собой метод, сочетающий адаптивное преобразование данных, добавление избыточности и временную зависимость преобразований. Такая комбинация обеспечивает универсальную защиту информации от различных видов вмешательства [53, 144].

С.А. Осмоловский выделяет ключевые этапы реализации этого метода с коррекцией ошибок:

Кодирование и декодирование — процессы, включающие введение и последующее устранение избыточных данных.

Прямое F и обратное F^{-1} стохастические преобразования, выполняемые с использованием квазислучайных чисел, генерируемых специальным датчиком.

Иллюстрация метода стохастического кодирования с исправлением ошибок, предложенного Осмоловским С.А., представлена на рисунке 2.1.

Система передачи информации, реализующая метод стохастического кодирования, содержит стохастический кодер на передающей стороне и стохастический декодер на приемной стороне, которые представляют из себя средства защиты информации, основанные на стохастическом применении АМФОКП. Для краткости назовем их стохастическими средствами защиты информации.

Иллюстрация метода стохастического кодирования с исправлением ошибок представлена на рисунке 2.2

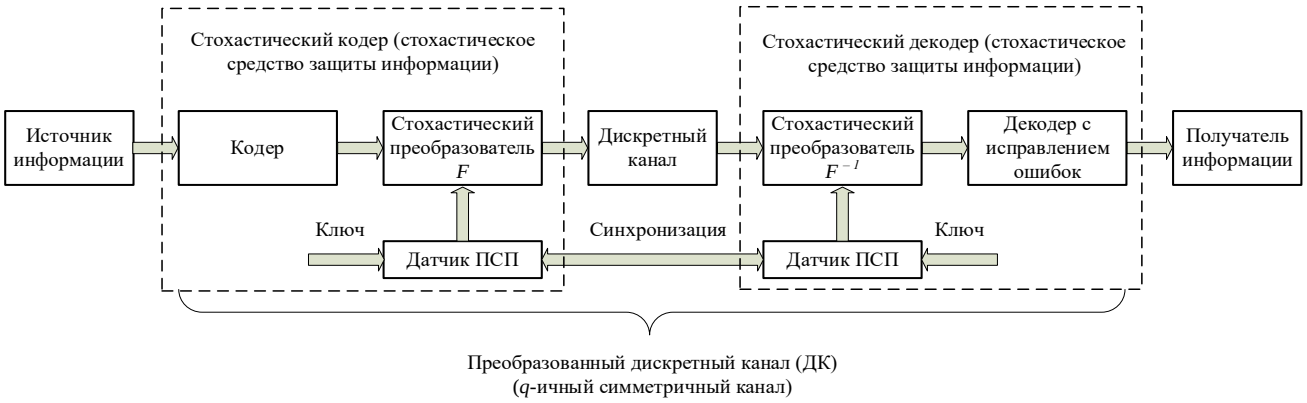


Рисунок 2.2 – Иллюстрация метода стохастического кодирования с исправлением ошибок

Отметим, что совершенствованию стохастического средства защиты информации применительно к системам спутниковой связи с кодовым разделением каналов посвящена данная работа.

Достоинством метода стохастического кодирования с исправлением ошибок является:

– возможность обеспечения гарантированной достоверности при передаче сообщений по дискретному каналу,

– возможность обеспечения требуемого уровня секретности (конфиденциальности) сообщений,

– возможность применения единого алгоритма преобразования информации в информационной системе с позиций классической постановки К. Шеннона, что упрощает выполнение операций в информационном процессе.

Отметим, что прямое и обратное стохастическое преобразование, выполняемые в каждый промежуток времени используют одинаковые и синхронно вырабатываемые параметры преобразования, что в свою очередь требует обеспечения синхронности работы датчиков последовательностей в кодере и декодере.

Осмоловский С.А. в работе [53] описывает синхронизацию как процесс установления и поддержания синхронного состояния, когда две последовательности событий происходят одновременно или с постоянным сдвигом по времени $\Delta T = const$.

При синхронизации датчиков выполняется тактовая синхронизация, кроме нее происходит синхронизация кодовых последовательностей и цикловая синхронизация датчиков.

Синхронизация кодовых последовательностей необходима для настройки декодера в приемной части на начало каждой кодовой последовательности. Синхронизация кодовых последовательностей устанавливается путем передачи синхросигналов по отдельному каналу или по каналу, где передается информация, но в режиме установления синхронизации.

Цикловая синхронизация датчиков служит для выработки синхронизированными по началу кодовых последовательностей датчиками одинаковых во времени кодовых последовательностей [53].

Существуют следующие периодические сигналы, обладающие хорошими синхронизирующими свойствами с множеством N значений (меток):

– импульс длительностью $\frac{T_0}{N}$, передаваемый каждые T_0 секунд;

– псевдошумовые последовательности максимальной длины линейного регистра сдвига с обратной связью, описываемого примитивным полиномом степени k;

– последовательности быстро входящие в синхронизм за счет наличия у них хорошей автокорреляционной функции.

В работах [31, 35, 37, 52, 53] отмечается, что средства стохастической защиты информации могут использоваться в следующих областях применения информационных систем:

- в областях использования туннелированных протоколов на различных уровнях модели ЭМВОС на сеансовом, сетевом и канальном уровнях модели, при этом стохастические методы поддерживают высокоскоростную обработку информации, одновременно решая задачи защиты информации;

- в областях, где применяются средства шифрования информации (криптографического преобразования информации). Стохастические методы обладают высокой скоростью преобразования и достаточной стойкостью ввиду использования блочного шифрования в сочетании с методом гаммирования [138, 139];

- в областях применения помехоустойчивых кодов для исправления ошибок (коды Рида-Соломона), для обнаружения ошибок (циклические коды). При использовании кодов Рида-Соломона стохастические методы позволяют обеспечить высокоскоростную обработку информации, в том числе для кодов с большим основанием q. При использовании циклических кодов стохастические методы не только обнаруживают, но и исправляют ошибки, тем самым гарантировано обеспечивают необходимый уровень вероятности ошибки при декодировании в любом канале связи, и, таким образом выполняют функцию имитозащиты при нахождении ошибок и их исправлении;

- в области создания генераторов псевдослучайных чисел для средств стохастической защиты информации с высокими статистическими и техническими характеристиками;

- в области перспективных информационных технологий, базирующихся на использовании стохастических средств защиты информации.

Также применение метода стохастического кодирования в системах коротковолновой радиосвязи описано в работах [37, 66, 67].

Для ССС с КРК применение метода стохастического кодирования, не смотря на его достоинства, не рассматривалось по ряду причин, в том числе, по причине отсутствия ансамблей ортогональных кодовых последовательностей для их стохастического использования, обеспечивающего требуемое значение структурной скрытности.

С учетом того, что в данной работе в качестве объекта исследований выступают ССС с КРК автором предлагается для решения задачи противодействия угрозе подмены сообщений в рассматриваемых системах связи разработать метод противодействия угрозе подмены сообщений для ССС с КРК на основе стохастического применения ансамблей ортогональных кодовых последовательностей.

В [137] под понятием «Метод» понимается «Способ, порядок, основания; принятый путь для хода, достижения чего-либо, в виде общих правил». В соответствии с этим понятием метод противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения АМФОКП должен содержать:

- модель противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП;

- модель АМФОКП и алгоритм их синтеза для стохастического применения в ССС с КРК, обеспечивающие требуемый уровень структурной скрытности;

- разработку принципа и технического решения по противодействию угрозе подмены сообщений в ССС с КРК.

Анализ известных подходов к повышению скрытности систем передачи информации с кодовым разделением каналов на основе стохастического применения АМФОКП показывает, что наибольшие возможности по показателю структурной скрытности имеются у способа передачи информации на основе стохастически формируемых ансамблей дискретных многоуровневых ортогональных сигналов [68]. По этой причине он выбран за основу для разработки метода противодействия угрозе подмены сообщений для ССС с КРК на основе стохастического применения АМФОКП.

2.2 Разработка модели противодействия угрозе подмены сообщений в системах спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей

Современные системы спутниковой связи должны обеспечивать конфиденциальность, целостность и доступность передаваемых сообщений. Как было установлено ранее в системе связи на примере ССС с КРК Globalstar весьма вероятным является реализация угрозы подмены сообщений, что безусловно будет нарушать их целостность [1-4].

Распространенными сервисами ССС с КРК Globalstar являются SPOT и SCADA. Сервис SPOT позволяет отслеживать местоположение и отправлять текстовые сообщения, сервис SCADA предназначен для телеметрического контроля и сбора данных.

Угроза подмены сообщений в системе связи на примере ССС с КРК Globalstar реализуется на основе осуществления следующих этапов [56]:

1. Перехват пакета данных с помощью SDR-устройства USRP B200, антенного устройства qualcomm antenna GSP-1620 1,6 ГГц, малошумящего радиочастотного усилителя Mini-Circuits (LNA) ZX60-1614LN-S, регулятора напряжения Dimension Engineering AnyVolt 3, радиочастотных кабелей, блока питания 12 V, настройка SDR-приемника на частоту и другие параметры сигнала, перехват сигнала, демодуляция сигнала.

2. Автоматическая запись перехваченного пакета в файл.

3. Анализ перехваченного пакета данных с помощью специального программного обеспечения.

4. Декодирование перехваченного пакета данных с целью определения кода расширяющей PN-последовательности, привязка к коду.

5. При помощи специального программного обеспечения ССС с КРК Globalstar SPOT Gen3 Support изменение электронного серийного номера (ESN) в SPOT или SCADA устройстве.

6. Формирование в ложном пакете данных ESN легального SPOT или SCADA устройства для формирования ложного пакета данных от его имени с использованием и передача ложного пакета данных с использованием PN-кода легального SPOT или SCADA устройства.

7. Осуществление ввода ложной информации в систему передачи данных для достижения поставленных целей.

Начальный этап перехвата сообщения легального отправителя сообщений начинается с осуществления разведки параметров ССС с КРК на основе поиска и обнаружение сигнала, измерения параметров и идентификации сигнала.

Вероятность реализации угрозы подмены сообщений будет тем успешнее, чем будет меньше скрытность передаваемых сигналов.

С учетом сказанного вероятность подмены сообщений $P_{\text{подм.}}$ можно выразить как функцию от вероятности разведки структуры сообщения $P_{\text{разв.}}$, при принятых допущениях.

$$P_{\text{подм.}} = f\left(P_{\text{разв.}}\right). \quad (2.1)$$

Скрытность структуры передаваемых сообщений обеспечивается за счет комплекса технических и организационных мер и скрытности используемых сигналов, которую разделяют на энергетическую, структурную и информационную.

В работах [10, 36, 136] представлена формула, позволяющая определить вероятность разведки структуры сигнала, которая имеет следующий вид:

$$P_{\text{разв.}} = P_{\text{обн.}} \cdot P_{\text{стр.}} \cdot P_{\text{инф.}}, \quad (2.2)$$

где $P_{\text{обн.}}$ – вероятность правильного обнаружения сигнала радиоэлектронного средства, которое зависит от его энергетической скрытности, $P_{\text{стр.}}$ – вероятность раскрытия структуры сигнала при условии его обнаружения, $P_{\text{инф.}}$ – вероятность раскрытия смысла передаваемой информации.

Структурная скрытность сигнала зависит от алгоритма кодирования и используемого вида модуляции [36, 37]. Вероятность раскрытия структуры сигнала $P_{\text{стр.}}$ при условии его обнаружения может выступать в качестве показателя для оценки структурной скрытности. В [35] показано, что потенциальная структурная скрытность S определяется по формуле (1.4) и зависит от количества сменяемых параметров сигнала.

Энергетическая скрытность определяет возможность противодействовать обнаружению сигнала противоборствующей стороной, которая зависит от ширины спектра ШПС, поскольку чем шире спектр ШПС, тем больше время анализа сигнала [52].

Для выявления сигнала обычно применяется энергетический детектор, который позволяет зафиксировать излучение на данной частоте. Также для решения данной задачи могут быть использованы автокорреляционный и циклостационарный обнаружители, описанные в [37, 59-61]. Для выявления сигналов с технологией

прямого расширения спектра в условиях низкого соотношения сигнал/шум злоумышленнику требуется информация о следующих параметрах: длина псевдослучайной последовательности (ПСП), используемый тип модуляции, скорость передачи данных и чиповая скорость (частота элементов ПСП), ширина занимаемой полосы частот, значение несущей частоты, а также статистические характеристики сигнала и шумовых помех [37].

Информационная скрытность характеризуется способностью противодействовать методам радиотехнической разведки, направленным на выявление смысла передаваемых данных [57, 141].

После обнаружения сигнала в радиолинии злоумышленник реализует перехват информации. Перехват основан на демодуляции обнаруженного сигнала.

Анализ основных этапов разработанной модели угроз подмены сообщений ССС с КРК Globalstar показывает, что частота канала спутниковой связи, на которой осуществляется информационный обмен с помощью терминальных устройств SPOT Satellite Messengers и модема дистанционного мониторинга и телеметрии, контроля и сбора данных (SCADA) GSP-1620 широко известна злоумышленнику. Также злоумышленнику известно техническое устройство приема и передачи спутникового сигнала (в составе SDR-устройства USRP B200, антенного устройства qualcomm antenna GSP-1620 1618 МГц в канале вверх и 2492 МГц в канале вниз, малошумящего радиочастотного усилителя Mini-Circuits (LNA) ZX60-1614LN-S и др.) для приема и передачи пакета данных по спутниковому каналу. Известным является и тот факт, что передаваемые сообщения передаются в открытом незашифрованном виде и имеют следующую структуру (рисунок 2.3).

С учетом данных обстоятельств можно сделать вывод, что для ССС с КРК Globalstar $P_{\text{обн.}} \to 1$, $P_{\text{стр.}} \to 1$, $P_{\text{инф.}} \to 1$, а с учетом формулы (2.2) в целом вероятность разведки структуры сигнала $P_{\text{разв.}}$ также будет стремиться к единице, что предопределяет реализацию угрозы подмены сообщений как вероятную.

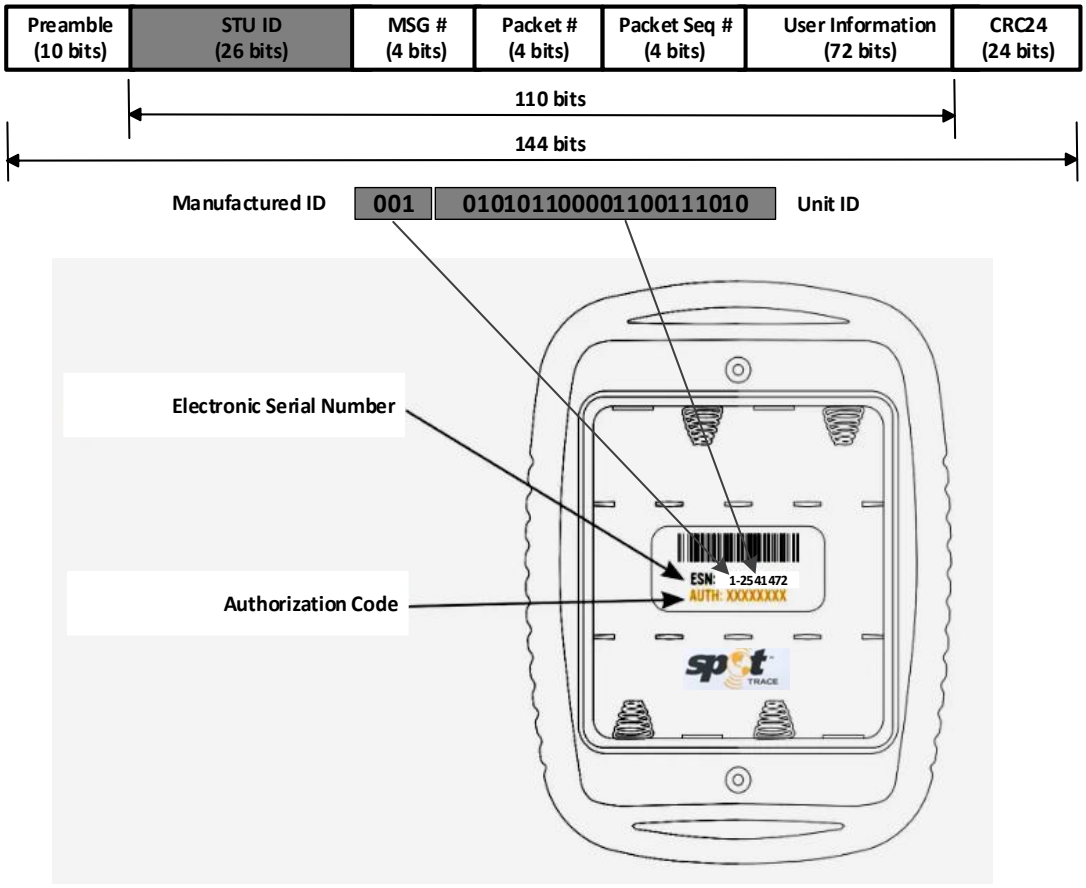


Рисунок 2.3 – Структура передаваемых сообщений ССС с КРК Globalstar

Снизить $P_{\text{обн.}}$ – вероятность правильного обнаружения сигнала радиоэлектронного средства можно на основе использования метода информационного обмена с повышенной энергетической скрытностью. Снизить $P_{\text{инф.}}$ – вероятность раскрытия смысла передаваемой информации можно лишь на основе применения криптографических средств защиты информации. Однако реализация этих мероприятий потребует полной замены терминальных устройств и оборудования спутниковой связи, что будет очень затратным с финансовой точки зрения и трудно реализуемым на практике.

Для реализации подмены сообщений злоумышленнику должна быть известна структура используемых сигналов. В противном случае злоумышленник не сможет реализовать угрозу подмены сообщений. На основании формулы (2.2) можно сделать вывод, что снижение вероятности разведки структуры сигнала $P_{\text{разв.}}$ может

быть обеспечено за счет снижения вероятности раскрытия структуры сигнала при условии его обнаружения $P_{\text{стр.}}$.

Если форма ПСП в процессе информационного обмена будет изменятся, то выполнить демодуляцию обнаруженного сигнала злоумышленнику практически невозможно. Поэтому изменение структуры используемых сигналов-переносчиков информации по определенному закону, известному только на передающей и приемной сторонах, позволяет создать эффективный механизм противодействия угрозе подмены сообщений в ССС с КРК.

Таким образом задачу разработки модели противодействия угрозе подмены сообщений в ССС с КРК предлагается решать на основе стохастического применения ансамблей ортогональных кодовых последовательностей.

С учетом изложенного, усовершенствованная модель противодействия угрозе подмены сообщений в ССС с КРК Globalstar будет содержать следующие этапы:

1. Расчет допустимого значения арсенала сменяемых параметров кодовых последовательностей $A_{\text{доп.}}$, зависящего от времени существования ССС $T_{\text{сущ. ССС}}$. и скорости передачи информации R

$$A_{\text{доп.}} = f\left(T_{\text{сущ. ССС}}, R\right). \tag{2.3}$$

2. Расчет допустимого значения структурной скрытности АОКП $S_{\text{доп.}}$ с учетом допустимого значения арсенала сменяемых параметров кодовых последовательностей $A_{\text{доп.}}$

$$S_{\text{доп.}} = \log_2 A_{\text{доп.}} \tag{2.4}$$

3. Формирование последовательности начального заполнения регистров ГПСКЧ $S_{\text{нач.}}$ инициатором сеанса связи для обеспечения одинакового начального заполнения $S_{\text{нач.}}$ регистров ГПСКЧ у участников информационного обмена

4. Для обеспечения скрытой передачи последовательности начального заполнения $S_{\text{нач.}}$ регистров ГПСКЧ осуществляется ее шифрование с помощью криптосистемы с открытым ключом (КОК) [83] в виде криптограммы $E_{\text{нач.}}$

$$S_{\text{нач.}} \cdot K_{\text{КОК}} = E_{\text{нач.}} \tag{2.5}$$

На приемной стороне из криптограммы $E_{\text{нач.}}$ путем дешифрования в криптосистеме с открытым ключом выделяется последовательность начального заполнения $S_{\text{нач.}}$ для приемного регистра ГПСКЧ.

5. Формирование последовательности псевдослучайных комплексных чисел с помощью ГПСКЧ на передающей и приемной стороне, на основе которых будет осуществляться генерация допустимого арсенала ансамблей ортогональных кодовых последовательностей $S_{\text{нач.}}$. Сформированная последовательность ПСКЧ в данном случае будет выступать в качестве конфиденциального параметра преобразования K.

$$\{Z_{\text{Н}}\} = f\,(S_{\text{нач.}}) \tag{2.6}$$

6. Генерация на основе последовательностей псевдослучайных комплексных чисел допустимого арсенала АМФОКП $A_{\text{доп.}}$.

7. Ввод исходного информационного сообщения I.

8. Стохастическое преобразование применяемого АМФОКП на последующий из арсенала АМФОКП.

Математически данное стохастическое преобразование АМФОКП можно представить следующим образом

$$F = (X, Y, K; f), \tag{2.7}$$

где X –множество исходных кодовых последовательностей; Y –множество АМФОКП; K – конфиденциальный параметр преобразования; f – функция преобразования $f: X \cdot K \to Y$.

Математическая модель процесса стохастического преобразования информационного сообщения на основе неповторяющихся АМФОКП представлена на рисунке 2.4.

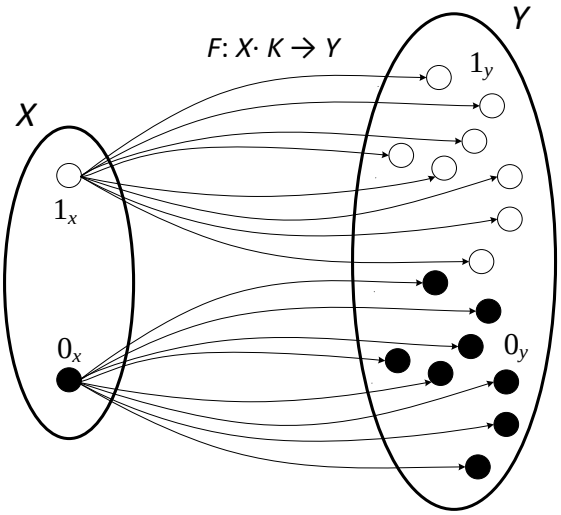


Рисунок 2.4 – Математическая модель процесса стохастического преобразования информационного сообщения на основе неповторяющихся АМФОКП

На рисунке обозначены 1_x, 0_x – символы 1 и 0 исходного информационного сообщения, 1_y, 0_y – множество (арсенал) АМФОКП для передачи соответственно 1_x, 0_x.

9. Модуляция применяемого АМФОКП информационным сообщением.

10. Передача модулированного АМФОКП в линию связи после его стохастического преобразования и модуляции.

11. Прием АМФОКП из линии связи.

12. Обратное стохастическое преобразование сообщения

$$F^{-1} = (X, Y, K; f). \qquad (2.8)$$

13. Выделение (демодуляция) информационного параметра сообщения.

14. Вывод полученного информационного сообщения *I*.

Схематично модель противодействия угрозе подмены сообщений в ССС с КРК можно представить следующим образом (рисунок 2.5).

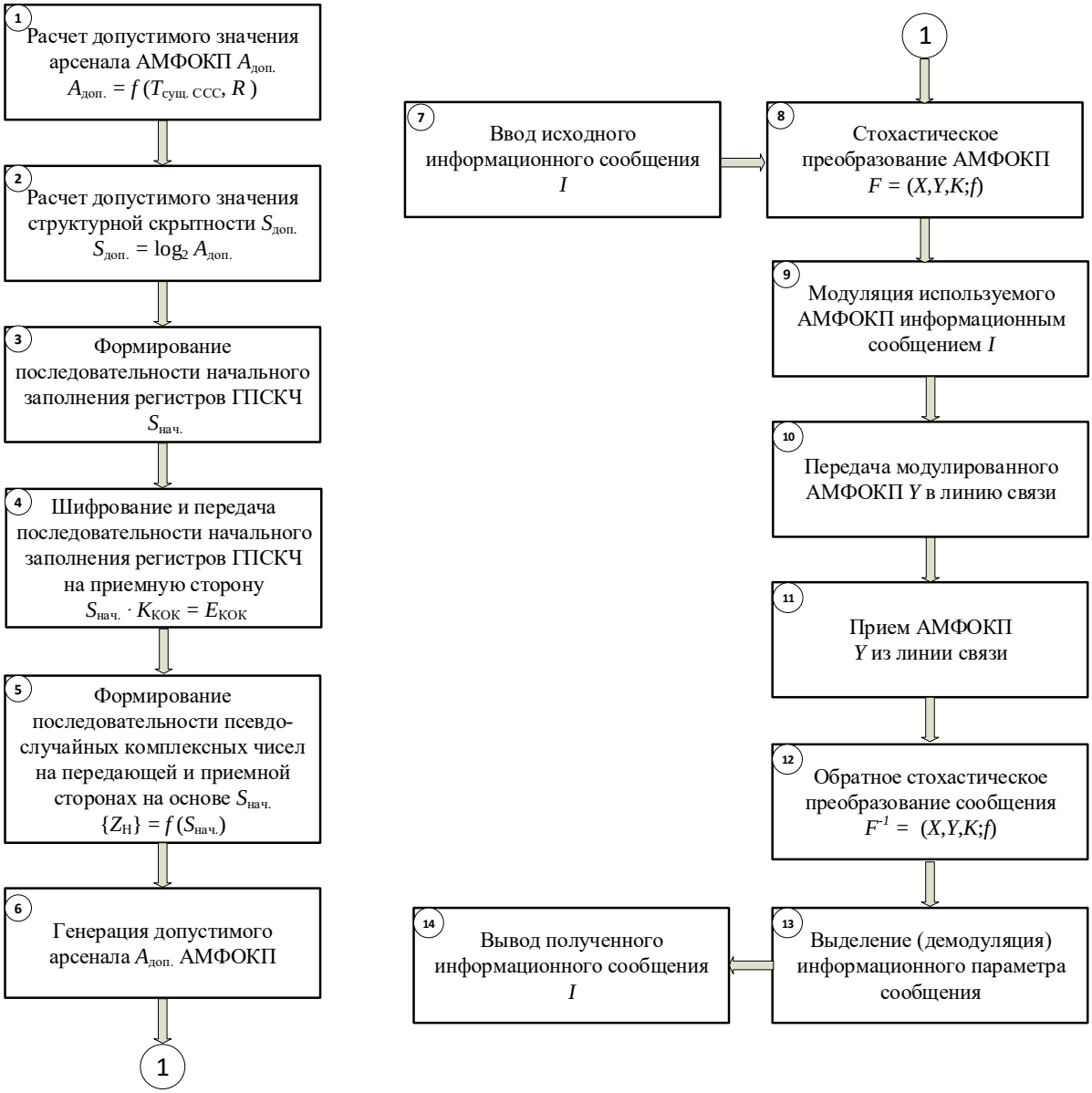
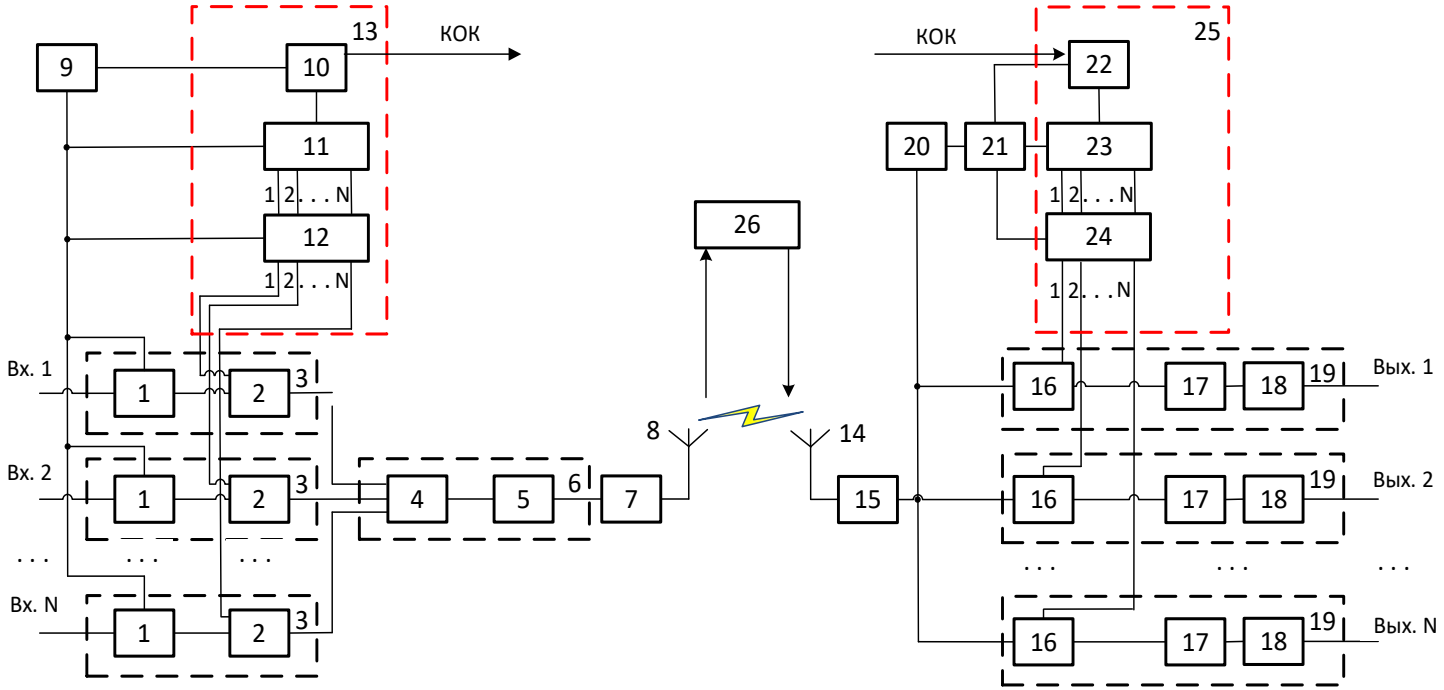


Рисунок 2.5 – Модель противодействия угрозе подмены сообщений в ССС с КРК

2.3 Разработка модели системы спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей

Модель ССС с КРК на основе стохастического применения АМФОКП, представленная на рисунке 2.6, содержит передатчик, включающий $N = 2^{m\text{-}1}$ каналов 3, состоящих из запоминающего устройства 1 и модулятора канального 2, причем вход запоминающего устройства является входом канала, первый выход запоминающего устройства подключен к управляющему входу блока синхронизации 9, а второй выход запоминающего устройства подключен к модулятору канальному 2 [76, 114].

Выход блока синхронизации 9 связан с управляющим входом генератора псевдослучайных комплексных чисел (ГПСКЧ) 10, блоком формирования АМФОКП передачи 11 и блоком накопителя (БН) передатчика 12. Генератор псевдослучайных комплексных чисел 10 на передающей и приемной стороне имеют одинаковое начальное заполнение для обеспечения синхронной генерации одинаковых АМФОКП. Для обеспечения скрытой передачи последовательности начального заполнения $S_{\text{нач.}}$ регистров ГПСКЧ 10 осуществляется ее шифрование с помощью криптосистемы с открытым ключом, которая дешифруется на приемной стороне и передается для начального заполнения регистра ГПСКЧ приемника 22.



Передатчик

1 – Запоминающее устройство.
2 – Модулятор канальный.
3 – Каналы.
4 – Объединитель входов.
5 – Модулятор групповой.
6 – Блок формирования группового сигнала.
7 – Усилитель мощности.
8 – Передающая антенна.
9 – Блок синхронизации.
10 – Генератор псевдослучайных комплексных чисел передатчика.
11 – Генератор псевдослучайных АМФОКП передатчика.
12 – Блок накопителя передатчика.
13 – Стохастическое средство защиты информации передатчика.

Приемник

14 – Приемная антенна.
15 – Блок ВЧ-селекции.
16 – Блок корреляционной обработки.
17 – Блок выделения информации.
18 – Блок приема информации.
19 – Каналы.
20 – Блок обнаружения сигнала синхронизации.
21 – Блок синхронизации.
22 – Генератор псевдослучайных комплексных чисел приемника.
23 – Генератор копий псевдослучайных АМФОКП приемника.
24 – Блок накопителя приемника.
25 – Стохастическое средство защиты информации приемника.
26 – Злоумышленник.
КОК – Криптосистема с открытым ключом.

Рисунок 2.6 – Структура системы спутниковой связи с кодовым разделением каналов на основе стохастического применения АМФОКП

Генератор псевдослучайных комплексных чисел 10 связан с генератором АМФОКП 11, выходы генератора АМФОКП 11 связаны с одноименными входами БН передатчика 12, выходы которого подключены ко вторым входам модулятора 2 соответствующего канала 3.

Выходы модуляторов 2 каждого канала соединены со входами объединителя входов 4. Выход объединителя входов 4 соединен со входом модулятора группового 5. Объединитель входов 4 и модулятор групповой 5, соединенные между собой входят в состав блока формирования группового сигнала 6. Выход блока формирования группового сигнала 6 соединен с входом усилителя мощности 7, назначением которого является усиление мощности группового сигнала, выход усилителя мощности 7 соединен с передающей антенной 8, предназначенной для излучения группового сигнала в эфир [114].

В передатчике рассматриваемой ССС с КРК по аналогии с рисунком 2.2 выделим стохастическое средство защиты информации 13, которое включает в себя генератор псевдослучайных комплексных чисел передатчика 10, генератор АМФОКП передатчика 11 и блок накопителя передатчика 12.

Приемная часть модели ССС с КРК на основе стохастического применения АМФОКП содержит приемную антенну 14, соединенную со входом блока высокочастотной селекции 15, которая принимает из эфира и выделяет групповой сигнал и передает его на блок высокочастотной селекции 15, выход которого соединен с первым входом блока обнаружения сигнала синхронизации 20 и вторыми входами блоков корреляционной обработки 16, имеющиеся в каждом из $N = 2^{m\text{-}1}$ каналов 19. Второй вход блока корреляционной обработки 16 соединен с блоком накопителя приемника 24, на выходах которого формируются копии АМФОКП. Выход блока корреляционной обработки 16 подключен к входу блока выделения информации 17, выход которого соединен с входом блока приема информации 18 в каждом из $N = 2^{m\text{-}1}$ каналов 19 [114].

Блок формирования копий АМФОКП 23 подключен к блоку накопителя приемника 24, функционирование которых управляется блоком синхронизации 21, работающим под управлением блока обнаружения сигнала синхронизации 20.

[114] Блок синхронизации 21 соединен с входом ГПСКЧ приемника 22 и входом буферного накопителя приемника 24. ГПСКЧ приемного устройства 22 функционирует по одному и тому же алгоритму, что и ГПСКЧ 12 передающего устройства, поэтому при их синхронной работе последовательность псевдослучайных комплексных чисел (ПСКЧ) на их выходах имеет одинаковые значения, на основании которых генератор АМФОКП 13 и генератор копий АМФОКП 25 соответственно на передающей и приемной сторонах формируют одинаковые ансамбли ортогональных кодовых последовательностей.

В приемнике рассматриваемой ССС с КРК по аналогии с рисунком 2.2 выделим стохастическое средство защиты информации 25, которое включает в себя генератор псевдослучайных комплексных чисел приемника 22, генератор копий АМФОКП приемника 23 и блок накопителя приемника 24.

С помощью применяемого в конкретный момент времени АМФОКП, поступающего из блока накопителя приемника 24 блок корреляционной обработки 16 в каждом канале 19 выделяет принятый бит информационной последовательности.

Смена диагональных коэффициентов ЭМ, на основе которых происходит формирование нового по сравнению с используемым до этого АМФОКП на приемной и передающей сторонах, осуществляется синхронно, для обеспечения корректной передачи и приема следующих информационных битов в каждом канале системы. На последующих этапах передачи информации для каждого информационного бита используется уникальный АМФОКП, получаемый по единым алгоритмам на передающей и приемной сторонах.

Данный подход позволяет повысить скрытность ССС с КРК и обеспечить её защиту от несанкционированных пользователей, которым неизвестен механизм получения и стохастического применения АМФОКП. Подробное описание разработанной модели ССС с КРК на основе стохастического применения АМФОКП представлено в работах [73,80].

Вероятность подмены сообщений в ССС с КРК снижается за счет внедрения стохастического средства защиты информации 13. Стохастическое применение

АМФОКП предъявляет дополнительные требования (устойчивость работы системы синхронизации, обеспечение требуемого времени установления синхронизации в начале работы и после сбоя и др.) и ограничения по функционированию ССС с КРК (распределение ключа между легальными пользователями, наличие дополнительного технического средства защиты информации и др.).

С целью создания одинаковых начальных условий для запуска ГПСКЧ на приемной и передающей сторонах необходимо их синхронное первоначальное заполнение одинаковой псевдослучайной последовательностью. Она по сути является последовательностью начального заполнения ГПСКЧ. Поскольку данное значение последовательности начального заполнения ГПСКЧ необходимо передать по открытому каналу перед началом сеанса связи, то ее следует передать в секрете от потенциальных злоумышленников. Для решения данной задачи передачи последовательности начального заполнения ГПСКЧ между пользователями возможно использование различных вариантов известных алгоритмов защищенного информационного обмена, в частности шифрования для криптосистемы с открытым ключом, основанного на применении односторонних функций с секретом, описанного в [138, 139].

На основе модели ССС с КРК разработаем алгоритм стохастического применения АМФОКП в ССС с КРК, который представлен на рисунках 2.7, 2.8.

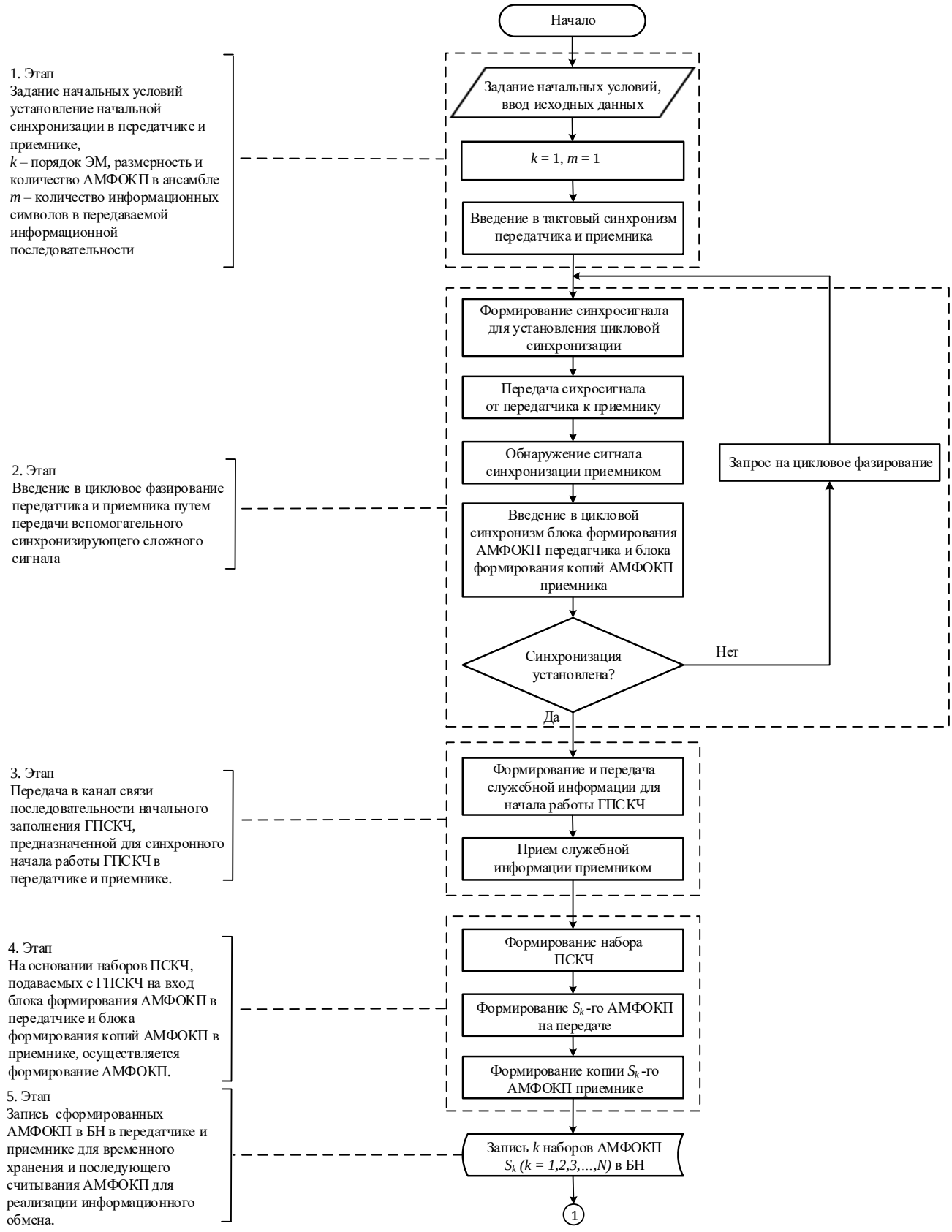


Рисунок 2.7 – Алгоритм стохастического применения АМФОКП в ССС с КРК (начало)

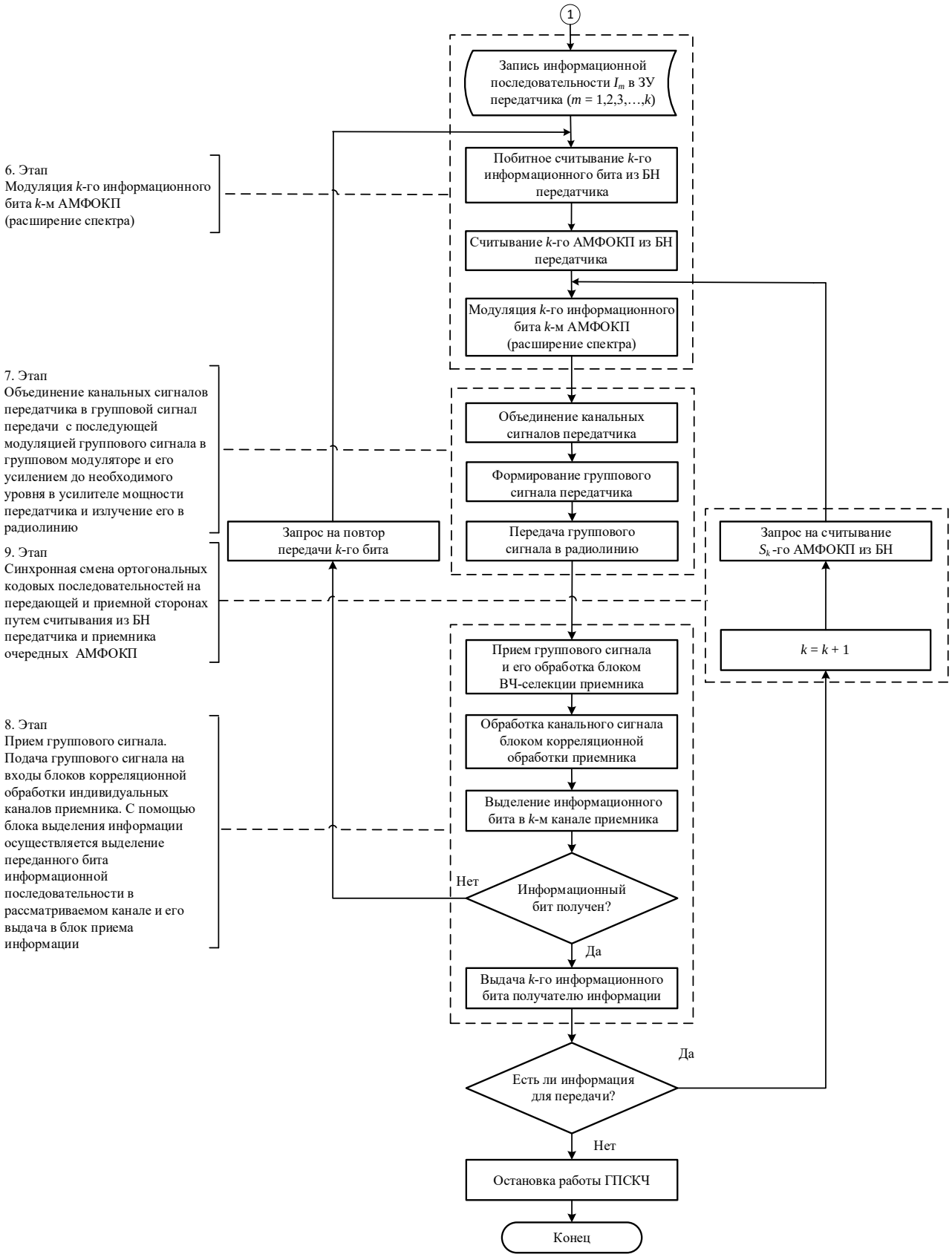


Рисунок 2.8 – Алгоритм стохастического применения АМФОКП в ССС с КРК (окончание)

Суть предлагаемого алгоритм стохастического применения АМФОКП в ССС с КРК заключается в следующем.

На первом этапе осуществляется задание начальных условий, а также установление начальной синхронизации в передатчике и приемнике.

На втором этапе с помощью вспомогательного синхронизирующего сложного сигнала передатчик и приемник вводятся в цикловую фазу.

На третьем этапе посредством манипуляции вспомогательного сигнала синхронизации в канал связи передается служебная информация, предназначенная для синхронного начала работы ГПСКЧ в передатчике и приемнике.

На четвертом этапе на основании наборов псевдослучайных комплексных чисел, подаваемых с ГПСКЧ передающей стороны на вход блока формирования АМФОКП в передатчике, а также с ГПСКЧ приемной стороны на вход блока формирования копий АМФОКП в приемнике, осуществляется формирование одинаковых ансамблей многофазных ортогональных кодовых последовательностей S_k $(k = 1, 2, 3, \dots, N)$ на приемной и передающей сторонах рассматриваемой системы передачи информации.

На пятом этапе осуществляется запись k сформированных АМФОКП в блоки накопителей в передатчике и приемнике для временного хранения и последующего считывания АМФОКП для их стохастического применения в качестве последовательностей в канальных блоках передатчика и приемника.

На шестом этапе информационная последовательность I_m $(m = 1, 2, 3, \dots, k)$, подлежащая передаче в каждом канале, записывается в запоминающее устройство индивидуального канала передатчика для промежуточного хранения. Затем из запоминающего устройства осуществляется побитное считывание записанной информационной последовательности I_m и побитная выдача её на канальный модулятор индивидуального канала передатчика, реализующий функцию расширения спектра прямой последовательностью direct-sequence (DS). В качестве расширяющей последовательности на второй вход канального модулятора каждого индивидуального канала поступает считываемая из блока накопителя одна из k ортогональных последовательностей, используемого в данный момент времени

АМФОКП. В результате чего осуществляется модуляция k – го информационного символа k – м АМФОКП, применяемым в качестве расширяющих последовательностей. Модуляция информационной последовательности с использованием расширяющей последовательности осуществляется по следующему принципу. В зависимости от значения информационного символа применяются разные варианты ортогональной кодовой последовательности. Если символ равен 1, используется последовательность с инверсной структурой – фаза каждого её элемента меняется на противоположную. Если же символ равен 0, задействуется прямая кодовая последовательность без изменения фаз элементов, как отмечается в источниках [9, 68].

Для примера на рисунке 2.9 представлен принцип модуляции кодовой последовательности Уолша информационной последовательностью с периодом T_s. Длина элемента кодовой последовательности Уолша $N = 8$. Длительность элемента модулируемой последовательности T_{ch}.

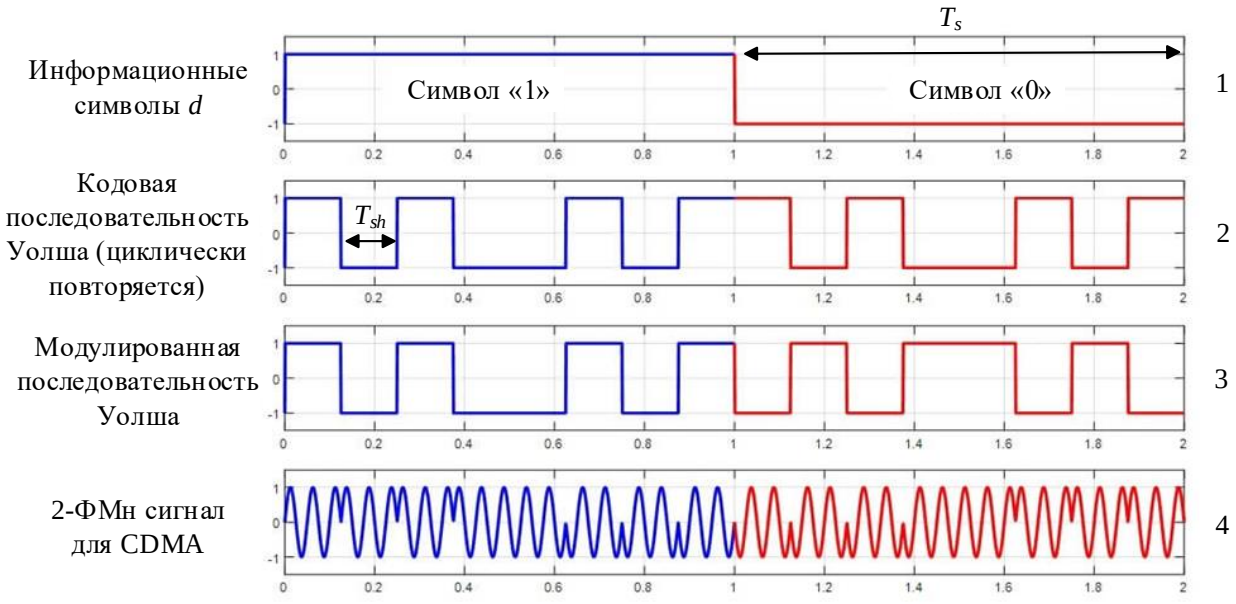


Рисунок 2.9 – Принцип модуляции кодовой последовательности Уолша информационной последовательностью

Каждому каналу назначается своя последовательность Уолша

$$S_k(t) = a_k(t) \times A\cos(2\pi f t + d\pi), \quad (2.9)$$

где d – это информационные символы $d = \{1; -1\}$, $a_k(t)$ – это k-я последовательность Уолша, A – амплитуда несущего колебания, f – частота несущего колебания.

На седьмом этапе осуществляется объединение канальных сигналов передатчика в групповой сигнал $S_{\text{гр}}$. Сформированный групповой сигнал $S_{\text{гр}}$ модулируется с помощью высокочастотного сигнала в БФГС, затем усиливается до необходимого уровня в усилителе мощности передатчика и излучается с помощью передающей антенны в радиолинию.

На восьмом этапе осуществляется прием группового сигнала $S^*_{\text{гр}}$, возможно искаженного помехами с помощью приемной антенны, его обработка блоком ВЧ-селекции приемника. Далее осуществляется подача группового сигнала на входы блоков корреляционной обработки индивидуальных каналов приемника. На вторые входы каждого N – го блока корреляционной обработки индивидуальных каналов приемника поступает считываемая из блока накопителя приемника одна из k последовательностей, используемого в данный момент времени АМФОКП. В результате чего с помощью блока выделения информации осуществляется выделение переданного бита информационной последовательности I_m в рассматриваемом канале и его выдача в блок приема информации.

На девятом этапе происходит синхронная смена ортогональных последовательностей на передающей и приемной стороне путем считывания из блоков накопителей передатчика и приемника очередных S_{k+1} АМФОКП, которые будут идентичны друг другу, для осуществления передачи и приема методом прямого расширения спектра следующего за первым второго информационного бита информационной последовательности I_m. Отметим, что используемый на данном этапе S_{k+1} АМФОКП, отличается по своей структуре от предыдущего S_k АМФОКП.

На последующих этапах передача каждого последующего бита информационной последовательности I_m будет осуществляться с помощью

очередных неповторяющихся АМФОКП, синхронно считываемых из блоков накопителей передатчика и приемника. Процесс заканчивается при условии передачи всех бит информационной последовательности I_m.

Подробное описание разработанного алгоритма стохастического применения АМФОКП в ССС с КРК представлено в работах [79,81].

Применение предложенного алгоритма позволяет в процессе сеанса связи при передаче каждого информационного бита использовать уникальную неповторяющуюся структуру ортогональных кодовых последовательностей, за счет чего обеспечивается высокая структурная скрытность АМФОКП в ССС с КРК.

Временные диаграммы, поясняющие алгоритм стохастического применения АМФОКП в ССС с КРК для бидиагональной ЭМ четвертого порядка подробно описаны в [75,77] и представлены на рисунке 2.10.

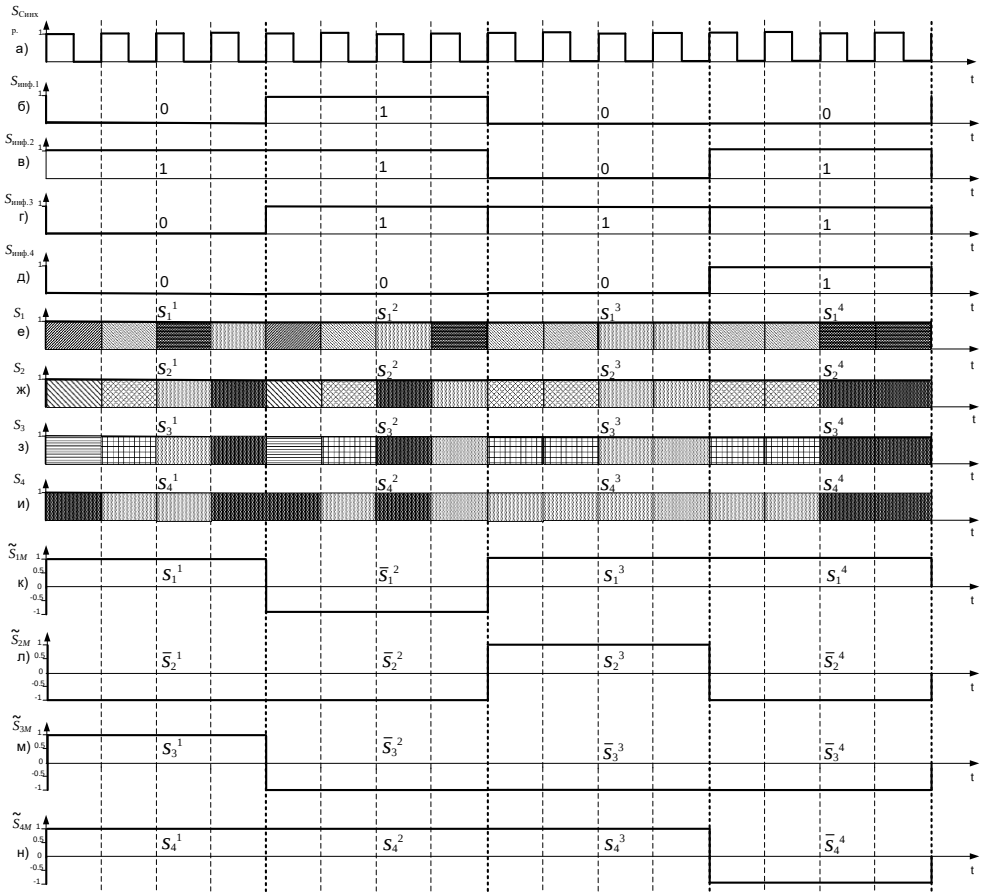


Рисунок 2.10 – Временные диаграммы, поясняющие алгоритм стохастического применения АМФОКП в ССС с КРК

На рисунке 2.11 представлены исходные АМФОКП и процесс их модуляции с расширением спектра информационной последовательностью в каждом канале во временной области

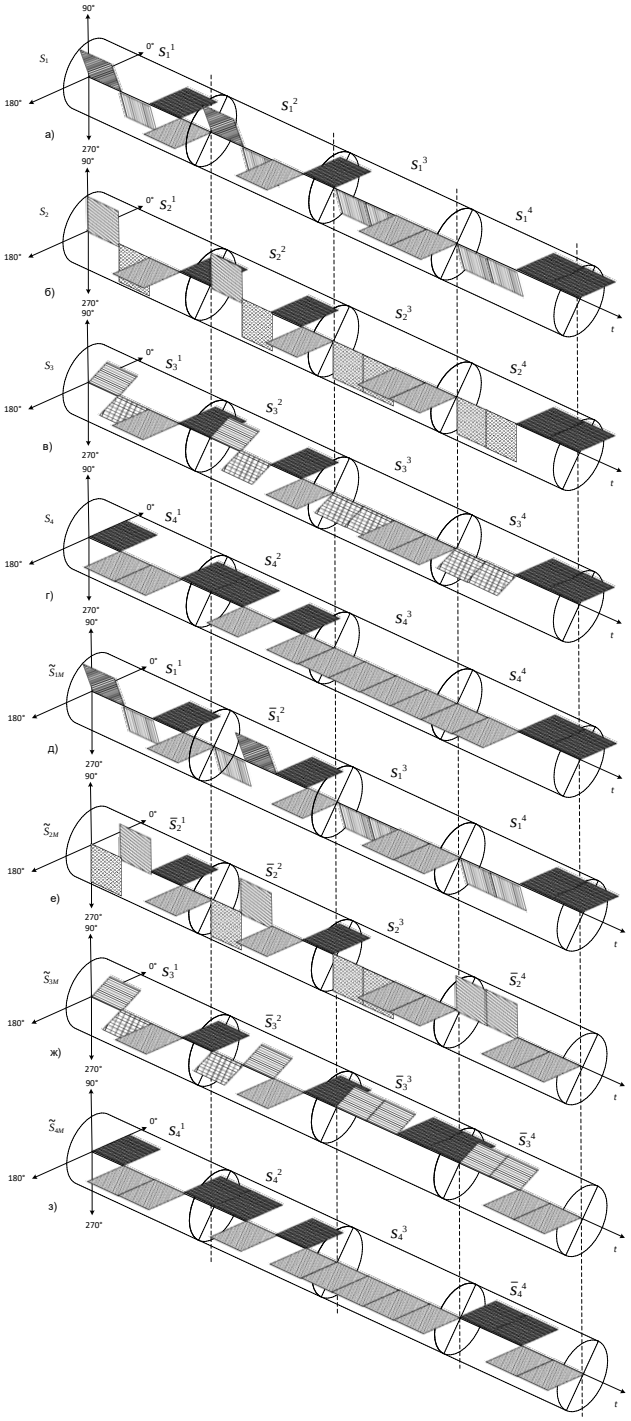


Рисунок 2.11 – Исходные АМФОКП и процесс их модуляции с расширением спектра информационной последовательностью в каждом канале во временной области

Процесс модуляции исходных АМФОКП с расширением спектра информационной последовательностью в каждом канале во временной области осуществляется следующим образом.

Для передачи бита 1 используется инвертированная кодовая последовательность, а для бита 0 – прямая кодовая последовательность. Инверсия подразумевает изменение фазы каждого элемента кодовой последовательности на противоположную [114].

Если приемное оборудование ССС с КРК используется легальным пользователем, то правило формирования ПСКЧ, на основе которых получаются АМФОКП в приемнике совпадает с правилом их формирования в передатчике. При этом структура АМФОКП, формируемая на передающей стороне и используемая для передачи информационной последовательности, а также структура АМФОКП, формируемая и используемая на приемной стороне для её выделения, будут совпадать, что позволит корректно осуществить информационный обмен с применением изменяющихся ортогональных кодовых последовательностей.

В случае использования разработанного алгоритма противодействия угрозе подмены сообщений за счет стохастического применения неповторяющихся АМФОКП происходит преобразование исходной информации и передача в канал связи в виде изменяющихся стохастическим образом последовательностей для передачи каждого информационного символа. Доступ к передаваемой информации может быть получен легальным пользователем ССС с КРК, которому известен алгоритм формирования и порядок стохастического применения АМФОКП.

Для надежной защиты передаваемой информации разработанным алгоритмом должны быть обеспечены следующие условия [70, 71]:

1. В пределах цикла передачи информации набор АМФОКП должен исключать возможность выявления закономерности их применения.

2. Количество неповторяющихся АМФОКП должно быть равно или больше количества информационных символов в передаваемом сообщении.

Для ПСП эти свойства (требования) проверяются с помощью различных тестов. Наиболее популярный и авторитетный из них «Набор статистических

тестов для генераторов случайных и псевдослучайных чисел для криптографических приложений» [70, 71].

Помимо этих условий, как было отмечено в первой главе данной работы, ансамбли ортогональных кодовых последовательностей по показателю структурной скрытности должны обеспечивать требуемое её значение $S_{\text{треб}} \geq 43$ ДИЗ.

В целом модель ССС с КРК на основе стохастического применения АМФОКП и алгоритм стохастического применения АМФОКП в ССС с КРК представляют собой модель противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП.

2.4 Выводы по главе

1. Метод стохастического кодирования, предложенный С.А. Осмоловским для защиты информации от угрозы подмены сообщений, лег в основу разрабатываемого подхода для систем спутниковой связи с кодовым разделением каналов. Данная концепция объединяет два ключевых этапа: кодирование с добавлением избыточности и декодирование. Стохастическое преобразование реализуется через прямое преобразование F при кодировании и обратное преобразование F^{-1} при декодировании. Основой для этих преобразований служат квазислучайные числа, генерируемые специальным датчиком. При этом целью метода является обеспечение устойчивости передаваемых данных к попыткам несанкционированного изменения.

2. Для решения задачи противодействия угрозе подмены сообщений в ССС с КРК предлагается внедрить в передатчике и приемнике стохастические средства

защиты информации, основанные на стохастическом применении АМФОКП под управлением генератора псевдослучайных комплексных чисел.

3. Модель противодействия угрозе подмены сообщений в ССС с КРК представлена на рисунке 2.5. Данная модель содержит четырнадцать этапов, выполнение которых позволяет снизить вероятность разведки структуры сигнала $P_{\text{разв.}}$ от которой зависит успешность реализации злоумышленником угрозы подмены сообщений. На основании формулы (2.2) сделан вывод о том, что снижение вероятности разведки структуры сигнала $P_{\text{разв.}}$ может быть обеспечено за счет снижения вероятности раскрытия структуры сигнала при условии его обнаружения $P_{\text{стр.}}$.

4. Разработаны структура ССС с КРК, реализующая модель противодействия угрозе подмены сообщений за счет стохастического применения АМФОКП, представленная на рисунке 2.6, и алгоритм стохастического применения АМФОКП в ССС с КРК, представленный на рисунках 2.7 и 2.8, которые позволяют в процессе информационного обмена при передаче каждого информационного бита использовать уникальную неповторяющуюся структуру АМФОКП.

5. Определены требования, предъявляемые к ансамблям ортогональных кодовых последовательностей, при которых обеспечивается надежная защита информации от противодействия угрозе подмены сообщений предлагаемым алгоритмом.

6. С учетом того, что ансамбли ортогональных кодовых последовательностей в случае их стохастического применения в ССС с КРК должны обеспечивать требуемый показатель их структурной скрытности $S_{\text{треб}} \geq 43$ ДИЗ при значении их арсенала $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$, необходимо разработать модель ансамблей многофазных ортогональных кодовых последовательностей и алгоритм их синтеза с учетом указанных требований.

3. РАЗРАБОТКА МОДЕЛИ АНСАМБЛЕЙ МНОГОФАЗНЫХ ОРТОГОНАЛЬНЫХ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И АЛГОРИТМА ИХ СИНТЕЗА

3.1 Разработка модели ансамблей многофазных ортогональных кодовых последовательностей на основе собственных векторов эрмитовых матриц

В соответствии с анализом, проведенным в первой главе данной работы установлено, что в современных ССС с КРК используются кодовые последовательности с длиной равной 128 и 256 элементов ($L = 128, 256$).

Анализ принципов построения и функционирования ССС с КРК, представленный в первой главе, показал, что используемые в них ансамбли ортогональных кодовых последовательностей легко предсказуемы и имеют низкую структурную скрытность.

Так же в первом разделе отмечено, что известные методы синтеза ансамблей ортогональных последовательностей имеют ограничения по их объему и корреляционным характеристикам.

В связи с вышеизложенным существует задача разработки модели ансамблей многофазных ортогональных кодовых последовательностей, удовлетворяющих изложенным выше требованиям по их количеству, объему и корреляционным характеристикам.

Метод векторного синтеза АДОП имеет преимущество перед известными методами и подробно описан в работах [9, 11-13, 57, 78-83].

Применение модели векторного синтеза ансамблей ортогональных последовательностей описано в известных работах Попенко В.С., Турко С.А.,

Самуса М.В., Гайчука Д.В., Сазонова В.В., Трошкова А.М., Жука А.П. [7, 8, 11-13, 17, 68, 72, 73, 77, 79, 81, 82, 88, 87-92, 95] направлено на решение задачи синтеза искомого ансамбля последовательностей по критерию безусловного предпочтения характеристик полученных последовательностей перед характеристиками известных. Для синтеза множества ансамблей с требуемыми корреляционными свойствами, объемами и размерностями, достаточного для их стохастического применения, данная модель ранее не исследовалась.

В работе [81] отмечено, что множество ЭМ порядка $(n \times n)$, все элементы которых – целые комплексные числа, задают все возможные базисы пространства C^n. Из этого следует, что перебором значений диагональных коэффициентов ЭМ возможно получение всех возможных базисов ортогональных функций, которыми могут быть описаны ансамбли дискретных ортогональных кодовых последовательностей.

Вариантом применения векторного синтеза ансамблей ортогональных последовательностей для повышения скрытности систем передачи информации является работа З.В. Черняка [57], где была разработана модель синтеза АДОМУС, подразумевающая присвоение случайных значений диагональным коэффициентам бидиагональных симметрических матриц. Симметрическая матрица четвертого порядка $(N = 4)$ имеет следующий вид

$$A = \begin{bmatrix} 0 & a_{12} & 0 & 0 \\ a_{21} & 0 & a_{23} & 0 \\ 0 & a_{32} & 0 & a_{34} \\ 0 & 0 & a_{43} & 0 \end{bmatrix}, \tag{3.1}$$

где a_{12}, a_{23}, a_{34} – диагональные коэффициенты симметрической матрицы, причем $a_{12} = a_{21}, a_{23} = a_{32}, a_{34} = a_{43}$.

Собственные векторы симметрической матрицы вида (3.1) в данной модели в работе рассматриваются АДОМУС, представляемых системой собственных векторов вида [57]

$$\overline{x}_{k,i} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1N} \\ x_{21} & x_{22} & \ldots & x_{2N} \\ \vdots & \vdots & \vdots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nN} \end{bmatrix}. \quad (3.2)$$

Из [84–86, 90] известно, что собственные векторы симметрического линейного оператора A, отвечающие различным собственным числам λ_1 и λ_2 ($\lambda_1 \neq \lambda_2$), ортогональны между собой. То есть, собственные векторы (3.2) бидиагональной симметрической матрицы вида (3.1) удовлетворяют условию ортогональности

$$\overline{X}_k \cdot \overline{X}_i = 0, \text{при } k \neq i. \quad (3.3)$$

Временная диаграмма ансамбля дискретных ортогональных многоуровневых сигналов при $N = 16$ представлена на рисунке 3.1.

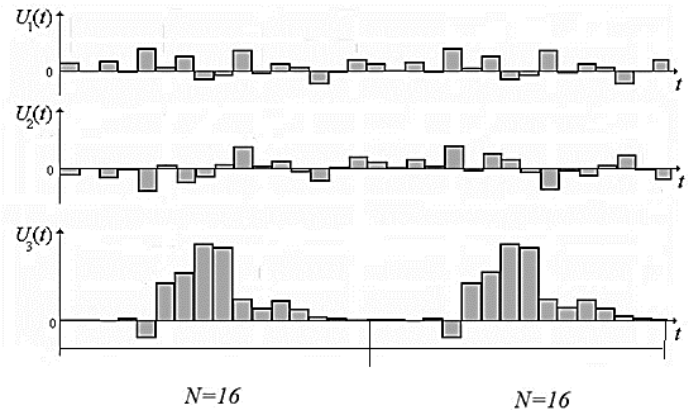


Рисунок 3.1 – Временная диаграмма ансамбля дискретных ортогональных многоуровневых сигналов при $N = 16$

Синтез АДОМУС с требуемыми корреляционными характеристиками реализуется целенаправленным перебором коэффициентов бидиагональной симметрической матрицы вида (3.1) и представлении модели АДОМУС получаемыми при этом собственными векторами матрицы (3.2).

Достоинство данной модели заключается в том, что количество получаемых АДОМУС имеет гораздо большее значение по сравнению с другими моделями и

достаточно для их стохастического применения в системе передачи информации с кодовым разделением каналов. Отметим, что данная модель ориентирована на применение последовательностей, имеющих длину в диапазоне $N = 4, 8, \cdots, 64$.

Однако область применения АДОМУС, синтезируемых при помощи данной модели, в СПИ с КРК ограничена каналами связи с низким уровнем помех, что характерно для проводных каналов связи и противоречит реальной помеховой обстановке в беспроводных каналах спутниковой связи [57]. Поэтому применение данной модели, для получения и последующего стохастического использования ортогональных кодовых последовательностей в ССС с КРК невозможно.

Также недостатком данной модели является то, что формирование ансамблей дискретных ортогональных многоуровневых сигналов требует более сложных программно-аппаратных устройств их генерации, поскольку они не являются двоичными.

С учетом того, что при организации трактов передачи и приема информации в ССС с КРК практически используется квадратурная фазовая манипуляция QPSK и квадратурная амплитудная модуляция QAM, которая является амплитудно-фазовым видом модуляции 16-QAM, то можно сделать вывод о том, что необходимые для решения поставленной в диссертационной работе задачи ансамбли многопозиционных ортогональных кодовых последовательностей относились к классу многофазных последовательностей. В работах А.В. Микушина, С.В. Дворникова, А.В. Пшеничникова, С.С. Манаенко, И.Н. Глухих и др. доказано, что повышение структурной скрытности многофазных ортогональных кодов может быть достигнуто за счет увеличения размерности формирующей фазовой плоскости [38, 145].

Таким образом, для ССС с КРК для повышения их структурной скрытности приемлемым может быть стохастическое применение многозначных кодов, в частности АМФОКП.

Ансамбли ортогональных кодовых последовательностей могут быть получены не только за счет описания их собственными векторами симметрических матриц. В работах В.С. Попенко, А.П. Жука, Д.В. Гайчука, В.В. Сазонова и др. [7,

8, 11-13, 17, 68, 72, 73, 77, 79, 81, 82, 88, 87-92, 95] отмечается, что более широкие возможности по охватываемому объему ортогональных базисов имеет подход, основанный на рассмотрении собственных векторов ЭМ.

В работах [81, 82] доказано, что для синтеза оптимального АМФОКП по критерию безусловного предпочтения по совокупности характеристик целесообразно рассматривать собственные векторы эрмитовых матриц. В этой связи отметим основные свойства эрмитовых матриц.

Матрица A называется эрмитовой [93], если её диагональные элементы по отношению к главной диагонали являются комплексно-сопряжёнными числами. При этом, элементы главной диагонали ЭМ являются вещественными числами.

$$A=\begin{pmatrix} d_{1,1} & a_{1,2}\cdot e^{j\varphi_{1,2}} & \cdots & a_{1,m-1}\cdot e^{j\varphi_{1,m-1}} & a_{1,m}\cdot e^{j\varphi_{1,m}} \\ a_{2,1}\cdot e^{-j\varphi_{2,1}} & d_{2,1} & \cdots & a_{2,m-1}\cdot e^{j\varphi_{2,m-1}} & a_{2,m}\cdot e^{j\varphi_{2,m}} \\ a_{3,1}\cdot e^{-j\varphi_{3,1}} & a_{3,2}\cdot e^{-j\varphi_{3,2}} & \cdots & a_{3,m-1}\cdot e^{j\varphi_{3,m-1}} & a_{3,m}\cdot e^{j\varphi_{3,m}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1,1}\cdot e^{-j\varphi_{n-1,1}} & a_{n-1,2}\cdot e^{-j\varphi_{n-1,2}} & \cdots & a_{n-1,m-1}\cdot e^{-j\varphi_{n-1,m-1}} & a_{n-1,m}\cdot e^{j\varphi_{n-1,m}} \\ a_{n,1}\cdot e^{-j\varphi_{n,1}} & a_{n,2}\cdot e^{-j\varphi_{n,2}} & \cdots & a_{n,m-1}\cdot e^{-j\phi_{n,m-1}} & d_{n,m} \end{pmatrix}, \quad (3.4)$$

где $a_{k,i}\cdot e^{-j\varphi_{k,i}}=a_{i,k}\cdot e^{j\varphi_{i,k}}$ – диагональные коэффициенты являются комплексно-сопряженными числами (представлены в показательной форме), $d_{1,1}\dots d_{n,m}$ – коэффициенты главной диагонали матрицы, которые всегда вещественные числа.

Отметим, что комплексно-сопряженные числа имеют равные модули, т.е. $a_{k,i}=a_{i,k}$, и противоположные по знаку аргументы, т.е. $\varphi_{k,i}=-\varphi_{k,i}$ на основании формулы Эйлера.

Для пояснения иллюстрация комплексно-сопряженных чисел в полярной системе координат показана на рисунке 3.2 при условии, что радиус вектора r может отождествляться с модулем диагонального коэффициента эрмитовой матрицы $a_{k,i}$.

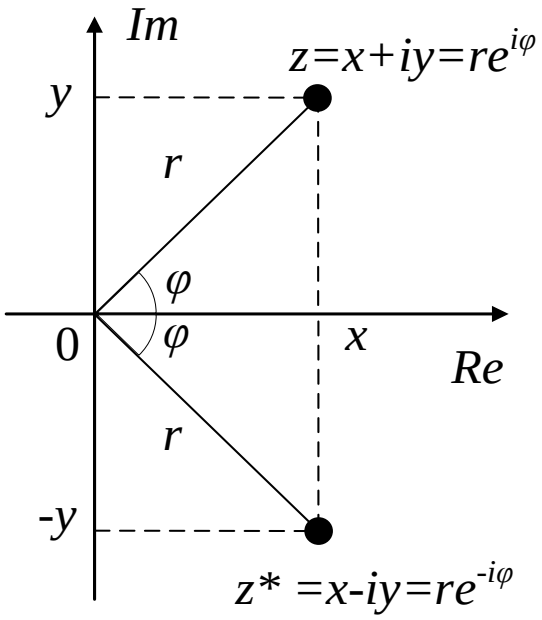


Рисунок 3.2 – Иллюстрация комплексно-сопряженных чисел в полярной системе координат

Иллюстрация комплексно-сопряженных чисел в полярной системе координат показана на рисунке 3.3 [143].

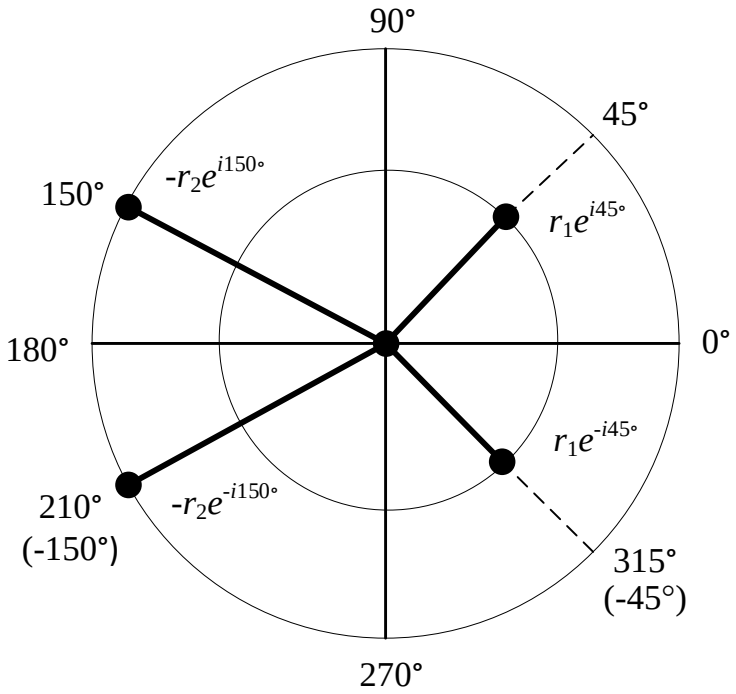


Рисунок 3.3 – Иллюстрация комплексно-сопряженных чисел в полярной системе координат

В выражении (3.4) диагональные коэффициенты, представляемые комплексными числами, для удобства показаны в показательной форме. Далее в данной работе будем использовать аналогичное представление эрмитовых матриц, т.е. представление диагональных коэффициентов в показательной форме. Это позволяет наглядно представить взаимосвязь между модулями и аргументами диагональных коэффициентов ЭМ, а также модулями и аргументами координат их собственных векторов.

Отметим, что координаты СВ ЭМ вида (3.4) в общем случае представляются комплексными числами.

Для примера ниже приведена бидиагональная ЭМ четвертого порядка $N = 4$

$$A = \begin{pmatrix} d_{1,1} & A_{1,2} \cdot e^{i \cdot \varphi_{1,2}} & 0 & 0 \\ A_{2,1} \cdot e^{-i \cdot \varphi_{2,1}} & d_{2,2} & A_{2,3} \cdot e^{i \cdot \varphi_{2,3}} & 0 \\ 0 & A_{3,2} \cdot e^{-i \cdot \varphi_{3,2}} & d_{3,3} & A_{3,4} \cdot e^{i \cdot \varphi_{3,4}} \\ 0 & 0 & A_{4,3} \cdot e^{-i \cdot \varphi_{4,3}} & d_{4,4} \end{pmatrix}. \quad (3.5)$$

Собственные значения матрицы A определяются как корни уравнения

$$det|A - \lambda E| = 0. \quad (3.6)$$

Уравнение (3.6) называется характеристическим уравнением матрицы A.

Выражение $det|A - \lambda E|$ является многочленом степени n от переменной λ и иначе называется характеристическим многочленом матрицы A.

Характеристический многочлен матрицы A вида (3.5) четвертого порядка будет иметь следующий вид

$$det|A - \lambda E| = \lambda^4 - \lambda^3 tr\, A + \lambda^2 - \Omega\lambda + \det A, \quad (3.7)$$

где $tr\ A$ – след матрицы A, Ω - коэффициент, определяемый как сумма миноров элементов, стоящих на главной диагонали матрицы A.

Для бидиагональной ЭМ вида (3.5) можно при помощи одной из известных моделей [84-86] получить систему её СВ, описываемую выражением следующего вида

$$\overline{\mathrm{X}} = \begin{pmatrix} x_{1,1} \cdot e^{j \cdot \psi_{1,1}} & x_{1,2} \cdot e^{j \cdot \psi_{1,2}} & x_{1,3} \cdot e^{j \cdot \psi_{1,3}} & x_{1,4} \cdot e^{j \cdot \psi_{1,4}} \\ x_{2,1} \cdot e^{j \cdot \psi_{2,1}} & x_{2,2} \cdot e^{j \cdot \psi_{2,2}} & x_{2,3} \cdot e^{j \cdot \psi_{2,3}} & x_{2,4} \cdot e^{j \cdot \psi_{2,4}} \\ x_{3,1} \cdot e^{j \cdot \psi_{3,1}} & x_{3,2} \cdot e^{j \cdot \psi_{3,2}} & x_{3,3} \cdot e^{j \cdot \psi_{3,3}} & x_{3,4} \cdot e^{j \cdot \psi_{3,4}} \\ x_{4,1} \cdot e^{j \cdot \psi_{4,1}} & x_{4,2} \cdot e^{j \cdot \psi_{4,2}} & x_{4,3} \cdot e^{j \cdot \psi_{4,3}} & x_{4,4} \cdot e^{j \cdot \psi_{4,4}} \end{pmatrix}, \quad (3.8)$$

где $x_{n,m}$ – модули координат СВ, а $\psi_{n,m}$ - аргументы координат СВ.

Каждый собственный вектор $\overline{X}_k$ эрмитовой матрицы соответствует своему собственному числу (значению) λ_k.

Собственные векторы матрицы (3.8), которые соответствуют различным собственным значениям ЭМ попарно ортогональны в соответствии со свойствами эрмитовых матриц [93]

$$\overline{X}_k \cdot \overline{X}_l = 0, \text{при } k \neq l. \quad (3.9)$$

В работах [79, 81] показано, что множество ЭМ порядка $(n \times n)$, все элементы которых – целые комплексные числа, задают все возможные базисы пространства C^n. Данное обстоятельство может позволить получить максимальное количество ортогональных базисов, что имеет важное значение при получении большого количества ортогональных базисов, которыми могут быть описаны ансамбли ортогональных кодовых последовательностей.

Такая модель задания ЭМ обеспечивает полный охват базисов пространства C^n, на основании подобной теоремы, рассмотренной в [79].

Обобщая вышеизложенное, можно сделать вывод, что при решении задачи синтеза АМФОКП в такой постановке в качестве моделей целесообразно

использовать множество наборов собственных векторов ЭМ, которые будут в каждом конкретном случае определяться набором значений модулей и аргументов диагональных коэффициентов эрмитовых матриц.

Таким образом, для синтеза ансамблей ортогональных кодовых последовательностей целесообразно рассматривать собственные векторы эрмитовых матриц, которые всегда являются ортогональными [84-86].

В данной работе с учетом обоснований, сделанных выше необходимо рассматривать ансамбли многофазных ортогональных кодовых последовательностей. Поэтому существует необходимость определения аналитических зависимостей между диагональными коэффициентами эрмитовых матриц и их собственными векторами, которые описывают класс АМФОКП.

Задав ограничения на значения диагональных коэффициентов эрмитовых матриц в процессе синтеза возможно осуществление целенаправленного отбора уникальных структур АМФОКП. На данном этапе синтеза АМФОКП необходимо определить условия, при которых координаты собственных векторов ЭМ имеют одинаковые по модулю значения. Затем необходимо определить условия, при которых определяются различные значения фаз координат СВ ЭМ.

3.2 Определение условий равенства модулей координат собственных векторов эрмитовых матриц

Определим условия, при которых координаты СВ ЭМ имеют одинаковые по модулю значения. Для этого рассмотрим решение задачи нахождении СВ бидиагональной ЭМ, представленной в следующем виде [95]:

$$\left|A^{'}-\lambda E\right|=$$

$$=\begin{vmatrix} d_{1,1}-\lambda & a_{1,2}\cdot e^{j\cdot\varphi_{1,2}} & 0 & 0 & \cdots & 0 & 0 \\ a_{2,1}\cdot e^{-j\varphi_{2,1}} & d_{2,2}-\lambda & a_{2,3}\cdot e^{j\varphi_{2,3}} & 0 & \cdots & 0 & 0 \\ 0 & a_{3,2}\cdot e^{-j\varphi_{3,2}} & d_{3,3}-\lambda & a_{3,4}\cdot e^{j\varphi_{3,4}} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & d_{n-1,m-1}-\lambda & a_{n-1,m}\cdot e^{j\varphi_{n-1,m}} \\ 0 & 0 & 0 & 0 & 0 & a_{n,m-1}\cdot e^{-j\varphi_{n,m-1}} & d_{n,m}-\lambda \end{vmatrix} \quad (3.10)$$

Для собственного значения λ определим собственные векторы матрицы $A^{'}$. В связи с этим запишем её характеристическое уравнение в развёрнутом виде

$$\begin{cases} \left(d_{1,1}-\lambda\right)x_1+a_{1,2}\cdot e^{j\varphi_{1,2}}\cdot x_2=0, \\ a_{2,1}\cdot e^{-j\varphi_{2,1}}\cdot x_1+\left(a_{2,2}-\lambda\right)\cdot x_2+a_{2,3}\cdot e^{j\varphi_{2,3}}\cdot x_3=0, \\ a_{3,2}\cdot e^{-j\varphi_{3,2}}\cdot x_2+\left(a_{3,3}-\lambda\right)\cdot x_3+a_{3,4}\cdot e^{j\varphi_{3,4}}\cdot x_4=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a_{n-1,m-2}\cdot e^{-j\varphi_{n-1,m-2}}\cdot x_{m-2}+\left(d_{n-1,m-1}-\lambda\right)\cdot x_{m-1}+a_{n-1,m}\cdot e^{j\varphi_{n-1,m}}\cdot x_m=0, \\ a_{n,m-1}\cdot e^{-j\varphi_{n,m-1}}+\left(d_{n,m}-\lambda\right)\cdot x_m=0. \end{cases} \quad (3.11)$$

В соответствии с [57, 81, 95] в системе (3.11) отбросим последнее уравнение и присвоим произвольное значение координате $x_1=\alpha$.

Остальные координаты $x_1, x_2, x_3, \ldots, x_n$ выразим через α:

$$x_2=-\alpha\frac{d_{1,1}-\lambda}{a_{1,2}}\cdot e^{-j\varphi_{1,2}}; \quad (3.12)$$

$$\begin{aligned} x_3 &= -\alpha\frac{a_{2,1}\cdot e^{-j\varphi_{2,1}}}{a_{2,3}\cdot e^{j\varphi_{2,3}}}-\frac{d_{2,2}-\lambda}{a_{2,3}\cdot e^{j\varphi_{2,3}}}x_2= \\ &= \frac{\left(d_{2,2}-\lambda\right)\cdot\left(d_{1,1}-\lambda\right)-a_{2,1}\cdot e^{-j\varphi_{2,1}}\cdot a_{1,2}\cdot e^{j\varphi_{1,2}}}{a_{1,2}\cdot e^{j\varphi_{1,2}}\cdot a_{2,3}\cdot e^{j\varphi_{2,3}}}x_2 \\ &== \alpha\frac{\Delta_2}{a_{1,2}\cdot e^{j\varphi_{1,2}}\cdot a_{2,3}\cdot e^{j\varphi_{2,3}}}= \\ &= \alpha\frac{\Delta_2}{a_{1,2}\cdot a_{2,3}}\cdot e^{-j\left(\varphi_{1,2}+\varphi_{2,3}\right)}, \end{aligned} \quad (3.13)$$

где Δ_2 – минор, составленный из элементов первых двух строк и столбцов бидиагональной ЭМ $\left|A^{'}-\lambda E\right|$.

$$x_4 = -\frac{a_{3,2}\cdot e^{-j\varphi_{3,2}}}{a_{3,4}\cdot e^{j\varphi_{3,4}}}x_2 - \frac{d_{3,3}-\lambda}{a_{3,4}\cdot e^{j\varphi_{3,4}}}x_3$$
$$= \alpha\frac{a_{2,3}\cdot e^{j\varphi_{2,3}}\cdot a_{3,2}\cdot e^{-j\varphi_{3,2}}\cdot\left(d_{1,1}-\lambda\right)-\left(d_{3,3}-\lambda\right)\Delta_2}{a_{1,2}\cdot e^{j\varphi_{1,2}}\cdot a_{2,3}\cdot e^{j\varphi_{2,3}}\cdot a_{3,4}\cdot e^{j\varphi_{3,4}}} = \quad (3.14)$$
$$= -\alpha\frac{\Delta_3}{a_{1,2}\cdot a_{2,3}\cdot a_{3,4}}\cdot e^{-j\left(\varphi_{1,2}+\varphi_{2,3}+\varphi_{3,4}\right)},$$

где Δ_3 - минор, составленный из элементов первых трёх строк и столбцов матрицы $\left|A^{'}-\lambda E\right|$. По аналогии можно записать и в общем случае значения k-й координаты собственного вектора

$$x_k = (-1)^{k-1}\cdot\alpha\cdot\frac{\Delta_{k-1}}{a_{1,2}\cdot a_{2,3}\cdot\ldots\cdot a_{k-1,k}}\cdot e^{-j\left(\varphi_{1,2}+\varphi_{2,3}+\cdots+\varphi_{k-1,k}\right)}, \quad (3.15)$$

где $\Delta_{k-1} = \lambda^{k-1} - \lambda^{k-3}\cdot\left(a_{1,2}\cdot a_{2,1} + a_{2,3}\cdot a_{3,2} + a_{3,4}\cdot a_{4,3} + \cdots + a_{\substack{k-2,\\k-1}}\cdot a_{\substack{k-1,\\k-2}}\right) +$

$+\lambda^{k-5}\cdot\left(a_{1,2}\cdot a_{2,1}\cdot a_{3,4}\cdot a_{4,3}\cdot\ldots\cdot a_{\substack{k-4,\\k-3}}\cdot a_{\substack{k-3,\\k-4}}\cdot a_{\substack{k-2,\\k-1}}\cdot a_{\substack{k-1,\\k-2}}\right) + \cdots + \lambda\left(a_{1,2}\cdot a_{2,1}\cdot\right.$

$\left.a_{3,4}\cdot a_{4,3}\cdot\ldots\cdot a_{\substack{k/2+1`,\\k/2+2}}\cdot a_{\substack{k/2+2,\\k/2+1}} + \ldots + a_{2,3}\cdot a_{4,5}\cdot\ldots\cdot a_{\substack{k-2,\\k-1}}\right)$ – минор, составленный из элементов первых $k-1$ строк и столбцов матрицы $\left|A^{'}-\lambda E\right|$.

В работах [81, 95] показано, что для обеспечения примерного равенства модулей координат собственных векторов бидиагональных эрмитовых матриц

$$x_1 \approx x_2 \approx x_3 \approx x_4. \quad (3.16)$$

необходимо задавать значения модулей диагональных коэффициентов рассматриваемой матрицы в соответствии с выражением

$$a_{1,2} \to \lambda; a_{2,3} \to 0;\ a_{3,4} \to \lambda;\ a_{4,5} \to 0;\ \dots;\ a_{n-2,m-1} \to 0;\ a_{n-1,m} \to \lambda. \qquad (3.17)$$

С учетом изложенного, сформулируем следующее утверждение.

Утверждение 1

Для обеспечения примерного равенства модулей координат собственных векторов бидиагональных эрмитовых матриц необходимо задавать значения модулей диагональных коэффициентов рассматриваемой матрицы в соответствии с выражением (3.17)

$$a_{1,2} \to \lambda; a_{2,3} \to 0;\ a_{3,4} \to \lambda;\ a_{4,5} \to 0;\ \dots;\ a_{n-2,m-1} \to 0;\ a_{n-1,m} \to \lambda.$$

Анализ показывает, что при использовании метода итераций (последовательных приближений) для решения задачи нахождения собственных чисел и собственных векторов матрицы (3.10) в случае $N = 4$, значение аргумента координаты собственного вектора $\dot{x}_1$ может быть выбрано произвольно. Из выражения (3.12) следует, что величина аргумента координаты собственного вектора $\dot{x}_2$ определяется величиной аргумента $\varphi_{1,2}$ диагонального коэффициента $a_{1,2}$. Из выражения (3.13) следует, что значение аргумента координаты собственного вектора $\dot{x}_3$ определяется суммой значений аргументов $\varphi_{1,2} + \varphi_{2,3}$ диагональных коэффициентов $a_{1,2}$ и $a_{2,3}$. Из выражения (3.14) следует, что значение аргумента координаты собственного вектора $\dot{x}_4$ определяется суммой значений аргументов $\varphi_{1,2} + \varphi_{2,3} + \varphi_{3,4}$ диагональных коэффициентов $a_{1,2}, a_{2,3}$ и $a_{3,4}$. [100].

В общем случае, как следует из выражения (3.15) значение аргумента k-й координаты собственного вектора для произвольного порядка эрмитовой матрицы ($N = k$) будет определяться суммой значений аргументов $\varphi_{1,2} + \varphi_{2,3} + \varphi_{3,4} + \dots + \varphi_{k-1,k}$ диагональных коэффициентов $a_{1,2}, a_{2,3}, a_{3,4}, \dots, a_{k-1,k}$.

С учетом установленных зависимостей сформулируем следующее утверждение.

Утверждение 2

Значения аргументов координат собственных векторов бидиагональных эрмитовых матриц k-ого порядка определяется следующим образом: значение аргумента ψ_1 координаты собственного вектора $\dot{x}_1$ выбирается произвольно, значение аргумента ψ_2 координаты собственного вектора $\dot{x}_2$ определяется величиной аргумента $\varphi_{1,2}$, диагонального коэффициента эрмитовой матрицы $a_{1,2}$, значения всех остальных k аргументов ψ_k координат собственных векторов бидиагональных эрмитовых матриц $\dot{x}_k$ определяются суммой значений аргументов её диагональных коэффициентов, т.е.

$$\psi_k = \varphi_{1,2} + \varphi_{2,3} + \cdots + \varphi_{k-1,k}. \quad (3.18)$$

Более подробно математическое моделирование дискретных ортогональных кодовых последовательностей представлено в [96]. Таким образом, с учетом аналитических соотношений, представленных выше, можно определить условия для задания значений диагональных коэффициентов эрмитовых матриц, при которых возможно получение множества АМФОКП.

Для решения воспользуемся программой [97, 98], выполненной в среде Matlab, представленной в приложении А.

Проведем эксперимент по синтезу различных реализаций АМФОКП для размерностей $N = 4$ на основе рассмотрения собственных векторов бидиагональных эрмитовых матриц при изменяющихся значениях аргументов коэффициентов её второй диагонали, которые представлены в приложении Б.

В приложении Б представлены следующие эксперименты:

Эксперимент 1. Для случая, когда рассматривается бидиагональная эрмитова матрица четвертого порядка $N = 4$, модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения, модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения

$a_{1,2} = 100;\ a_{2,3} = 0.01;\ a_{3,4} = 100,$ диагональные коэффициенты эрмитовой матрицы третьей и четвертой диагонали равны нулю, коэффициенты главной диагонали равны нулю $d_{1,1} = 0; d_{2,2} = 0;\ d_{3,3} = 0;\ d_{4,4} = 0,$ аргументы диагональных коэффициентов второй диагонали $a_{2,3}$ и $a_{3,4}$ имеют фиксированное значений $\varphi_{2,3} = \varphi_{3,4} = 0°$, аргументы коэффициента $a_{1,2}$ второй диагонали имеют следующий набор значений $\varphi_{1,2} = 0°, 45°, 90°, 135°, 180°, 225°, 270°, 315°.$

Эксперимент 2. Для случая, когда рассматривается бидиагональная эрмитова матрица четвертого порядка N=4, модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения, модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения $a_{1,2} = 100;\ a_{2,3} = 0.01;\ a_{3,4} = 100,$ диагональные коэффициенты эрмитовой матрицы третьей и четвертой диагонали равны нулю, коэффициенты главной диагонали равны нулю $d_{1,1} = 0; d_{2,2} = 0;\ d_{3,3} = 0;\ d_{4,4} = 0,$ аргументы диагональных коэффициентов второй диагонали $a_{1,2}$ и $a_{3,4}$ имеют фиксированное значение $\varphi_{1,2} = \varphi_{3,4} = 0°$, аргументы коэффициента $a_{2,3}$ второй диагонали имеют следующий набор значений $\varphi_{2,3} = 0°, 45°, 90°, 135°, 180°, 225°, 270°, 315°.$

Эксперимент 3. Для случая, когда рассматривается бидиагональная эрмитова матрица четвертого порядка $N = 4$, модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения, модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения $a_{1,2} = 100;\ a_{2,3} = 0.01;\ a_{3,4} = 100,$ диагональные коэффициенты эрмитовой матрицы третьей и четвертой диагонали равны нулю, коэффициенты главной диагонали равны нулю $d_{1,1} = 0; d_{2,2} = 0;\ d_{3,3} = 0;\ d_{4,4} = 0,$ аргументы диагональных коэффициентов второй диагонали $a_{1,2}$ и $a_{2,3}$ имеют фиксированное значение $\varphi_{1,2} = \varphi_{2,3} = 0°$, аргументы коэффициента $a_{3,4}$ второй диагонали имеют следующий набор значений $\varphi_{3,4} = 0°, 45°, 90°, 135°, 180°, 225°, 270°, 315°.$

На основании результатов решения задач, представленных в приложении Б, можно сделать следующие выводы:

1. На значение фаз (аргументов) первых координат системы собственных векторов эрмитовой бидиагональной матрицы четвертого порядка влияет только значение фазы (аргумента) $\varphi_{1,2}$ у диагонального коэффициента $a_{1,2}$ рассматриваемой матрицы.

2. На значение фаз (аргументов) одновременно первых и вторых координат системы собственных векторов эрмитовой бидиагональной матрицы четвертого порядка влияет значение фазы (аргумента) $\varphi_{2,3}$ у диагонального коэффициента $a_{2,3}$ рассматриваемой матрицы.

3. На значение фаз (аргументов) одновременно первых, вторых и третьих координат системы собственных векторов эрмитовой бидиагональной матрицы четвертого порядка влияет значение фазы (аргумента) $\varphi_{3,4}$ у диагонального коэффициента $a_{3,4}$ рассматриваемой матрицы.

4. Одновременное изменение фаз (аргументов) всех диагональных коэффициентов бидиагональной ЭМ четвертого порядка приводит к суммарному изменению фаз (аргументов) координат собственных векторов рассматриваемых матриц в соответствии с закономерностями, установленными выше.

5. Количество различных систем собственных векторов ЭМ, описывающих АМФОКП, будет наибольшим, если одновременно рассматривать изменение фаз у всех диагональных коэффициентов ЭМ. Данное обстоятельство предлагается к применению в разрабатываемом алгоритме синтеза АМФОКП.

3.3 Разработка алгоритма синтеза увеличенного количества ансамблей многофазных ортогональных кодовых последовательностей

С учетом выявленных ранее в данном разделе закономерностей, разработаем алгоритм синтеза АМФОКП основан на работе [17] и включает в себя семь этапов.

Описанный алгоритм синтеза увеличенного количества ансамблей многофазных ортогональных кодовых последовательностей представлен на рисунке 3.4.

Первый этап. Задание исходных данных.

На данном этапе определяются следующие исходные данные:

1) размерность формируемых последовательностей N;

2) максимально-допустимое значение боковых пиков функции автокорреляции $R_i(\tau)_{\text{макс. доп.}}$;

3) максимально-допустимое значение боковых пиков функции взаимокорреляции $R_{ij}(\tau)_{\text{макс. доп.}}$;

4) K – количество формируемых АМФОКП.

Второй этап. Определение значений модулей диагональных коэффициентов бидиагональной эрмитовой матрицы размерности N вида (2.3) при которых обеспечивается примерное равенство модулей координат собственных векторов ЭМ вида (2.5).

$$x_{n,1} \approx x_{n,2} \approx x_{n,3} \approx \cdots \approx x_{n,m}, \quad n = \overline{1,N}, m = \overline{1,N}\,. \tag{3.19}$$

На этом же этапе осуществляется присвоение выбранных значений модулей диагональных коэффициентов бидиагональной эрмитовой матрицы размерности N и их фиксация при всех дальнейших этапах реализации модели синтеза.

$$a_{1,2} = a_1, a_{2,1} = a_2, \dots, a_{N-1,N} = a_{N-1}.$$

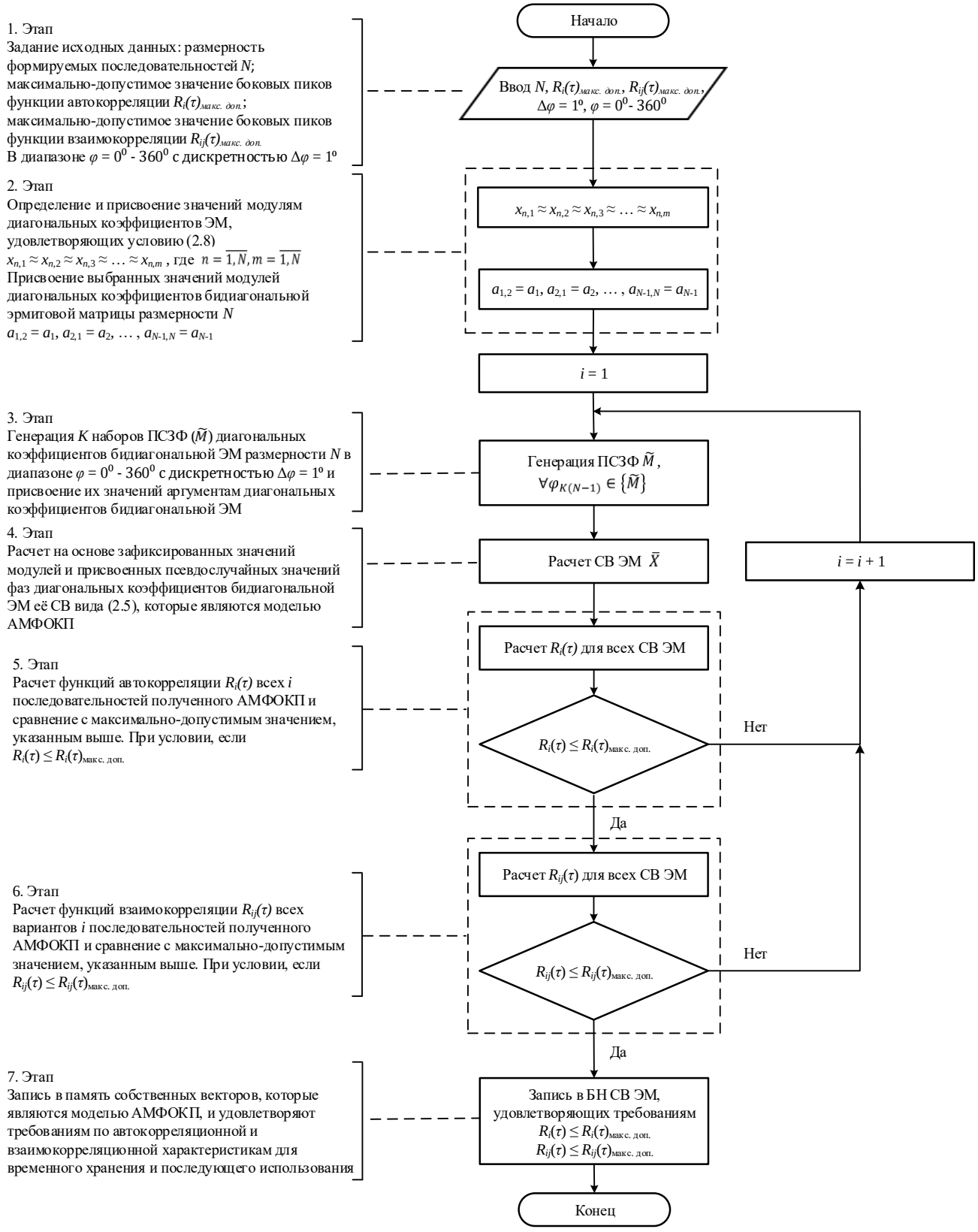


Рисунок 3.4 – Алгоритм синтеза увеличенного количества АМФОКП

Третий этап. Генерация псевдослучайных значений фаз (ПСЗФ) диагональных коэффициентов бидиагональной эрмитовой матрицы размерности N в диапазоне от $\varphi = 0^0$ до $\varphi = 360^0$ с дискретностью $\Delta\varphi = 1^0$ и присвоение их значений аргументам диагональных коэффициентов бидиагональной ЭМ.

На данном этапе формируется псевдослучайная последовательность в диапазоне значений от 0 до 360 с дискретностью $\Delta = 1$ в виде

$$\{\widetilde{M}\} = \begin{matrix}\{(\varphi_{1,1}, \varphi_{1,2}, \dots, \varphi_{1,N-1}), (\varphi_{2,1}, \varphi_{2,2}, \dots, \varphi_{2,N-1}),\\ (\varphi_{3,1}, \varphi_{3,2}, \dots, \varphi_{3,N-1}), \dots, (\varphi_{K,1}, \varphi_{K,2}, \dots, \varphi_{K,N-1})\}\end{matrix}, \quad (3.20)$$

которая представляет собой K – наборов псевдослучайных значений фаз диагональных коэффициентов бидиагональной ЭМ. При этом любое значение фаз диагональных коэффициентов бидиагональной ЭМ принадлежит множеству $\{\widetilde{M}\}$, т.е.

$$\forall\varphi_{K(N-1)} \in \{\widetilde{M}\}.$$

Например, для ЭМ четвертого порядка $N = 4$, получим

$$A_1 = \begin{bmatrix} 0 & a_1 \cdot e^{j\cdot\varphi_{1,1}} & 0 & 0 \\ a_1 \cdot e^{-j\cdot\varphi_{1,1}} & 0 & a_2 \cdot e^{j\cdot\varphi_{1,2}} & 0 \\ 0 & a_2 \cdot e^{-j\cdot\varphi_{1,2}} & 0 & a_3 \cdot e^{j\cdot\varphi_{1,3}} \\ 0 & 0 & a_3 \cdot e^{-j\cdot\varphi_{1,3}} & 0 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0 & a_1 \cdot e^{j\cdot\varphi_{2,1}} & 0 & 0 \\ a_1 \cdot e^{-j\cdot\varphi_{2,1}} & 0 & a_2 \cdot e^{j\cdot\varphi_{2,2}} & 0 \\ 0 & a_2 \cdot e^{-j\cdot\varphi_{2,2}} & 0 & a_3 \cdot e^{j\cdot\varphi_{2,3}} \\ 0 & 0 & a_3 \cdot e^{-j\cdot\varphi_{2,3}} & 0 \end{bmatrix},$$

…

$$A_K = \begin{bmatrix} 0 & a_1 \cdot e^{j\cdot\varphi_{K,1}} & 0 & 0 \\ a_1 \cdot e^{-j\cdot\varphi_{K,1}} & 0 & a_2 \cdot e^{j\cdot\varphi_{K,2}} & 0 \\ 0 & a_2 \cdot e^{-j\cdot\varphi_{K,2}} & 0 & a_3 \cdot e^{j\cdot\varphi_{K,3}} \\ 0 & 0 & a_3 \cdot e^{-j\cdot\varphi_{K,3}} & 0 \end{bmatrix}.$$

То есть модули диагональных коэффициентов бидиагональной ЭМ при каждом из K – наборов псевдослучайных значений фаз не изменяются, а изменяются значения фаз этих коэффициентов в соответствии с последовательностью $\widetilde{M}$.

Четвертый этап. Расчет на основе зафиксированных значений модулей и присвоенных псевдослучайных значений фаз диагональных коэффициентов бидиагональной эрмитовой матрицы её собственных векторов вида

$$\overline{\mathrm{X}} = \begin{pmatrix} x_{1,1} \cdot e^{j\cdot\psi_{1,1}} & x_{1,2} \cdot e^{j\cdot\psi_{1,2}} & x_{1,3} \cdot e^{j\cdot\psi_{1,3}} & x_{1,4} \cdot e^{j\cdot\psi_{1,4}} \\ x_{2,1} \cdot e^{j\cdot\psi_{2,1}} & x_{2,2} \cdot e^{j\cdot\psi_{2,2}} & x_{2,3} \cdot e^{j\cdot\psi_{2,3}} & x_{2,4} \cdot e^{j\cdot\psi_{2,4}} \\ x_{3,1} \cdot e^{j\cdot\psi_{3,1}} & x_{3,2} \cdot e^{j\cdot\psi_{3,2}} & x_{3,3} \cdot e^{j\cdot\psi_{3,3}} & x_{3,4} \cdot e^{j\cdot\psi_{3,4}} \\ x_{4,1} \cdot e^{j\cdot\psi_{4,1}} & x_{4,2} \cdot e^{j\cdot\psi_{4,2}} & x_{4,3} \cdot e^{j\cdot\psi_{4,3}} & x_{4,4} \cdot e^{j\cdot\psi_{4,4}} \end{pmatrix},$$

которые являются моделью АМФОКП.

Пятый этап. Расчет функций автокорреляции $R_i(\tau)$ всех $i = N$ последовательностей полученного АМФОКП и сравнение с максимально-допустимым значением, указанным выше. При условии, если

$$R_i(\tau) \leq R_i(\tau)_{\text{макс. доп.}},$$

то осуществляется переход к следующему этапу алгоритма синтеза.

В противном случае анализируемый АМФОКП считается не удовлетворяющим требованиям по автокорреляционной характеристике и исключается из дальнейшего рассмотрения.

Шестой этап. Расчет функций взаимокорреляции $R_{ij}(\tau)$ всех вариантов $i = N$ последовательностей полученного АМФОКП и сравнение с максимально-допустимым значением, указанным выше. При условии, если

$$R_{ij}(\tau) \leq R_{ij}(\tau)_{\text{макс. доп.}},$$

то осуществляется переход к следующему этапу алгоритма синтеза. В противном случае анализируемый АМФОКП считается не удовлетворяющим требованиям по взаимокорреляционной характеристике и исключается из дальнейшего рассмотрения.

Седьмой этап. Запись в память (буферный накопитель) найденных наборов собственных векторов $\overline{X}_i$, которые являются моделью АМФОКП, и удовлетворяют требованиям по автокорреляционной и взаимокорреляционной характеристикам для временного хранения и последующего стохастического применения.

Таким образом можно сделать вывод, что алгоритм синтеза АМФОКП, включает в себя семь этапов: определение начальных условий, определение значений модулей ДК бидиагональной ЭМ, генерация псевдослучайных значений аргументов ДК бидиагональной ЭМ, вычисление СВ ЭМ [103], расчет функций автокорреляции $R_i(\tau)$ всех $i = N$ последовательностей полученного АМФОКП и сравнение с максимально-допустимым значением, расчет функций взаимокорреляции $R_{ij}(\tau)$ всех вариантов $i = N$ последовательностей полученного АМФОКП и сравнение с максимально-допустимым значением, запись в память (буферный накопитель) найденных наборов собственных векторов $\overline{\mathrm{X}}_i$, которые являются моделью АМФОКП и удовлетворяют требованиям по автокорреляционной и взаимокорреляционной характеристикам [103].

Автором экспериментально было установлено, что модули координат СВ ЭМ имеют равные значения при следующих значениях модулей диагональных коэффициентов ЭМ.

Для бидиагональной ЭМ четвертого порядка $N = 4$ модули диагональных коэффициентов второй диагонали могут иметь следующие значения: $a_{1,2} = 100;\ a_{2,3} = 0.01;\ a_{3,4} = 100$. При этих модулях диагональных коэффициентов модули координат СВ равны между собой.

Для бидиагональной ЭМ 128-го порядка $N = 128$ модули диагональных коэффициентов второй диагонали могут иметь следующие значения:

$a_{1,2} = 100;\ a_{2,3} = 1;\ a_{3,4} = 100;\ a_{4,5} = 0{,}05\ a_{5,6} = 100;\ a_{6,7} = 1;\ a_{7,8} = 100;$
$a_{8,9} = 0{,}0025; a_{9,10} = 100;\ a_{10,11} = 1;\ a_{11,12} = 100; a_{12,13} = 0{,}05;\ a_{13,14} = 100;$
$a_{14,15} = 1; a_{15,16} = 100; a_{16,17} = 0{,}0001; a_{17,18} = 100; a_{18,19} = 1; a_{19,20} = 100;$
$a_{20,21} = 0{,}05; a_{21,22} = 100; a_{22,23} = 1; a_{23,24} = 100; a_{24,25} = 0{,}0025; a_{25,26} = 100;$
$a_{26,27} = 1; a_{27,28} = 100; a_{28,29} = 0{,}05; a_{29,30} = 100; a_{30,31} = 1; a_{31,32} = 100;$
$a_{32,33} = 0{,}0001; a_{33,34} = 100; a_{34,35} = 1;\ a_{35,36} = 100;\ a_{36,37} = 0{,}05;$
$a_{37,38} = 100; a_{38,39} = 1; a_{39,40} = 100; a_{40,41} = 0{,}0025; a_{41,42} = 100; a_{42,43} = 1;$
$a_{43,44} = 100; a_{44,45} = 0{,}05; a_{45,46} = 100; a_{46,47} = 1; a_{47,48} = 100;$
$a_{48,49} = 0{,}0001; a_{49,50} = 100; a_{50,51} = 1; a_{51,52} = 100; a_{52,53} = 0{,}05; a_{53,54} = 100;$
$a_{54,55} = 1;\ a_{55,56} = 100; a_{56,57} = 0{,}0025; a_{57,58} = 100; a_{58,59} = 1; a_{59,60} = 100;$
$a_{60,61} = 0{,}05;\ a_{61,62} = 100; a_{62,63} = 1; a_{63,64} = 100;\ a_{64,65} = 0{,}00001 + 10i;$
$a_{65,66} = 100;\ a_{66,67} = 1;\ a_{67,68} = 100;\ a_{68,69} = 0{,}05\ a_{69,70} = 100;\ a_{70,71} = 1;$
$a_{71,72} = 100; a_{72,73} = 0{,}0025; a_{73,74} = 100; a_{74,75} = 1; a_{75,76} = 100; a_{76,77} = 0{,}05;$
$a_{77,78} = 100; a_{78,79} = 1; a_{79,80} = 100; a_{80,81} = 0{,}0001; a_{81,82} = 100; a_{82,83} = 1;$
$a_{83,84} = 100; a_{84,85} = 0{,}05; a_{85,86} = 100; a_{86,87} = 1; a_{87,88} = 100; a_{88,89} = 0{,}0025;$
$a_{89,90} = 100; a_{90,91} = 1; a_{91,92} = 100; a_{92,93} = 0{,}05; a_{93,94} = 100; a_{94,95} = 1;$
$a_{95,96} = 100; a_{96,97} = 0{,}0001; a_{97,98} = 100;\ a_{98,99} = 1;\ a_{99,100} = 100;$
$a_{100,101} = 0{,}05;\ a_{101,102} = 100;\ \ a_{102,103} = 1; a_{103,104} = 100; a_{104,105} = 0{,}0025;$
$a_{105,106} = 100; a_{106,107} = 1; a_{107,108} = 100; a_{108,109} = 0{,}05; a_{109,110} = 100;$
$a_{110,111} = 1; a_{111,112} = 100; a_{112,113} = 0{,}0001; a_{113,114} = 100; a_{114,115} = 1;$
$a_{115,116} = 100; a_{116,117} = 0{,}05;\ a_{117,118} = 100; a_{118,119} = 1;\ a_{119,120} = 100;$
$a_{120,121} = 0{,}0025; a_{121,122} = 100; a_{122,123} = 1; a_{123,124} = 100; a_{124,125} = 0{,}05;$

$a_{125,126} = 100; a_{126,127} = 1; a_{127,128} = 100.$

Для бидиагональной ЭМ 256-го порядка $N = 256$ модули диагональных коэффициентов второй диагонали могут иметь следующие значения:

$a_{1,2} = 100;\ a_{2,3} = 1;\ a_{3,4} = 100;\ a_{4,5} = 0{,}05\ a_{5,6} = 100;\ a_{6,7} = 1;\ a_{7,8} = 100;$

$a_{8,9} = 0{,}0025; a_{9,10} = 100;\ a_{10,11} = 1;\ a_{11,12} = 100; a_{\ 12,13} = 0{,}05;\ a_{13,14} = 100;$

$a_{14,15} = 1; a_{15,16} = 100; a_{16,17} = 0{,}0001; a_{17,18} = 100; a_{18,19} = 1; a_{19,20} = 100;$

$a_{20,21} = 0{,}05; a_{21,22} = 100; a_{22,23} = 1; a_{23,24} = 100; a_{24,25} = 0{,}0025; a_{25,26} = 100;$

$a_{26,27} = 1; a_{27,28} = 100; a_{28,29} = 0{,}05; a_{29,30} = 100; a_{30,31} = 1; a_{31,32} = 100;$

$a_{32,33} = 0{,}0001; a_{33,34} = 100; a_{34,35} = 1;\ a_{35,36} = 100;\ a_{36,37} = 0{,}05;$

$a_{37,38} = 100; a_{38,39} = 1; a_{39,40} = 100; a_{40,41} = 0{,}0025; a_{41,42} = 100; a_{42,43} = 1;$

$a_{43,44} = 100; a_{44,45} = 0{,}05; a_{45,46} = 100; a_{46,47} = 1; a_{47,48} = 100;$

$a_{48,49} = 0{,}0001; a_{49,50} = 100; a_{50,51} = 1; a_{51,52} = 100; a_{52,53} = 0{,}05; a_{53,54} = 100;$

$a_{54,55} = 1;\ a_{55,56} = 100; a_{56,57} = 0{,}0025; a_{57,58} = 100; a_{58,59} = 1; a_{59,60} = 100;$

$a_{60,61} = 0{,}05;\ a_{61,62} = 100; a_{62,63} = 1; a_{63,64} = 100;\ a_{64,65} = 0{,}00001;$

$a_{65,66} = 100;\ a_{66,67} = 1;\ a_{67,68} = 100;\ a_{68,69} = 0{,}05\ a_{69,70} = 100;\ a_{70,71} = 1;$

$a_{71,72} = 100; a_{72,73} = 0{,}0025; a_{73,74} = 100; a_{74,75} = 1; a_{75,76} = 100; a_{76,77} = 0{,}05;$

$a_{77,78} = 100; a_{78,79} = 1; a_{79,80} = 100; a_{80,81} = 0{,}0001; a_{81,82} = 100; a_{82,83} = 1;$

$a_{83,84} = 100; a_{84,85} = 0{,}05; a_{85,86} = 100; a_{86,87} = 1; a_{87,88} = 100; a_{88,89} = 0{,}0025;$

$a_{89,90} = 100; a_{90,91} = 1; a_{91,92} = 100; a_{92,93} = 0{,}05; a_{93,94} = 100; a_{94,95} = 1;$

$a_{95,96} = 100; a_{96,97} = 0{,}0001; a_{97,98} = 100;\ a_{98,99} = 1;\ a_{99,100} = 100;$

$a_{100,101} = 0{,}05;\ a_{101,102} = 100;\ \ a_{102,103} = 1; a_{103,104} = 100; a_{104,105} = 0{,}0025;$

$a_{105,106} = 100; a_{106,107} = 1; a_{107,108} = 100; a_{108,109} = 0{,}05; a_{109,110} = 100;$

$a_{110,111} = 1; a_{111,112} = 100; a_{112,113} = 0{,}0001; a_{113,114} = 100; a_{114,115} = 1;$

$a_{115,116} = 100; a_{116,117} = 0{,}05;\ a_{117,118} = 100; a_{118,119} = 1;\ a_{119,120} = 100;$

$a_{120,121} = 0{,}0025; a_{121,122} = 100; a_{122,123} = 1; a_{123,124} = 100; a_{124,125} = 0{,}05;$

$a_{125,126} = 100; a_{126,127} = 1; a_{127,128} = 100;\ a_{128,129} = 0{,}00000001 + 10i;$

$a_{129,130} = 100;\ a_{130,131} = 1;\ a_{131,132} = 100;\ a_{132,133} = 0{,}05\ a_{133,134} = 100;$

$a_{134,135} = 1;\ a_{135,136} = 100; a_{136,137} = 0{,}0025; a_{137,138} = 100;\ a_{138,139} = 1;$

$a_{139,140} = 100; a_{140,141} = 0{,}05;\ a_{141,142} = 100; a_{142,143} = 1; a_{143,144} = 100;$
$a_{144,145} = 0{,}0001; a_{145,146} = 100; a_{146,147} = 1; a_{147,148} = 100; a_{148,149} = 0{,}05;$
$a_{149,150} = 100; a_{150,151} = 1; a_{151,152} = 100; a_{152,153} = 0{,}0025; a_{153,154} = 100;$
$a_{154,155} = 1; a_{155,156} = 100; a_{156,157} = 0{,}05; a_{157,158} = 100; a_{158,159} = 1;$
$a_{159,160} = 100; a_{160,161} = 0{,}0001; a_{161,162} = 100; a_{162,163} = 1;\ a_{163,164} = 100;$
$a_{164,165} = 0{,}05; a_{165,166} = 100; a_{166,167} = 1; a_{167,168} = 100; a_{168,169} = 0{,}0025;$
$a_{169,170} = 100; a_{170,171} = 1;\ a_{171,172} = 100; a_{172,173} = 0{,}05; a_{173,174} = 100;$
$a_{174,175} = 1; a_{175,176} = 100; a_{176,177} = 0{,}0001; a_{177,178} = 100; a_{178,179} = 1;$
$a_{179,180} = 100; a_{180,181} = 0{,}05; a_{181,182} = 100; a_{182,183} = 1;\ a_{183,184} = 100;$
$a_{184,185} = 0{,}0025; a_{185,186} = 100; a_{186,187} = 1; a_{187,188} = 100; a_{188,189} = 0{,}05;$
$a_{189,190} = 100; a_{190,191} = 1; a_{191,192} = 100;\ a_{192,193} = 0{,}00001; a_{193,194} = 100;$
$a_{194,195} = 1;\ a_{195,196} = 100;\ a_{196,197} = 0{,}05\, a_{197,198} = 100;\ a_{198,199} = 1;$
$a_{199,200} = 100; a_{200,201} = 0{,}0025; a_{201,202} = 100; a_{202,203} = 1; a_{203,204} = 100;$
$a_{204,205} = 0{,}05;\ a_{205,206} = 100; a_{206,207} = 1; a_{207,208} = 100; a_{208,209} = 0{,}0001;$
$a_{209,210} = 100; a_{210,211} = 1;\ a_{211,212} = 100; a_{212,213} = 0{,}05; a_{213,214} = 100;$
$a_{214,215} = 1; a_{215,216} = 100; a_{216,217} = 0{,}0025;\ a_{217,218} = 100; a_{218,219} = 1;$
$a_{219,220} = 100; a_{220,221} = 0{,}05; a_{221,222} = 100; a_{222,223} = 1; a_{223,224} = 100;$
$a_{224,225} = 0{,}0001; a_{225,226} = 100;\ a_{226,227} = 1;\ a_{227,228} = 100;\ a_{228,229} = 0{,}05;$
$a_{229,230} = 100;\ \ a_{230,231} = 1; a_{231,232} = 100; a_{232,233} = 0{,}0025;\ a_{233,234} = 100;$
$a_{234,235} = 1; a_{235,236} = 100; a_{236,237} = 0{,}05; a_{237,238} = 100; a_{238,239} = 1;$
$a_{239,240} = 100; a_{240,241} = 0{,}0001; a_{241,242} = 100; a_{242,243} = 1; a_{243,244} = 100;$
$a_{244,245} = 0{,}05;\ a_{245,246} = 100; a_{246,247} = 1;\ a_{247,248} = 100;\ a_{248,249} = 0{,}0025;$
$a_{249,250} = 100; a_{250,251} = 1; a_{251,252} = 100; a_{252,253} = 0{,}05;\ a_{253,254} = 100;$
$a_{254,255} = 1; a_{255,256} = 100.$

При этих модулях диагональных коэффициентов модули координат СВ также равны между собой.

Для практического подтверждения применимости разработанного алгоритма синтеза увеличенного количества АМФОКП автором была разработана программа

синтеза АМФОКП на основе собственных векторов эрмитовых матриц, представленная в приложении А. На основе разработанной программы проведены эксперименты по решению задач синтеза АМФОКП размерности $N = 4$, которые представлены в приложении Б.

С помощью программы проведены экспериментальные исследования по синтезу ансамблей двоичных ортогональных кодовых последовательностей размерности $N = 128$, представленные на рисунке 3.5, размерности $N = 256$, представленные на рисунке 3.6, которые свидетельствуют о применимости разработанного алгоритма синтеза увеличенного количества АМФОКП.

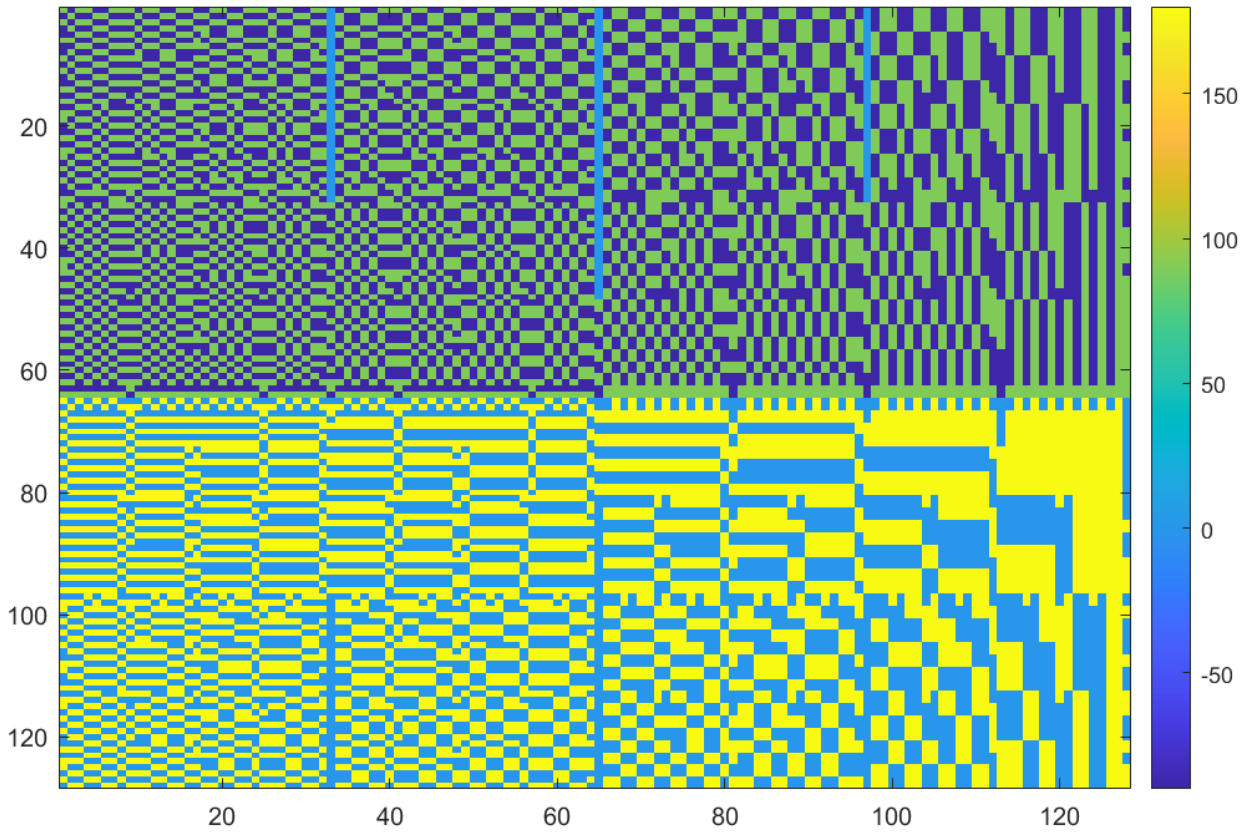


Рисунок 3.5 – Вариант синтезированного АМФОКП размерности $N = 128$

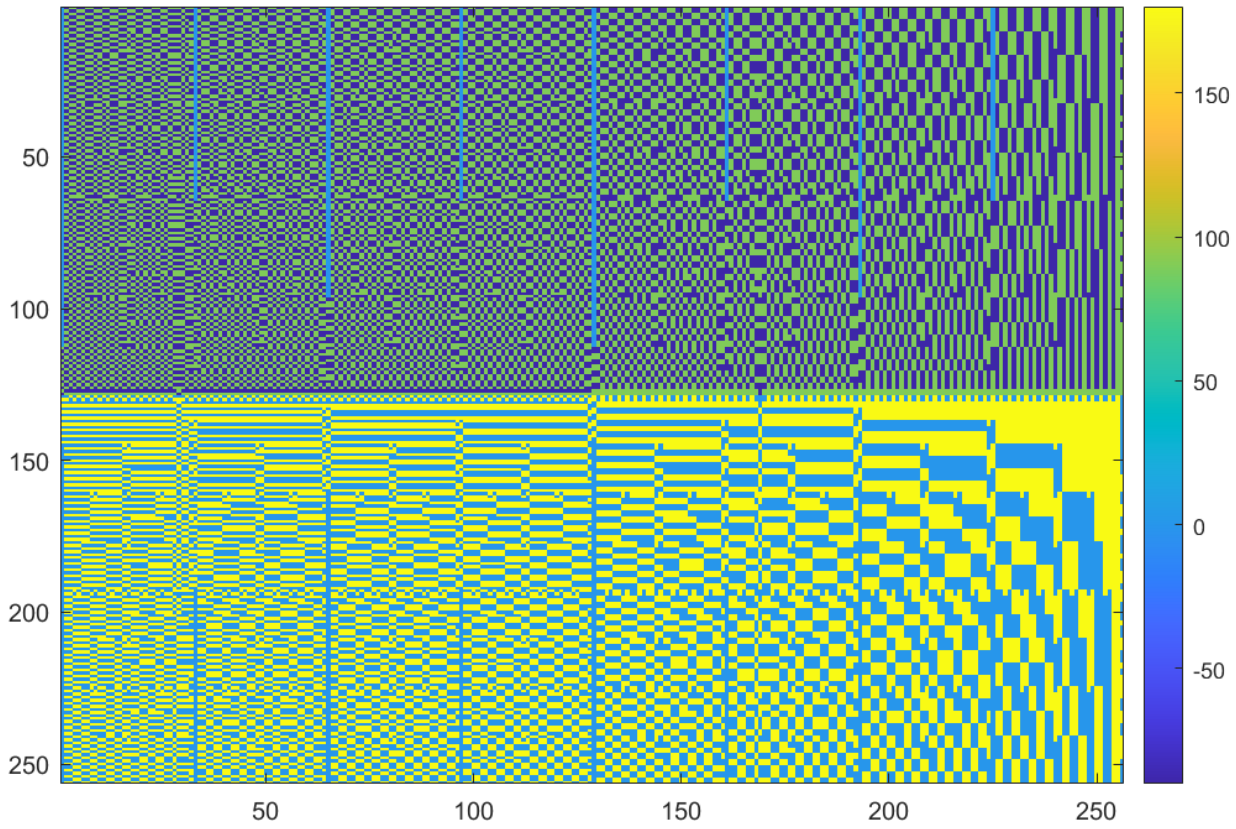


Рисунок 3.6 – Вариант синтезированного АМФОКП размерности $N = 256$

На рисунках 3.5 и 3.6 желтым цветом обозначены элементы кодовых последовательностей, имеющих значения фазы $\varphi = 180°$, голубым цветом обозначены элементы кодовых последовательностей, имеющих значения фазы $\varphi = 0°$, зеленым цветом обозначены элементы кодовых последовательностей, имеющих значения фазы $\varphi = 90°$, синим цветом обозначены элементы кодовых последовательностей, имеющих значения фазы $\varphi = -90°$.

Анализ результатов синтеза показывает, что разработанный алгоритм синтеза увеличенного количества АМФОКП, показанный на рисунке 3.4 позволяет синтезировать АМФОКП заданных размерностей.

Таким образом для случая синтеза ансамблей многофазных ортогональных кодовых последовательностей их изображение имеет количество градаций цвета, соответствующее количеству фаз элементов СВ ЭМ.

3.4 Оценка структурной скрытности ансамблей многофазных ортогональных кодовых последовательностей

Для оценки структурной скрытности АМФОКП, предназначенных для стохастического применения в ССС с КРК, проведем расчет их количества на примере бидиагональной ЭМ четвертого порядка ($n = 4$).

В бидиагональной ЭМ вида (3.5) элементы главной диагонали обязательно вещественные, а диагональные коэффициенты являются комплексно-сопряженными числами, т.е.

$$A_{k,l} \cdot e^{-i \cdot \varphi_{k,l}} = A_{l,k} \cdot e^{i \cdot \varphi_{l,k}}. \quad (3.21)$$

У комплексно-сопряженных чисел бидиагональной ЭМ модули равны, т.е. $|A_{k,l}| = |A_{l,k}|$, а аргументы $-\varphi_{k,l} = \varphi_{l,k}$ комплексно-сопряжены.

При этом коэффициенты главной диагонали $d_{1,1}$, $d_{2,2}$,…, $d_{n,n}$ являются вещественными числами.

В зависимости от значений модулей и аргументов, присваиваемых коэффициентам бидиагональной ЭМ вида 3.5, осуществляется получение модели АМФОКП системой собственных векторов вида (3.8).

Для расчета количества уникальных АМФОКП, получаемых на основе СВ бидиагональной ЭМ, необходимо [116]:

– определить диапазон значений фаз коэффициентов бидиагональной ЭМ, при котором возможно получение уникальных АМФОКП;

– определить значения СВ бидиагональной ЭМ, описываемой выражением (3.5), позволяющие получить ансамбль из N сигналов для каждого дискретного минимального значения фазы с шагом $\Delta\varphi_{k,l} = 1°$ у диагональных коэффициентов $A_{l,k}$ бидиагональной ЭМ на тригонометрической окружности $360°$.

Определим общее количество АМФОКП, получаемых при изменении фазы одного диагонального коэффициента $A_{l,k} \cdot e^{i \cdot \varphi_{l,k}}$ бидиагональной ЭМ на угол $\Delta\varphi$.

Количество используемых фаз K рассматриваемого диагонального коэффициента A бидиагональной ЭМ будет определяться отношением возможного количества градусов на тригонометрической окружности к шагу изменения фазы $\Delta\varphi$. Таким образом количество используемых фаз K при учете ранее описанных ограничений и условий будет определяться по следующей формуле:

$$K_i = \frac{360°}{\Delta\varphi_i}, \tag{3.22}$$

где K_i – общее количество АМФОКП при изменении фазы i −ого коэффициента бидиагональной ЭМ на угол $\Delta\varphi_i$.

Например, при условии, что $\Delta\varphi_i = 1°$, получим K=360, а при условии, что $\Delta\varphi = 36°$, получим $K = 10$.

Для примера в таблице 3.1 представлены АМФОКП, полученные при значении фазы $\varphi_{1,2} = 45°$ коэффициента $A_{1,2}$. Для коэффициентов $A_{2,3}$ и $A_{3,4}$ $\varphi_{2,3} = \varphi_{3,4} = 0°$.

Таблица 3.1 – АМФОКП, полученные при значениях фаз коэффициентов $\varphi_{1,2} = 45°$, $\varphi_{2,3} = 0°$,$\varphi_{3,4} = 0°$

№	Значения последовательностей $X_1 - X_4$			
X_1	$0.5e^{i45°}$	$-0.5e^{i \cdot 0°}$	$0.5e^{i \cdot 0°}$	$-0.5e^{i \cdot 0°}$
X_2	$0.5e^{i45°}$	$-0.5e^{i \cdot 0°}$	$-0.5e^{i \cdot 0°}$	$0.5e^{i \cdot 0°}$
X_3	$0.5e^{i45°}$	$0.5e^{i \cdot 0°}$	$-0.5e^{i \cdot 0°}$	$-0.5e^{i \cdot 0°}$
X_4	$0.5e^{-i45°}$	$-0.5e^{i \cdot 0°}$	$-0.5e^{i \cdot 0°}$	$-0.5e^{i \cdot 0°}$

На рисунке 3.7 представлены АМФОКП, иллюстрирующие последовательности $X_1 - X_4$ по данным из таблицы 3.1.

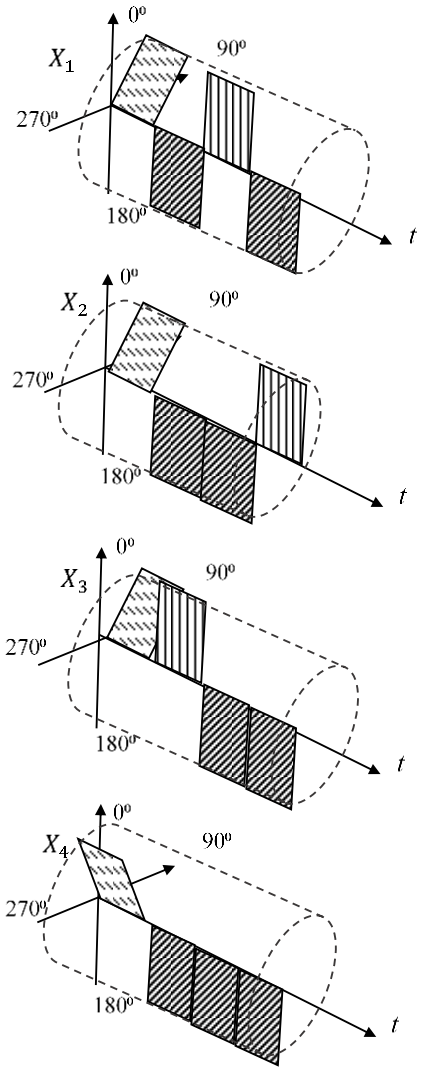


Рисунок 3.7 – Последовательности X_1 $-X_4$ при значениях фаз коэффициентов $\varphi_{1,2} = 45°$, $\varphi_{2,3} = 0°$,$\varphi_{3,4} = 0°$

Следует учитывать, что возможно одновременное изменение фаз всех трех диагональных коэффициентов ЭМ четвертого порядка $A_{1,2}$, $A_{2,3}$, $A_{3,4}$.

Из выражения (3.21) следует, что количество значений фаз у диагональных коэффициентов ЭМ будет зависеть от величины изменения угла фазы $\Delta\varphi$ на тригонометрической окружности от 0° до 360°.

Поскольку нам необходимо найти количество комбинаций при одновременном изменении фаз всех диагональных коэффициентов ЭМ воспользуемся комбинаторным принципом умножения [101]

$$Q = K_1 \cdot K_2 \cdot K_3, \tag{3.23}$$

где K_1 – количество вариантов фаз, принимаемых первым диагональным коэффициентом ЭМ, K_2 и K_3 соответственно – количество различных вариантов фаз, принимаемых вторым и третьим диагональными коэффициентами ЭМ.

Вследствие того, что одновременно изменяемое количество диагональных коэффициентов бидиагональной ЭМ, зависит от ее порядка (размерности) n, то количество сомножителей в выражении (3.23) будет всегда на единицу меньше n и равно $n-1$, поскольку во второй диагонали бидиагональной ЭМ количество диагональных коэффициентов на единицу меньше порядка (размерности) ЭМ n.

В общем случае формула для определения количества вариантов возможных значений фаз, принимаемых всеми диагональными элементами бидиагональной ЭМ $n-$ го порядка примет вид

$$Q = \prod_{i=1}^{n-1} K_i. \tag{3.24}$$

С учетом утверждения 1 и утверждения 2, сделанных в третьей главе данной работы, которые определяют прямую взаимосвязь между аргументами диагональных коэффициентов ЭМ и аргументами координат СВ ЭМ, здесь и далее будем отождествлять количество вариантов изменения фаз у аргументов диагональных коэффициентов ЭМ с количеством вариантов изменения фаз у аргументов координат СВ ЭМ.

При изменении фазы, принимаемых всеми диагональными элементами бидиагональной ЭМ на угол $\Delta\varphi_i = 1°$, рассчитаем количество АМФОКП и их структурную скрытность.

Тогда при условии $\Delta\varphi_i = 1°$ и $n = 4$, общее количество АМФОКП равно

$$Q = \prod_{1}^{3} 360 = \ 4.666 \cdot 10^{7} \ .$$

Аналогично можно рассчитать количество АМФОКП для бидиагональной ЭМ более высоких порядков. В таблице 3.2 представлены результаты расчетов для матриц порядков $n = 8, 16, 32, 64, 128, 256$, рассчитанные по формуле (3.24) при условии, что фаза каждого элемента кодовой последовательности изменяется на угол $\Delta\varphi_i = 1°$.

Таблица 3.2 – Результаты расчетов количества АМФОКП Q при условии, что фаза каждого элемента кодовой последовательности изменяется на угол $\Delta\varphi_i = 1°$

Порядок матрицы, n	Количество АМФОКП, Q
4	$4{,}67 \cdot 10^{7}$
8	$7{,}84 \cdot 10^{17}$
16	$2{,}21 \cdot 10^{38}$
32	$1{,}76 \cdot 10^{79}$
64	$1{,}11 \cdot 10^{161}$
128	$6{,}46 \cdot 10^{324}$
256	$5{,}37 \cdot 10^{651}$

Результаты расчетов количества АМФОКП при условии, что фаза каждого элемента кодовой последовательности изменяется на угол $\Delta\varphi_i = 1°$ можно принять за максимально-возможное (потенциальное) количество структур последовательностей, поскольку фаза каждого диагонального коэффициента исходной бидиагональной ЭМ изменяется в процессе получения оригинальной последовательности на минимальный угол $\Delta\varphi_i = 1°$.

На основании результатов расчетов количества АМФОКП Q при условии $\Delta\varphi_i = 1°$ рассчитаем структурную скрытность АМФОКП S_Q по следующей формуле

$$S_Q = \log_2 Q = \log_2 \prod_{i=1}^{n-1} K_i = (n-1) \cdot \log_2 K, \qquad (3.25)$$

где K – количество различных вариантов фаз, принимаемых диагональным коэффициентом ЭМ при условии, что все диагональные коэффициенты ЭМ принимают одинаковое количество значений фаз.

По результатам вычислений по формулам (3.22) и (3.25) составим таблицу 3.3 с полученными значениями структурной скрытности АМФОКП при условии изменения фазы каждого диагонального коэффициента ЭМ и соответственно фазы каждого элемента кодовой последовательности изменяется на угол $\Delta\varphi_i = 1°$.

Таблица 3.3 – Результаты расчетов структурной скрытности АМФОКП при условии изменении фазы каждого элемента кодовой последовательности на угол $\Delta\varphi_i = 1°$

Порядок матрицы, n	Структурная скрытность АМФОКП, $S_{\text{потенц}}$, ДИЗ
4	25,48
8	59,44
16	127,38
32	263,25
64	534,99
128	1078,00
256	2165,00

Расчеты структурной скрытности $S_{\text{потенц}}$ АМФОКП при условии, что диагональные коэффициенты бидиагональной ЭМ порядка n, могут принимать все возможные значения для каждого дискретного минимального значения фазы с шагом $\Delta\varphi_i = 1°$. Поэтому данное значение структурной скрытности можно назвать потенциальной структурной скрытностью $S_{\text{потенц}}$, потому что элементы рассматриваемых последовательностей меняют значения фазы с минимальным углом фазы $\Delta\varphi_i = 1°$.

Для оценки реальной структурной скрытности будем исходить из

следующего условия. Поскольку в ССС с КРК как установлено в главе 1 используются следующие виды модуляции QPSK с минимальным углом фазового сдвига $\Delta\varphi_i = 90°$ и 16-QAM с минимальным углом фазового сдвига $\Delta\varphi_i = 18°$, то будем считать возможное количество АМФОКП с учетом указанных значений фазового сдвига. Данные значения фазового сдвига очевидно обнаруживаются фазовым детектором ССС с КРК. Поэтому выберем эти значения фазового сдвига для расчета общего количества АМФОКП и показателя их структурной скрытности для случая стохастического применения в реальных условиях с учетом ограничений, накладываемых фазовым детектором ССС с КРК на минимальный угол фазового сдвига.

Рассчитаем количество АМФОКП для бидиагональной ЭМ при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 18°$ по формуле (3.24). В таблице 3.4 показаны расчеты количества АМФОКП для матриц порядков $n = 8, 16, 32, 64, 128, 256$, рассчитанные по формуле (3.24).

Таблица 3.4 – Результаты расчетов количества АМФОКП при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 18°$

Порядок матрицы, n	Количество АМФОКП, Q
4	$8{,}00 \cdot 10^{3}$
8	$1{,}28 \cdot 10^{9}$
16	$3{,}28 \cdot 10^{19}$
32	$2{,}15 \cdot 10^{40}$
64	$9{,}22 \cdot 10^{81}$
128	$1{,}70 \cdot 10^{165}$
256	$5{,}43 \cdot 10^{331}$

Также рассчитаем структурную скрытность АМФОКП $S_{\text{АМФОКП}}$ при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 18°$, соответствующий 16-QAM по формулам (3.22) и (3.25).

По результатам вычислений структурной скрытности АМФОКП $S_{\text{АМФОКП}}$ при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 18°$ составим таблицу 3.5 с полученными значениями.

Таблица 3.5 – Результаты расчетов структурной скрытности АМФОКП $S_{\text{АМФОКП}}$ при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 18°$

Порядок матрицы, n	Структурная скрытность АМФОКП, $S_{\text{АМФОКП}}$, ДИЗ
4	12,97
8	30,25
16	64,83
32	133,98
64	272,28
128	548,89
256	1102,00

Рассчитаем количество АМФОКП для бидиагональной ЭМ при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 90°$ по формуле (3.24). В таблице 3.6 показаны расчеты количества АМФОКП для матриц порядков $n = 8, 16, 32, 64, 128, 256$, рассчитанные по формуле (3.24).

Таблица 3.6 – Результаты расчетов количества АМФОКП при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 90°$

Порядок матрицы, n	Количество АМФОКП, Q
4	64
8	$1{,}64 \cdot 10^{4}$
16	$1{,}08 \cdot 10^{9}$
32	$4{,}61 \cdot 10^{18}$
64	$8{,}52 \cdot 10^{37}$
128	$2{,}89 \cdot 10^{76}$
256	$3{,}35 \cdot 10^{153}$

Также рассчитаем структурную скрытность АМФОКП $S_{\text{АМФОКП}}$ при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 90°$ соответствующий QPSK по формулам (3.22) и (3.25).

По результатам вычислений структурной скрытности АМФОКП $S_{\text{АМФОКП}}$ при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 90°$

составим таблицу 3.7 с полученными значениями.

Таблица 3.7 – Результаты расчетов структурной скрытности АМФОКП $S_{\text{АМФОКП}}$ при угле фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 90°$

Порядок матрицы, n	Структурная скрытность АМФОКП, $S_{\text{АМФОКП}}$, ДИЗ
4	6
8	14
16	30
32	62
64	126
128	254
256	510

По результатам расчетов в таблице 3.8 приведем численные значения количества АМФОКП Q при углах фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$ $\Delta\varphi_i = 90°$ и АДОМУС для порядков матрицы $N = 128, 256$

Таблица 3.8 – Численные значения количества АМФОКП Q при $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$ $\Delta\varphi_i = 90°$ и АДОМУС для порядков матрицы $N = 128, 256$

Порядок матрицы, N	Количество АМФОКП при $\Delta\varphi_i = 1°$, Q	Количество АМФОКП при $\Delta\varphi_i = 18°$, Q	Количество АМФОКП при $\Delta\varphi_i = 90°$, Q	Количество АДОМУС, Q
128	$6{,}46\cdot10^{324}$	$1{,}70\cdot10^{165}$	$2{,}89\cdot10^{76}$	$1{,}59\cdot10^{161}$
256	$5{,}37\cdot10^{651}$	$5{,}43\cdot10^{331}$	$3{,}35\cdot10^{153}$	$1{,}62\cdot10^{324}$

Сравнительный анализ численных значений количества АМФОКП Q, приведенных в таблице 3.8 показал, что разработанные модель АМФОКП и алгоритм их синтеза обладают преимуществами по сравнению с известными АДОМУС в количестве синтезируемых ансамблей ортогональных кодовых

последовательностей при углах фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$.

В таблице 3.9 приведем численные значения показателей структурной скрытности АДОМУС $S_{\text{АДОМУС}}$ и АМФОКП $S_{\text{АМФОКП}}$ при углах фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$, $\Delta\varphi_i = 90°$.

Таблица 3.9 – Численные значения показателей структурной скрытности АДОМУС $S_{\text{АДОМУС}}$ и АМФОКП $S_{\text{АМФОКП}}$ при углах фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$, $\Delta\varphi_i = 90°$

Порядок матрицы, n	Структурная скрытность АДОМУС, $S_{\text{АДОМУС}}$	Структурная скрытность АМФОКП, $S_{\text{АМФОКП}}$ при $\Delta\varphi_i = 1°$	Структурная скрытность АМФОКП, $S_{\text{АМФОКП}}$ при $\Delta\varphi_i = 18°$	Структурная скрытность АМФОКП, $S_{\text{АМФОКП}}$ при $\Delta\varphi_i = 90°$
4	10,98	25,48	12,97	6
8	27,9	59,44	30,25	14
16	61,74	127,38	64,83	30
32	129,42	263,25	133,98	62
64	264,78	534,99	272,28	126
128	535,5	1078	548,88	254
256	1077	2165	1102	510

По результатам численных значений показателя структурной скрытности S, представленным в таблице 3.9 построим графики зависимостей структурных скрытностей АДОМУС и АМФОКП, получаемых при изменении фазового сдвига между элементами кодовой последовательности на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$, и $\Delta\varphi_i = 90°$ от длины последовательностей L (рисунок 3.8).

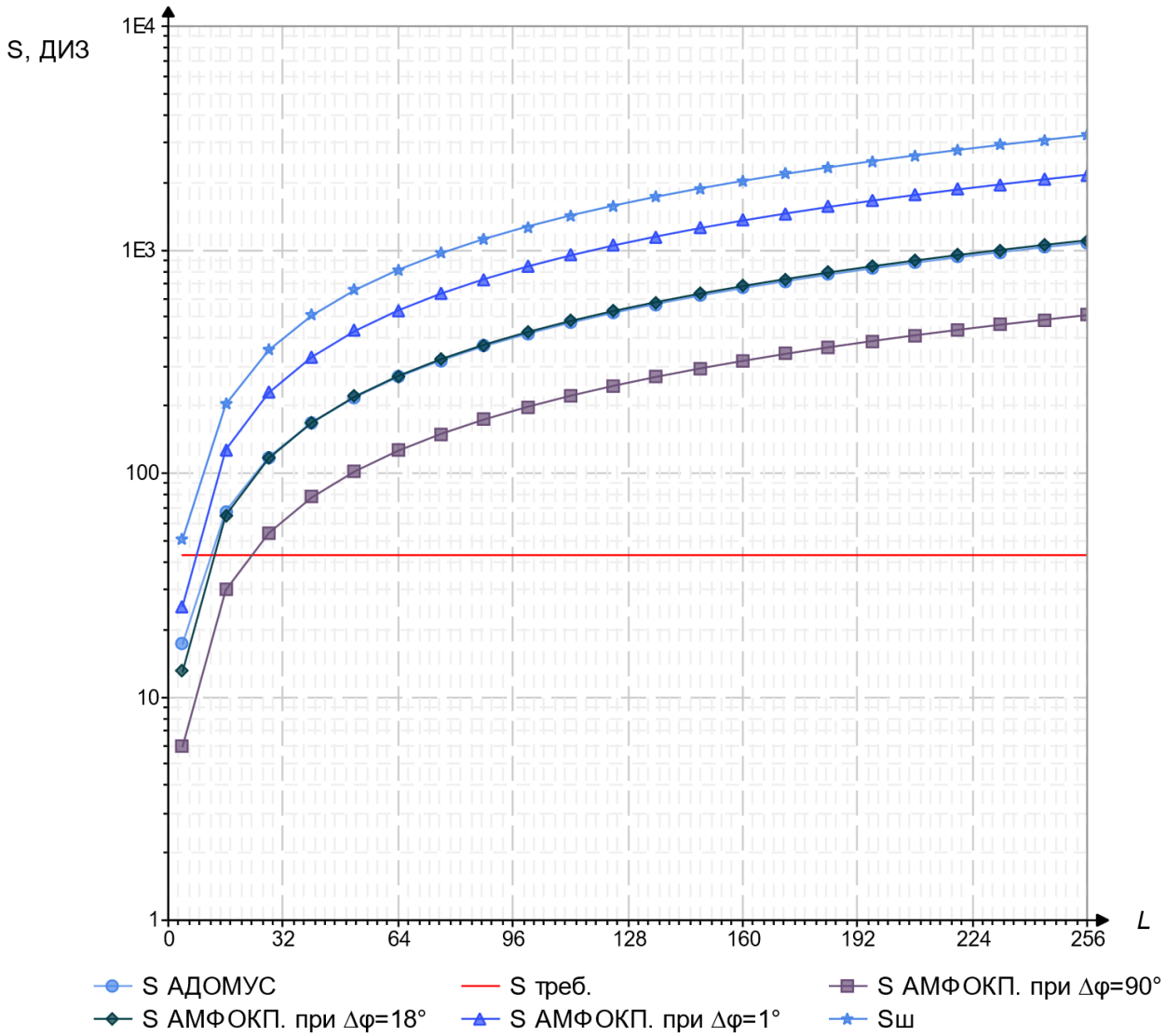


Рисунок 3.8 – Графики зависимостей структурных скрытностей АДОМУС и АМФОКП, получаемых при изменении фазового сдвига между элементами кодовой последовательности на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$, и $\Delta\varphi_i = 90°$ от длины последовательностей L

В соответствии с полученными результатами найдем абсолютное значение прироста структурной скрытности ΔS при стохастическом применении АМФОКП, получаемых при изменениях фазового сдвига между элементами кодовой последовательности на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$ по сравнению со структурной скрытностью АДОМУС $S_{\text{АДОМУС}}$.

Расчет отношения выполним по следующей формуле

$$\Delta S = S_{\text{АМФОКП}} - S_{\text{АДОМУС}} \quad (3.26)$$

Значение прироста структурной скрытности, выраженной в процентах σ_Sпри стохастическом применении АМФОКП, получаемых при изменениях фазового сдвига между элементами кодовой последовательности на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$ по сравнению со структурной скрытностью АДОМУС $S_{\text{АДОМУС}}$

$$\sigma_S = \frac{\Delta S}{S_{\text{АДОМУС}}} \cdot 100\%, \quad (3.27)$$

где σ_S – отношение абсолютного значения прироста структурной скрытности ΔS АМФОКП к структурной скрытности АДОМУС $S_{\text{АДОМУС}}$, выраженное в процентах.

Поскольку порядок ЭМ n определяет размерность системы собственных векторов ЭМ, которые описывают АМФОКП длиной L, причем в этом случае $L = n$, то с учетом значений структурных скрытностей АМФОКП и АДОМУС для L=128 и L=256, получим при $\Delta\varphi_i = 18°$

$$\Delta_{S128} = 548{,}88 - 535{,}5 = 13{,}38 \text{ ДИЗ},$$

$$\Delta_{S128} = 1102 - 1077 = 25 \text{ ДИЗ}.$$

При $\Delta\varphi_i = 1°$ получим следующие значения

$$\Delta_{S128} = 1078 - 535{,}5 = 542{,}5 \text{ ДИЗ},$$

$$\Delta_{S128} = 2165 - 1077 = 1088 \text{ ДИЗ}.$$

Рассчитаем отношение абсолютного значения прироста структурной скрытности ΔS АМФОКП к структурной скрытности АДОМУС $S_{\text{АДОМУС}}$. Для L=128 и L=256 при $\Delta\varphi_i = 18°$

$$\sigma_{S128} = \frac{13{,}38}{535{,}5} \cdot 100\% = 2{,}5\ \%,$$

$$\sigma_{S256} = \frac{25}{1077} \cdot 100\% = 2{,}32\ \%.$$

при $\Delta\varphi_i = 1°$ получим следующие значения

$$\sigma_{S128} = \frac{542{,}5}{535{,}5} \cdot 100\% = 101{,}31\ \%,$$

$$\sigma_{S256} = \frac{1088}{1077} \cdot 100\% = 101{,}02\ \%.$$

В таблице 3.10 представлены результаты расчетов значений прироста структурной скрытности АМФОКП к структурной скрытности АДОМУС σ_S, выраженной в процентах для матриц порядков $n =$, 128 и 256 при изменении фазового сдвига между элементами кодовой последовательности на углы $\Delta\varphi_i = 1°$, $\Delta\varphi_i = 18°$.

Таблица 3.10 – Значение прироста структурной скрытности σ_S АМФОКП к структурной скрытности АДОМУС

Порядок матрицы, n	σ_S при $\Delta\varphi_i = 1°$, %	σ_S при $\Delta\varphi_i = 18°$, %
128	101,31	2,5
256	101,02	2,32

Таким образом, в работе предложены аналитические выражения для определения количества комбинаций кодовых последовательностей и значений показателя структурной скрытности АМФОКП, получаемых на основе СВ бидиагональной ЭМ при одновременном изменении фаз всех диагональных коэффициентов ЭМ. Получаемые с помощью предложенного в 3 главе алгоритма АМФОКП имеют прирост структурной скрытности АМФОКП по отношению к

структурной скрытности АДОМУС, который лежит в пределах для $n = 128$ от 2,5 до 101,31%, для $n = 256$ от 2,32 до 101,02%.

Данный выигрыш обеспечивается при условии, что фаза каждого диагонального коэффициента ЭМ и соответственно элементов кодовой последовательности изменяется на угол от $\Delta\varphi_i = 1^{\circ}$ до $\Delta\varphi_i = 18^{\circ}$.

Значение структурной скрытности АМФОКП для $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для L=128 и L=256, что позволяет их использовать в существующих ССС с КРК.

Выявленные преимущества АМФОКП, получаемых на основе СВ бидиагональной ЭМ, по показателю структурной скрытности обосновывают целесообразность их применения, в современных ССС с КРК для повышения их защищенности на основе стохастического применения АМФОКП с изменяющейся структурой, например для 16-QAM, QPSK.

3.5 Выводы по главе

1. Разработанная модель АМФОКП основана на использовании множества наборов собственных векторов ЭМ, которые в каждом конкретном случае вычисляются в соответствии с набором значений модулей и аргументов диагональных коэффициентов ЭМ. Используя различные наборы таких коэффициентов, в соответствии с разработанным алгоритмом синтеза, определяются различные по своей структуре ансамбли ортогональных кодовых последовательностей в количестве, превышающем требуемое значение $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$ для размерностей $N = 128, 256$.

2. Для стохастического применения ортогональных кодовых последовательностей в ССС с КРК предложено использовать ансамбли многофазных ортогональных кодовых последовательностей, представляемые собственными векторами бидиагональных эрмитовых матриц, которые в силу своих свойств являются всегда ортогональными.

3. С учетом того, что множество эрмитовых матриц порядка $(n \times n)$, все элементы которых – целые комплексные числа, задают все возможные ортогональные базисы пространства C^n можно получить требуемое количество ортогональных базисов $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$, что имеет важное значение при получении большого количества ортогональных базисов, которыми могут быть описаны ансамбли ортогональных кодовых последовательностей.

4. Установлены условия для модулей диагональных коэффициентов эрмитовых матриц, при которых обеспечивается получение ансамблей ортогональных собственных векторов ЭМ с равными значениями модулей их координат. Экспериментально установлены значения модулей диагональных коэффициентов ЭМ $N = 128, 256$ при которых модули координат СВ ЭМ имеют равные значения.

5. С помощью формул (3.17) - (3.18) установлено, что имеется соответствие между изменением аргументов диагональных коэффициентов эрмитовых матриц на определенный угол $\Delta\varphi$, и изменением аргументов координат собственных векторов бидиагональных ЭМ на аналогичный угол $\Delta\psi$. Данная зависимость позволяет в процессе синтеза АМФОКП осуществить целенаправленный отбор всех возможных их уникальных структур.

6. Получена формула (3.24) для определения количества вариантов возможных значений фаз, принимаемых всеми диагональными коэффициентами бидиагональной ЭМ n-го порядка и формула (3.25) для определения количества значений показателя структурной скрытности АМФОКП, получаемых на основе СВ бидиагональной ЭМ при одновременном изменении фаз всех диагональных коэффициентов ЭМ.

7. Для расчета количества уникальных АМФОКП, получаемых на основе СВ бидиагональной ЭМ предложено выполнить следующие операции:

– определить диапазон значений фаз коэффициентов бидиагональной ЭМ,

при котором возможно получение уникальных АМФОКП;

– определить значения СВ бидиагональной ЭМ, описываемой выражением (3.5), позволяющие получить ансамбль из N сигналов для каждого дискретного минимального значения фазы с шагом $\Delta\varphi_{k,l} = 1°$ у диагональных коэффициентов $A_{l,k}$ бидиагональной ЭМ на тригонометрической окружности $360°$.

8. Рассмотрены примеры синтеза АМФОКП для размерностей ансамблей сигналов $N = 4$ на основе рассмотрения собственных векторов бидиагональных эрмитовых матриц при изменяющихся значениях аргументов её коэффициентов второй диагонали, которые подтверждают аналитические зависимости между модулями и аргументами диагональных коэффициентов ЭМ и модулями и аргументами координат их СВ.

9. Результаты проведенных экспериментов позволили разработать алгоритм синтеза АМФОКП. Разработан алгоритм синтеза АМФОКП, включающий в себя семь этапов, который позволяет получить требуемое для стохастического применения в ССС с КРК количество ансамблей $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$.

10. С помощью программы проведены экспериментальные исследования по синтезу ансамблей двоичных ортогональных кодовых последовательностей размерности $N = 128$, представленные на рисунке 3.5, размерности $N = 256$ представленные на рисунке 3.6, которые свидетельствуют о применимости разработанного алгоритма синтеза увеличенного количества АМФОКП, удовлетворяющему показателю $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$.

11. С помощью разработанного алгоритма получены АМФОКП, которые имеют прирост структурной скрытности АМФОКП по сравнению со структурной скрытностью АДОМУС, который лежит в пределах для $n = 128$ от 2,5 до 101,31%, для $n = 256$ от 2,32 до 101,02%. Данный выигрыш обеспечивается при условии, что фазовый сдвиг между элементами кодовой последовательности изменяется на угол от $\Delta\varphi_i = 1^{\circ}$ до $\Delta\varphi_i = 18^{\circ}$. Значение структурной скрытности АМФОКП для фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для L=128 и L=256, что позволяет их использовать в существующих ССС с КРК.

12. Выявленные преимущества АМФОКП, получаемых на основе СВ бидиагональной ЭМ, по показателю структурной скрытности и возможность их практической реализации обосновывают целесообразность их применения в современных ССС с КРК для повышения их защищенности на основе стохастического применения АМФОКП с изменяющейся структурой, например для 16-QAM, QPSK.

13. Для обоснования возможности стохастического применения ортогональных кодовых последовательностей в ССС с КРК необходимо разработать принцип построения и техническое решение стохастического средства защиты информации для рассматриваемых систем.

4. РАЗРАБОТКА ПРИНЦИПА ПОСТРОЕНИЯ И ТЕХНИЧЕСКОГО РЕШЕНИЯ СТОХАСТИЧЕСКОГО СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ СИСТЕМ СПУТНИКОВОЙ СВЯЗИ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

4.1 Разработка принципа, структуры и алгоритма функционирования генератора ансамблей многофазных ортогональных кодовых последовательностей для стохастического средства защиты информации

Во второй главе диссертационной работы разработана модель системы спутниковой связи с кодовым разделением каналов на основе стохастического применения АМФОКП, представленная на рисунке 2.6, в состав которой входит стохастическое средство защиты информации.

Отметим, что в соответствии с п. 2.7.2 ГОСТ Р 50922-2006 [120] дано следующее определение средства защиты информации. «Средство защиты информации: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации)».

Как было установлено выше, повышение скрытности ССС с КРК, лежит на основе увеличения количества последовательностей, структурной скрытности АМФОКП и процедуре их стохастического применения. Как следует из работ Л.М. Финка, С.А. Мухаметшина, С.А. Осмоловского, Кандаурова Н.А. и изображено на рисунке 2.3 стохастическое средство защиты информации содержит кодирующее устройство на передаче, стохастический преобразователь и датчик псевдослучайных последовательностей, который формирует множество кодовых комбинаций и

определяет их стохастическое применение. На приемной стороне содержатся стохастическое средство защиты информации, состоящее из датчика ПСП приема, которое работает синхронно с датчиком ПСП передатчика стохастического преобразователя, реализующего функцию обратного преобразования по сравнению со стохастическим преобразователем передатчика и декодер.

Применительно к ССС с КРК будем использовать принцип, заложенный в основе построения системы передачи информации с применением стохастических ортогональных кодов, на которую автором в соавторстве имеются патенты [110] Система передачи информации с применением стохастических ортогональных кодов, [114] Система непрерывной передачи информации ансамблями стохастических ортогональных кодов.

Суть данного принципа заключается в получении АМФОКП из последовательности псевдослучайных комплексных чисел. В предлагаемом принципе функции стохастического преобразования выполняет ГПСКЧ, задачей которого является задание начальных исходных данных для функционирования генератора псевдослучайных АМФОКП. Поскольку ГПСКЧ на передающей и приемной сторонах должны функционировать одинаково, то в качестве ключа в них вводится идентичное начальное заполнение псевдослучайной последовательностью чисел и в дальнейшем поддерживается синхронная работа устройством синхронизации. При этих условиях обеспечивается формирование одинаковых последовательностей ПСКЧ в передающей и приемной сторонах участников информационного обмена.

На основе сформированных ПСКЧ на выходах ГПСКЧ передатчика и приемника осуществляется стохастическое формирование АМФОКП для их последующей подачи в генератор псевдослучайных АМФОКП. Сформированные таким образом АМФОКП на основе ПСКЧ записываются в буферный накопитель.

В случае необходимости стохастического применения АМФОКП для передачи информации он считывается из буферного накопителя по принципу «первый пришел, первый вышел» и выдается в ССС с КРК.

Стохастическое средство защиты информации включает генератор ПСКЧ, генератор псевдослучайных АМФОКП, устройство синхронизации и буферный накопитель, которые имеют техническую возможность формировать множество кодовых последовательностей и осуществлять их стохастическое применение.

Опишем порядок функционирования стохастического средства защиты информации. На начальном этапе задается размерность формируемого АМФОКП N. Значение последовательности псевдослучайных чисел $\{Z_i\}$ на выходе генератора псевдослучайных чисел формируется на основе функции преобразования k последних членов последовательности псевдослучайных чисел $Z_{\mathrm{m-k+1}}$, $Z_{\mathrm{m-k+2}}$,…, Z_{m} в очередное значение $Z_{\mathrm{m+1}}$ последовательности псевдослучайных чисел $\{N_i\}$

$$Z_{m+1} = f(Z_{m-k} + 1, Z_{m-k} + 2, \dots, Z_m).$$

С учетом сформированной последовательности ПСКЧ $\{Z_i\}$ формируется верхняя треугольная часть эрмитовой матрицы A [103]

$$A = [a_m], m \in [1, k], k = N - 1.$$

На основании верхней треугольной части эрмитовой матрицы формируется квадратная эрмитова матрица, причем в нижней треугольной её части располагаются комплексно-сопряженные коэффициенты верхней треугольной части эрмитовой матрицы A'

$$A' = \left[a^*{}_{ji} = a_{ij}\right], i \in [1, k], j \in [1, k].$$

Вычисляются собственные числа матрицы A' как корни характеристического уравнения

$$det(A' - \lambda E) = 0,$$

где E – единичная матрица.

Определяется j-й собственный вектор квадратной матрицы A', удовлетворяющий условию $A \cdot x^{(j)} = \lambda_j \cdot x^{(j)}$

$$x^{(j)} = \begin{pmatrix} x_1^{(j)} \\ . \\ . \\ . \\ x_N^{(j)} \end{pmatrix}, j = (1,2,\dots,N).$$

Вычисляется ансамбль многофазных ортогональных кодовых последовательностей $S_i(t)$, определяемый совокупностью собственных векторов $x_i^{(j)}$ квадратной матрицы A', полученной на основе последовательности псевдослучайных комплексных чисел $\{Z_i\}$

$$x_i^{(j)} = \left(\begin{pmatrix} x_1^{(1)} \\ . \\ . \\ . \\ x_N^{(1)} \end{pmatrix}, \begin{pmatrix} x_1^{(2)} \\ . \\ . \\ . \\ x_N^{(2)} \end{pmatrix}, \dots, \begin{pmatrix} x_1^{(j)} \\ . \\ . \\ . \\ x_N^{(j)} \end{pmatrix} \right) \Rightarrow \begin{pmatrix} S_1(t), \\ S_2(t), \\ . \\ . \\ . \\ S_N(t) \end{pmatrix}.$$

Схематично данный принцип иллюстрируется на рисунке 4.1.

На рисунке 4.1 используются следующие обозначения. УС – устройство сопряжения, ГПСКЧ – генератор псевдослучайных комплексных чисел, ГП АМФОКП – генератор псевдослучайных ансамблей многофазных ортогональных кодовых последовательностей, БН – буферный накопитель.

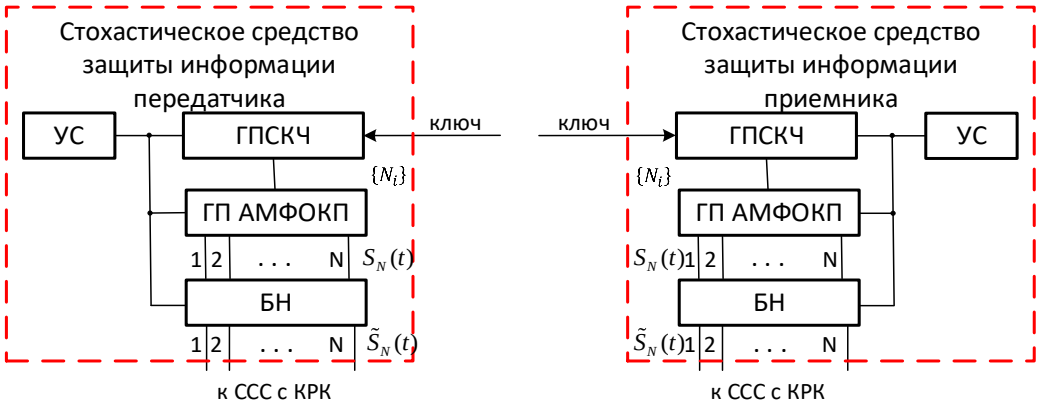


Рисунок 4.1 – Иллюстрация принципа построения стохастического средства защиты информации для ССС с КРК

На основе изложенного принципа разработаем техническое решение, позволяющее реализовать стохастическое средство защиты информации.

Анализ источников [110, 111, 112] показывает, что генераторы псевдослучайных комплексных чисел и накопители достаточно изучены и описаны технические решения, позволяющие их использовать при построении стохастического средства защиты информации для ССС с КРК. Поиск технических решений в области построения генераторов псевдослучайных АМФОКП показал, что известны следующие устройства и способы их формирования [103, 105, 107, 110-115, 119-130]. Однако общим недостатком данных генераторов является то, что они рассчитаны на генерацию двоичных ортогональных кодовых последовательностей и не позволяют формировать АМФОКП. Поэтому для решения третьей частной научной задачи и построения недостающего элемента стохастического средства защиты информации ССС с КРК необходимо разработать структуру и алгоритм функционирования генератора псевдослучайных ансамблей многофазных ортогональных кодовых последовательностей [103].

Анализ известных подходов к псевдослучайному формированию ансамблей ортогональных последовательностей [103, 105] показывает, что наибольшие возможности по формированию ортогональных функций имеются у генератора функций Попенко – Турко (ГФПТ) [11]. По этой причине он выбран за основу для построения генератора псевдослучайных ортогональных последовательностей.

Автором на основе ГФПТ были запатентованы два технических решения [111, 115], которые имеют расширенные возможности по стохастическому формированию ортогональных кодовых последовательностей.

Работа ГФПТ основана на вычислении ортогонального базиса положительно определенной симметрической матрицы с действительными положительными коэффициентами, принадлежащими интервалу (0;1). В предлагаемом генераторе осуществлена замена рассмотрения симметрической матрицы на ЭМ, с комплексными коэффициентами, которые могут иметь значения в диапазоне модулей в интервале (0;1) и диапазоне аргументов в интервале (от 0 до 360 градусов).

$$A = \begin{pmatrix} d_{1,1} & A_{1,2} \cdot e^{i \cdot \varphi_{1,2}} & 0 & 0 \\ A_{2,1} \cdot e^{-i \cdot \varphi_{2,1}} & d_{2,2} & A_{2,3} \cdot e^{i \cdot \varphi_{2,3}} & 0 \\ 0 & A_{3,2} \cdot e^{-i \cdot \varphi_{3,2}} & d_{3,3} & A_{3,4} \cdot e^{i \cdot \varphi_{3,4}} \\ 0 & 0 & A_{4,3} \cdot e^{-i \cdot \varphi_{4,3}} & d_{4,4} \end{pmatrix}. \quad (4.1)$$

где $A_{k,l} = A_{l,k}$ – модули диагональных коэффициентов ЭМ [140], $-\varphi_{l,k}$ и $\varphi_{k,l}$ – комплексно-сопряженные аргументы диагональных коэффициентов ЭМ [140].

Для обеспечения возможности применения ЭМ A должна удовлетворять условию комплексной сопряженности диагональных коэффициентов.

СВ ЭМ вида (3.10) являются векторными функциями, которые соответствуют каждому из собственных чисел и определяются в соответствии с формулами (3.11)-(3.15), представленными в третьем разделе данной работы. Таким образом АМФОКП представляется системой СВ ЭМ, которые возможно сгенерировать на основе исходных значений модулей и аргументов эрмитовых матриц [99, 103, 105, 107-109, 111, 115, 140].

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

Для устранения указанных недостатков ГФПТ автором в работах [103, 112, 114, 115] предложена структура генератора псевдослучайных АМФОКП, представленная на рисунке 4.2 и описана его работа.

Рисунок 4.2 – Структура генератора псевдослучайных АМФОКП

Исходная структура ГФПТ дополнена блоком псевдослучайного формирования комплексно-сопряженных коэффициентов ЭМ, состоящим из микроконтроллера, ГПСКЧ, блока накопителя БН, блока N – разрядного (N – разрядность генерируемых ГПСКЧ псевдослучайных комплексно-сопряженных коэффициентов ЭМ) оперативного запоминающего устройства (ОЗУ). Кроме того, в ГФПТ исключена обратная 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 СВ матрицы вида (4.1) для исключения цикличности вывода ортогонального базиса.

За счет добавления вышеперечисленных элементов и исключения связей в ГФПТ появляется возможность автоматизировать процесс присвоения псевдослучайных комплексных исходных данных диагональным комплексно-сопряженным коэффициентам ЭМ и тем самым обеспечить формирование различных по форме АМФОКП на выходе генератора псевдослучайных АМФОКП.

Алгоритм формирования АМФОКП представлен на рисунке 4.3 и состоит из одиннадцати этапов [103].

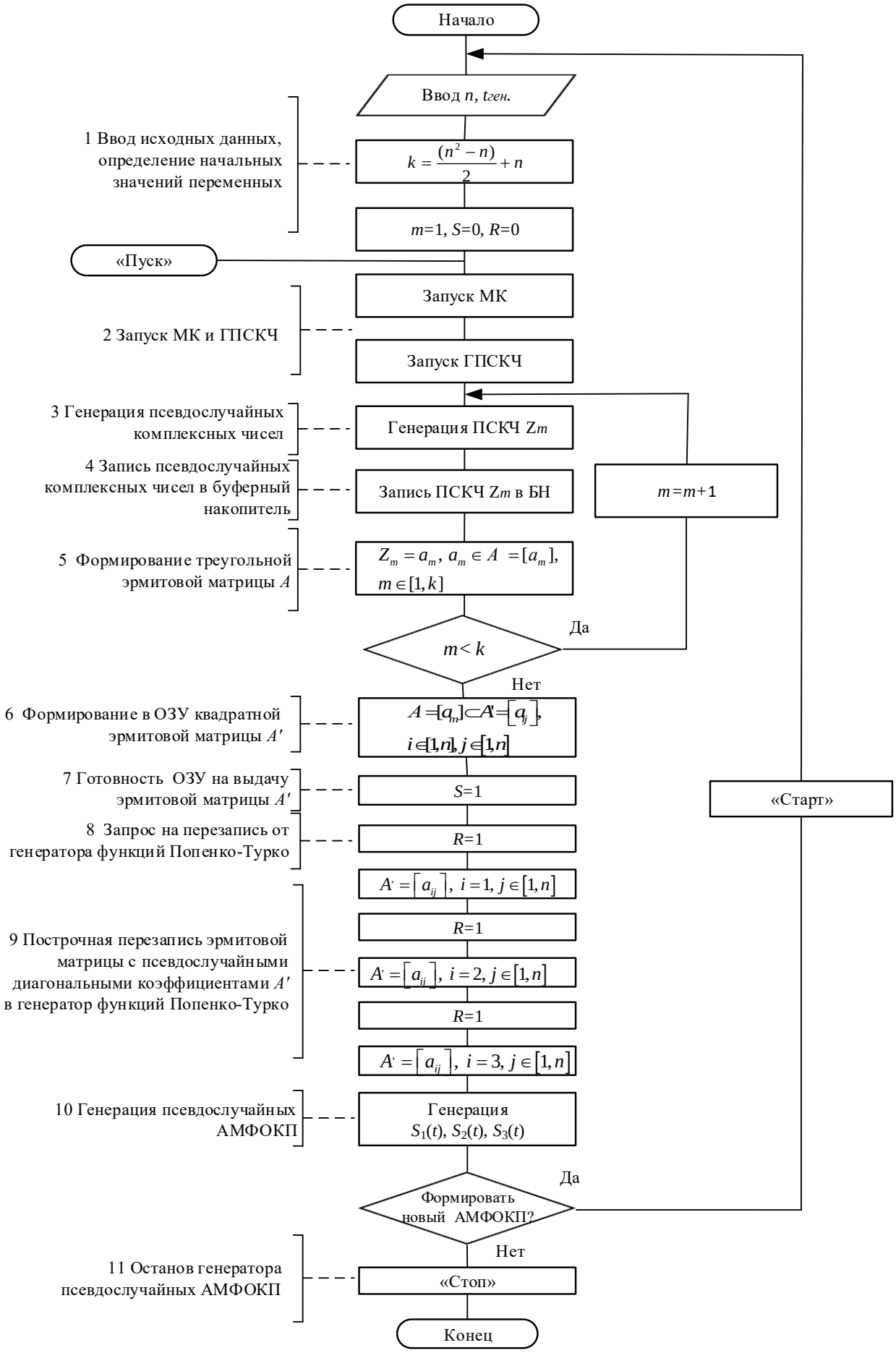


Рисунок 4.3 – Алгоритм формирования АМФОКП

Рассмотрим основное содержание этапов предлагаемого алгоритма.

На первом этапе осуществляется ввод исходных данных, определение начальных значений комплексных переменных, как указано на рисунке 4.3 в комментарии 1. В качестве исходных данных выступают порядок ЭМ n и время, необходимое ГПСКЧ на генерацию ПСКЧ $t_{\text{ген}}$. На основании введенных исходных данных производится расчет и присвоение начальных значений переменных $k, m = 1, S = 0, R = 0$.

С учетом необходимости обеспечения условия комплексной сопряженности диагональных коэффициентов ЭМ в качестве исходных данных необходимо ввести лишь элементы верхней ее треугольной части. Предполагается, что операция присвоения комплексно-сопряженных значений нижней треугольной части ЭМ осуществляется автоматически в блоке накопителя БН.

Формула расчета количества элементов k треугольной матрицы порядка n для получения квадратной матрицы вида (4.1) порядка n выглядит следующим образом [11]:

$$k = \frac{(n^2 - n)}{2} + n. \qquad (4.2)$$

Второй этап алгоритма начинается с поступления команды «Пуск» на начало работы генератора, как указано на рисунке 4.3 в комментарии 2. По данной команде запускается в работу микроконтроллер (МК), который запускает в работу ГПСКЧ.

На третьем этапе ГПСКЧ формируется первое ПСКЧ Z_1 из последовательности k ПСКЧ с определенным временным интервалом $t_{\text{ген.}}$, как указано на рисунке 4.3 в комментарии 3.

На четвертом этапе осуществляется запись сформированного ПСКЧ в БН, как указано на рисунке 4.3 в комментарии 4.

Пятый этап алгоритма характеризуется началом формирования треугольной ЭМ A первым ПСКЧ, как указано на рисунке 4.3 в комментарии 5. В результате

выполнения k итераций и повторных операций, предусмотренных третьим, четвертым и пятым этапами алгоритма, формируется серия из k ПСКЧ $Z_{m-k+1}, Z_{m-k+2}, \dots, Z_m$, для формирования верхней части треугольной ЭМ A в БН, на основе которой с учетом комплексной сопряженности диагональных коэффициентов эрмитовой матрицы достраивается её нижняя треугольная часть.

На шестом этапе осуществляется поступление в ОЗУ квадратной ЭМ A' с комплексно-сопряженными диагональными коэффициентами из БН, как указано на рисунке 4.3 в комментарии 6.

На седьмом этапе после завершения формирования квадратной ЭМ A', из ОЗУ поступает команда готовности в виде сигнала $S = 1$, выдаваемого по линии «S, R», который свидетельствует о возможности выдачи заполненной ПСКЧ ЭМ A' в качестве исходных данных для ГФПТ, как указано на рисунке 4.3 в комментарии 7.

На восьмом этапе в ответ на команду готовности из ОЗУ ($S = 1$) ГФПТ делает запрос в ОЗУ на перезапись от ГПФТ путем формирования сигнала $R = 1$, выдаваемого по линии «S, R», как указано на рисунке 4.3 в комментарии 8.

На девятом этапе реализуется построчная перезапись эрмитовой матрицы с псевдослучайными диагональными коэффициентами A' в генератор функций Попенко-Турко, как показано на рисунке 4.3 в комментарии 9 [103].

На десятом этапе осуществляется генерация АМФОКП, состоящего из набора последовательностей $S_1(t), S_2(t), \dots, S_n(t)$. В алгоритме показан случай формирования сигналов для $n = 3$, как указано на рисунке 4.3 в комментарии 10.

АМФОКП описывается совокупностью СВ ЭМ порядка n вида (4.1), имеющими вид (4.2), являющимися комплексными и удовлетворяющими условию ортогональности [84, 85, 100].

$$\sum_{i=1}^{n} x_i^{(j)} x_i^{(k)} = 0, j \neq k\,. \qquad (4.4)$$

Таким образом, квадратная ЭМ A' порядка n имеет n СВ, т.е. их число равно порядку матрицы A'.

На одиннадцатом этапе осуществляется следующий цикл работы генератора псевдослучайных АМФОКП по команде «Старт», поступающей от ГФПТ, начиная с этапа ввода исходных данных и определения начальных значений переменных, и заканчивая этапом генерации АМФОКП $S_1(t), S_2(t), S_3(t), \dots, S_n(t)$, сгенерированных из нового набора ПСКЧ, как указано на рисунке 4.3 в комментарии 11.

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

Таким образом, данный алгоритм позволяет из наборов последовательностей ПСКЧ, формируемых ГПСКЧ, получить наборы различных АМФОКП. Генерируемые наборы АМФОКП будут отличаться друг от друга по форме, а в случае их стохастического применения в качестве расширяющих последовательностей в беспроводных системах ССС с КРК с учетом их представительного количества могут в течение длительного времени не повторяться.

Для примера рассмотрим реализацию алгоритма формирования ансамблем, состоящим из трех псевдослучайных ортогональных многофазных кодовых последовательностей.

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

По команде «Пуск» запускается МК, который далее запускает ГПСКЧ.

Для заполнения ЭМ A ПСКЧ от ГПСКЧ достаточно будет сформировать три ПСКЧ $Z_1 - Z_3$. ГПСКЧ формирует ПСКЧ Z_1 и со своего первого выхода передает его на третий вход БН для временного хранения. По прошествии определенного времени, равному $t_{\text{ген}}$, необходимого ГПСКЧ на выработку ПСКЧ Z_1, МК с первого выхода подает на первый вход ГПСКЧ команду на генерацию следующего ПСКЧ

Z_2. Величина $t_{\text{ген}}$ выбирается согласно соответствующей характеристике аппаратной реализации АМФОКП и записывается предварительно в память МК. МК одновременно с третьего выхода подает команду на первый вход БН на запоминание им выработанного ГПСКЧ Z_2и с первого выхода подает на первый вход ГПСКЧ команду на генерацию следующего псевдослучайного числа Z_3.

МК одновременно с третьего выхода подает команду на первый вход БН на запоминание им выработанного ГПСКЧ Z_3. Данный процесс продолжается до окончания ввода первых шести чисел $Z_1 - Z_6$ верхней треугольной части ЭМ.

Далее в БН в качестве второй нижней треугольной части ЭМ на основании введенных коэффициентов $Z_1 - Z_6$ формируются комплексно-сопряженные диагональные коэффициенты $Z_7 - Z_9$ ЭМ [103].

Сформированная эрмитова матрица из БН поступает в блок N – разрядного ОЗУ, где ЭМ преобразуется в массив данных, в виде девяти псевдослучайных комплексно-сопряженных чисел относительно главной диагонали ЭМ A'.

Окончание процесса формирования массива данных, состоящих из ПСКЧ, 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 АМФОКП 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 $t_{\text{зап.}}$ поступают в ГФПТ и присваиваются в качестве исходных данных коэффициентам первой строки ЭМ. 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 $t_{\text{зап.}}$ поступают в ГФПТ и присваиваются в качестве исходных данных коэффициентам второй строки ЭМ. 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 $t_{\text{зап.}}$ поступают в ГФПТ и присваиваются в качестве исходных данных коэффициентам третьей строки ЭМ. После этого считается, что массив исходных данных в виде псевдослучайных комплексно-сопряженных диагональных коэффициентов ЭМ для работы ГФПТ задан. На основании заданного набора псевдослучайных комплексно-сопряженных диагональных коэффициентов ЭМ ГФПТ в течение некоторого времени $t_{\text{выч.}}$ производит вычисление СВ этой матрицы, которые представляют собой следующий АМФОКП $S_1(t), S_2(t), S_3(t)$ на его выходах

$$x_3^{(3)} = \left(\begin{pmatrix} x_1^{(1)} \\ x_2^{(1)} \\ x_3^{(1)} \end{pmatrix}, \begin{pmatrix} x_1^{(2)} \\ x_2^{(2)} \\ x_3^{(2)} \end{pmatrix}, \begin{pmatrix} x_1^{(3)} \\ x_2^{(3)} \\ x_3^{(3)} \end{pmatrix} \right) \Rightarrow \begin{pmatrix} S_1(t) \\ S_2(t) \\ S_3(t) \end{pmatrix}. \tag{4.3}$$

В последующем с помощью тактового генератора в тактовые моменты времени $t_{\text{так.}}$ АМФОКП $S_1(t), S_2(t), S_3(t)$ по параллельным выходам выдается на выходы ГФПТ.

После формирования АМФОКП $S_1(t), S_2(t), S_3(t)$ на основании первого массива псевдослучайных данных ГФПТ выдает команду «Старт» на первый вход МК. На основании этой команды МК формирует команду на первый вход ГПСКЧ на генерацию следующего набора ПСКЧ $Z_1 - Z_6$. Эта процедура выполняется согласно описанного выше алгоритма. На основании сформированного набора ПСКЧ $Z_1 - Z_6$ с помощью ГФПТ будет сформирован новый АМФКОП вида (4.3). С учетом того, что последующие наборы $Z_1 - Z_6$ каждый раз будут отличны от предшествующих, псевдослучайный АМФОКП $S_1(t), S_2(t), S_3(t)$, которые получены на их основе, тоже будут отличаться друг от друга. За счет этого будет

обеспечиваться уникальность формируемых АМФКОП на выходах предлагаемого генератора.

Остановка процесса формирования АМФКОП на выходах генератора осуществляется командой «Стоп», поступающей в необходимый момент времени на вход Вх. 2 МК, который блокирует работу ГПСКЧ, БН, блока N – разрядного ОЗУ и ГФПТ. Описанный выше процесс иллюстрируется на рисунке 4.4.

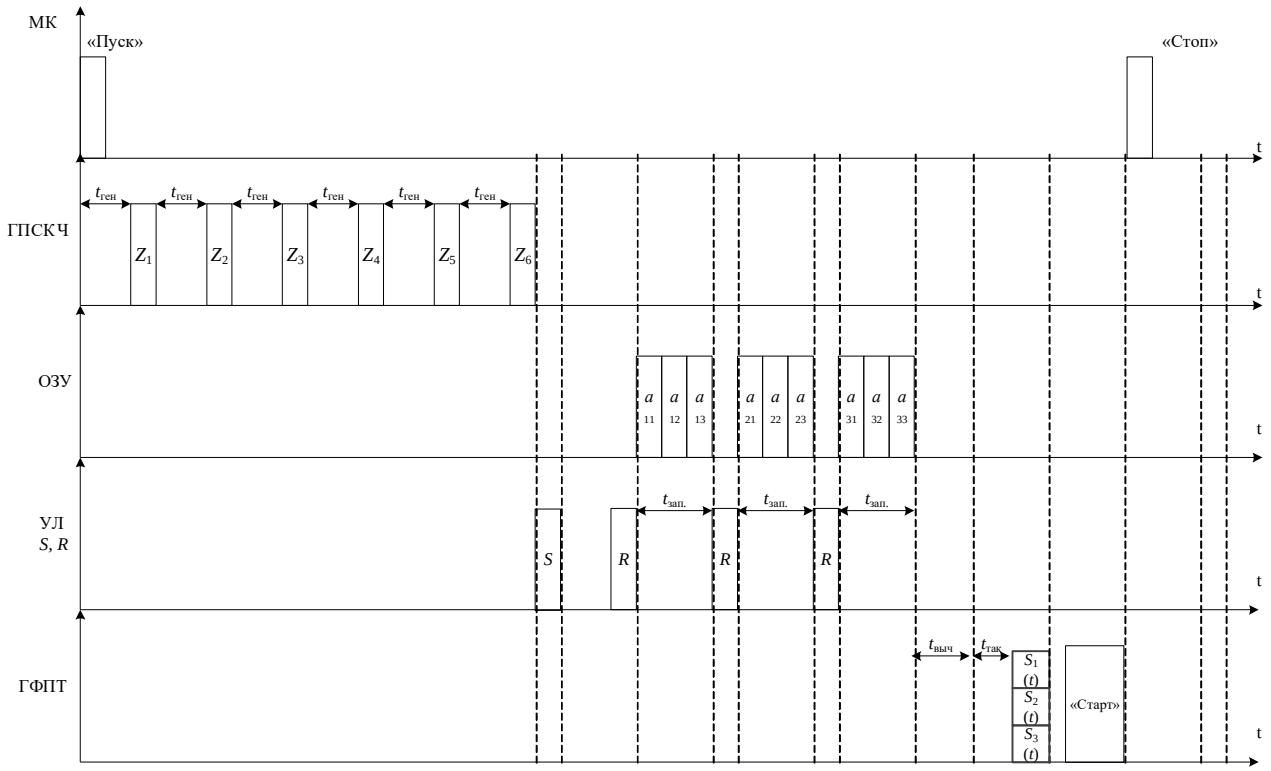


Рисунок 4.4 – Временные диаграммы работы генератора псевдослучайных АМФОКП

На рисунке 4.4 показаны следующие временные диаграммы (сверху вниз):

- запуска и остановки МК;

- работы ГПСКЧ по формированию ПСКЧ $Z_1 - Z_6$;

- построчной выдачи псевдослучайных комплексно-сопряженных диагональных коэффициентов ЭМ;

- работы управляющей линии «S, R» при окончании формирования набора ПСКЧ $Z_1 - Z_6$ и поступлении запроса на их перезапись в ГФПТ;

- работы ГФПТ при псевдослучайном формировании АМФОКП $S_1(t), S_2(t), S_3(t)$ и останове генератора.

Для примера рассмотрим генерацию ортогональных последовательностей рассматриваемым генератором псевдослучайных АМФОКП. Предположим, что с помощью ГПСКЧ данного генератора была сформирована ЭМ А третьего порядка $(n = 3)$.

$$A = \begin{bmatrix} 0 & 1-1i & 0 \\ 1+1i & 0 & 3i \\ 0 & -3i & 0 \end{bmatrix}. \tag{4.4}$$

В результате выполнения описанных выше процедур в генераторе псевдослучайных АМФОКП на его выходе будет сформирована система дискретных базисных функций $S_1(t), S_2(t), S_3(t)$, представляющих собой АМФОКП в алгебраической форме следующего вида:

$$\begin{pmatrix} S_1(t) = (-0{,}213 + 0{,}213i;\ -0{,}707i;\ -0{,}639) \\ S_2(t) = (-0{,}639 + 0{,}639i;\ 0;\ 0{,}426) \\ S_3(t) = (0{,}213 - 0{,}213i;\ -0{,}707i;\ 0{,}639) \end{pmatrix}. \tag{4.5}$$

Выражение (4.5) для наглядности представим в показательной форме:

$$\begin{pmatrix} S_1(t) = 0{,}301 \cdot e^{i\cdot 135^\circ}; 0{,}707 \cdot e^{-i\cdot 90^\circ}; 0{,}639 \cdot e^{i\cdot 180^\circ} \\ S_2(t) = 0{,}904 \cdot e^{i\cdot 135^\circ};\ 0;\ 0{,}426 \cdot e^{i\cdot 0^\circ} \\ S_3(t) = 0{,}301 \cdot e^{i\cdot 315^\circ};\ 0{,}707 \cdot e^{i\cdot 270^\circ};\ 0{,}639 \cdot e^{i\cdot 0^\circ} \end{pmatrix}. \tag{4.6}$$

На рисунке 4.5 представлена временная диаграмма АМФОКП вида (4.6), формируемая на выходе рассматриваемого генератора псевдослучайных АМФОКП, на основе диагональной ЭМ вида (4.4) [103].

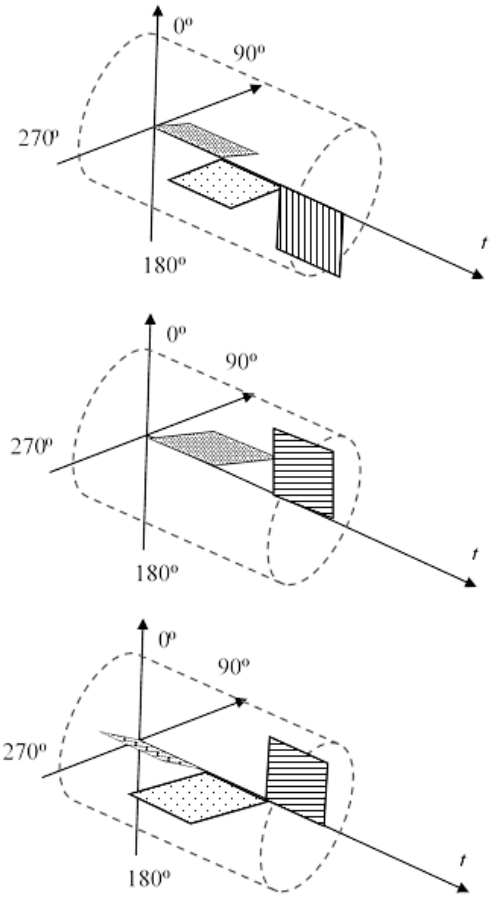


Рисунок 4.5 – Временная диаграмма АМФОКП

Разработанный генератор псевдослучайных АМФОКП может иметь широкую область применения, заключающуюся в генерировании псевдослучайных АМФОКП, число которых может быть отлично от 2^m, где m – натуральное число, имеющих широкий набор значений периодов генерируемых функций и большое число значений ортогональных базисных функций за счет автоматизации процесса присвоения псевдослучайных значений диагональным коэффициентам ЭМ A вида (4.1).

Нелинейность формируемых структур ортогональных последовательностей достигается за счет того, что на каждом такте его работы АМФОКП, представляемый СВ ЭМ, формируется путем псевдослучайного задания набора ее диагональных комплексно-сопряженных коэффициентов с помощью ГПСКЧ [113].

Таким образом:

1. Стохастическое средство защиты информации ССС с КРК включает в себя генератор псевдослучайных комплексных чисел, генератор псевдослучайных

АМФОКП и блок накопителя. С учетом того, что широко известны различные виды ГПСКЧ и накопителей, но не проработаны вопросы построения генераторов псевдослучайных АМФОКП, для решения третьей частной задачи и построения недостающего элемента стохастического средства защиты информации ССС с КРК обоснована необходимость разработки структуры и алгоритма функционирования генератора псевдослучайных ансамблей многофазных ортогональных кодовых последовательностей.

2. В качестве прототипа для построения генератора псевдослучайных АМФОКП выбран ГФПТ в силу наличия у него достоинств и универсальности. Структура прототипа дополнена блоком псевдослучайного формирования комплексно-сопряженных коэффициентов ЭМ, состоящим из МК, ГПСКЧ, БН, блока N – разрядного ОЗУ. Кроме того, в ГФПТ исключена обратная 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 СВ ЭМ вида (4.1) для исключения цикличности вывода ортогонального базиса.

3. Алгоритм формирования АМФОКП состоит из одиннадцати этапов, как указано на рисунке 4.3 и позволяет из наборов последовательностей ПСКЧ, формируемых ГПСКЧ, получить наборы различных псевдослучайных АМФОКП.

4. Разработанный генератор псевдослучайных АМФОКП может иметь широкую область применения, заключающуюся в генерировании АМФОКП, число которых может быть отлично от 2^m, где m – натуральное число, имеющих широкий набор значений периодов генерируемых функций и большое число значений ортогональных базисных функций за счет автоматизации процесса присвоения псевдослучайных значений диагональным коэффициентам ЭМ A вида (4.1).

4.2 Разработка программной модели системы спутниковой связи на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей

Для обоснования реализуемости модели системы спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей разработаем программную модель ССС с КРК с повышенной скрытностью в среде моделирования Matlab SIMULINK.

За основу разрабатываемой модели использована модель, представленная в [110, 113, 114].

Модель ССС с КРК на основе стохастического применения АМФОКП состоит из передающей части, как указано на рисунке 4.6, приемной части и канала связи, как указано на рисунке 4.7.

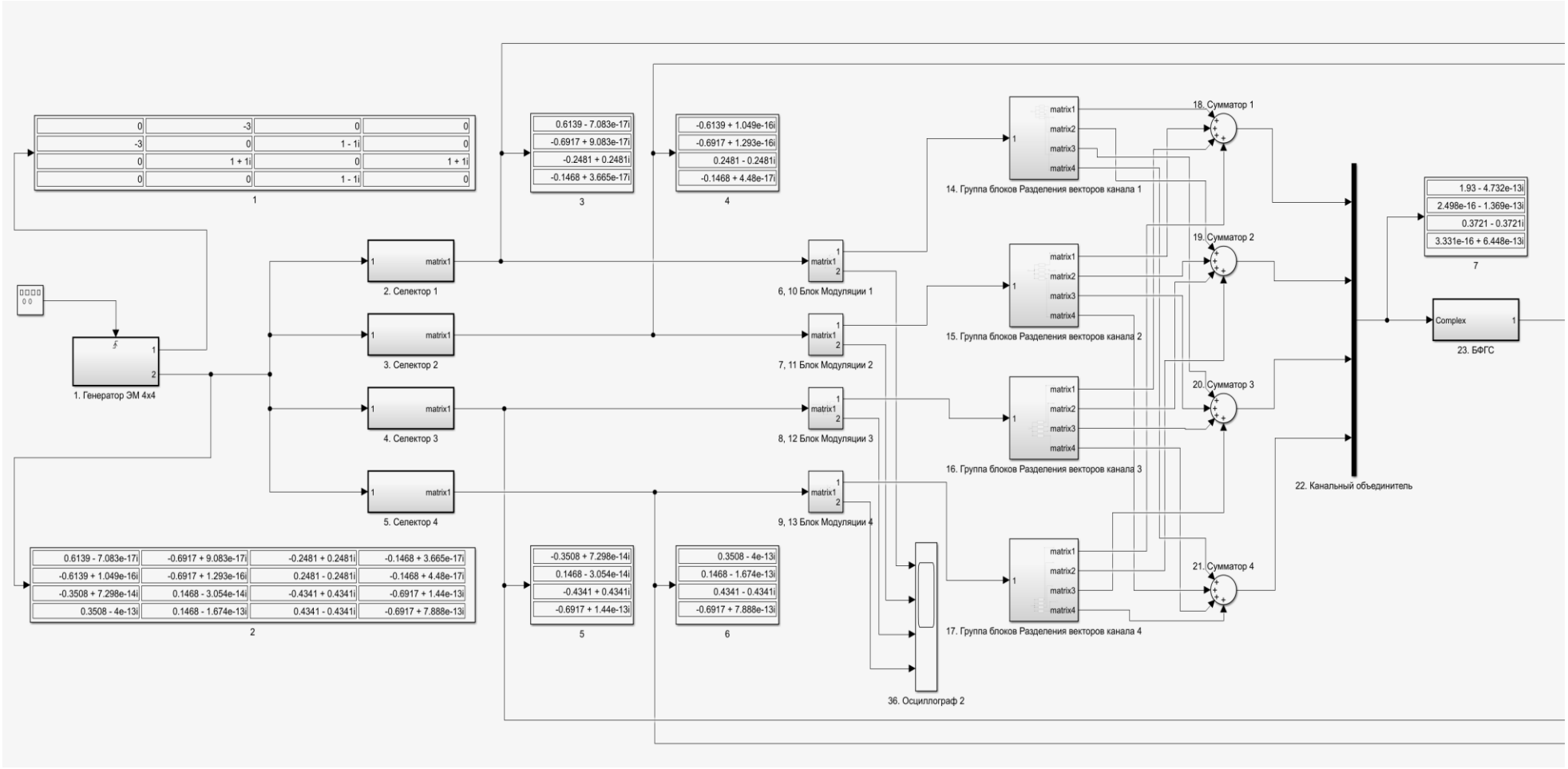


Рисунок 4.6 – Модель передающей части ССС с КРК на основе стохастического применения АМФОКП

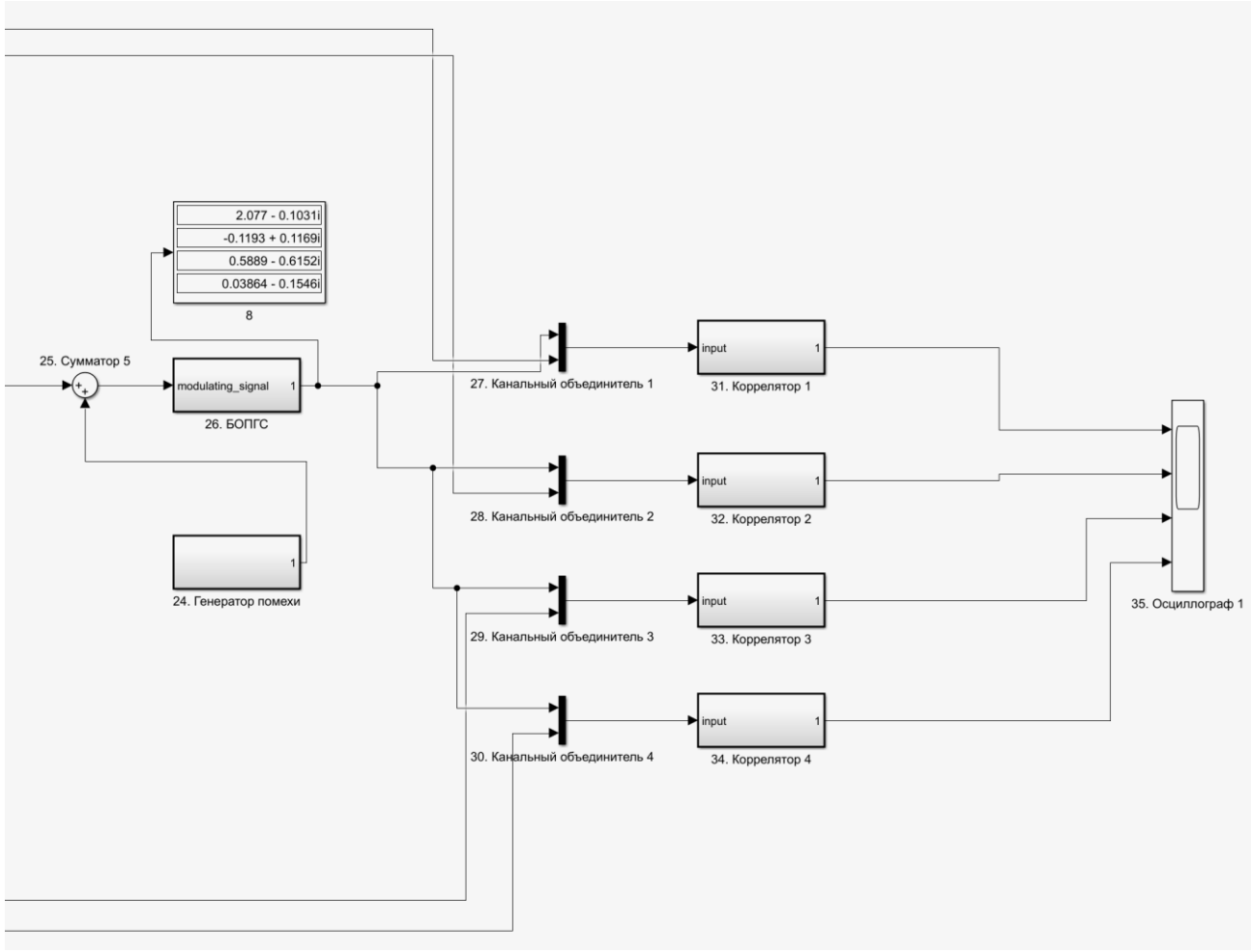


Рисунок 4.7 – Модель приемной части ССС с КРК на основе стохастического применения АМФОКП

Рассмотрим состав, назначение и порядок соединения блоков, входящих в состав рассматриваемой модели.

В состав передающей части модели ССС с КРК на основе стохастического применения АМФОКП входят блоки 1-23. Блоки 24-25 являются имитацией линии связи. Блоки 26-34 являются элементами приемной части ССС с КРК, блоки 35-36 являются элементами визуализации процессов функционирования модели.

Для оценки достоверности работы СПИ с КРК на основе стохастического применения АМФОКП в состав схемы включены счётчики битовых ошибок в каждом информационном канале.

Отметим, что блоки 6 и 10, 7 и 11, 8 и 12, 9 и 13 входят соответственно в состав блоков модуляции 1, 2, 3 и 4 [114].

На дисплеях 1-8 модели ССС с КРК отображаются результаты проводимых преобразований.

1. Блок генератор ЭМ 4×4 предназначен для генерации ЭМ 4×4 и матрицы СВ для этой ЭМ. На выходе 1 блока выводится сама ЭМ, на выходе 2 выводится матрица СВ ЭМ, которые иллюстрируются соответственно на дисплеях 1 и 2.

2. Блок селектор 1 предназначен для разделения матрицы СВ ЭМ на отдельные векторы. При этом блок селектор 1 выделяет первый СВ, находящийся в первой строке матрицы СВ ЭМ, который иллюстрируется на дисплее 3.

3. Блок селектор 2 предназначен для разделения матрицы СВ ЭМ на отдельные векторы. При этом блок селектор 2 выделяет второй СВ, находящийся в второй строке матрицы СВ ЭМ, который иллюстрируется на дисплее 4.

4. Блок селектор 3 предназначен для разделения матрицы СВ ЭМ на отдельные векторы. При этом блок селектор 3 выделяет третий СВ, находящийся в третьей строке матрицы СВ ЭМ, который иллюстрируется на дисплее 5.

5. Блок селектор 4 предназначен для разделения матрицы СВ ЭМ на отдельные векторы. При этом блок селектор 4 выделяет четвертый СВ, находящийся в четвертой строке матрицы СВ ЭМ, который иллюстрируется на дисплее 6.

6. Блок информационный сигнал 1 входит в состав блока модуляции 1 и предназначен для генерации информационного сигнала 1 для его последующей модуляции в блоке модуляции 1.

7. Блок информационный сигнал 2 входит в состав блока модуляции 2 и предназначен для генерации информационного сигнала 2 для его последующей модуляции в блоке модуляции 2.

8. Блок информационный сигнал 3 входит в состав блока модуляции 3 и предназначен для генерации информационного сигнала 3 для его последующей модуляции в блоке модуляции 3.

9. Блок информационный сигнал 4 входит в состав блока модуляции 4 и предназначен для генерации информационного сигнала 4 для его последующей модуляции в блоке модуляции 4.

10. Блок модуляции 1 предназначен для осуществления фазовой модуляции МФОКП, представленной первым СВ ЭМ, при помощи информационного сигнала 1.

11. Блок модуляции 2 предназначен для осуществления фазовой модуляции МФОКП, представленной вторым СВ ЭМ, при помощи информационного сигнала 2.

12. Блок модуляции 3 предназначен для осуществления фазовой модуляции МФОКП, представленной третьим СВ ЭМ, при помощи информационного сигнала 3.

13. Блок модуляции 4 предназначен для осуществления фазовой модуляции МФОКП, представленной четвертым СВ ЭМ, при помощи информационного сигнала 4.

14. Группа блоков разделения векторов 1-4 канала 1 предназначена для разделения модулированного СВ ЭМ на составные части и подачи его на блоки сумматор 1-4.

15. Группа блоков разделения векторов 5-8 канала 2 предназначена для разделения модулированного СВ ЭМ на составные части и подачи его на блоки сумматор 1-4.

16. Группа блоков разделения векторов 9-12 канала 3 предназначена для разделения модулированного СВ ЭМ на составные части и подачи его на блоки сумматор 1-4.

17. Группа блоков разделения векторов 13-16 канала 4 предназначена для разделения модулированного СВ ЭМ на составные части и подачи его на блоки сумматор 1-4.

18. Блок сумматор 1 предназначен для суммирования первых элементов модулированных СВ 1-4, поступающих с выходов блока разделения вектора 1, 5, 9, 13 и передачи их на блок канального объединителя.

19. Блок сумматор 2 предназначен для суммирования первых элементов модулированных СВ 1-4, поступающих с выходов блока разделения вектора 2, 6, 10, 14 и передачи их на блок канального объединителя.

20. Блок сумматор 3 предназначен для суммирования первых элементов модулированных СВ 1-4, поступающих с выходов блока разделения вектора 3, 7, 11, 15 и передачи их на блок канального объединителя.

21. Блок сумматор 4 предназначен для суммирования первых элементов модулированных СВ 1-4, поступающих с выходов блока разделения вектора 4, 8, 12, 16 и передачи их на блок канального объединителя.

22. Блок канальный объединитель предназначен для объединения сигналов, поступающие на его входы 1-4 от блоков сумматор 1-4 и передачи их на блок БФГС, как иллюстрируется на дисплее 7.

23. Блок формирования группового сигнала БФГС предназначен для формирования группового сигнала, поступающего с выхода блока канального объединителя в квадратурную форму и подачи его на вход 1 блока сумматора 5, имитирующего канал связи, как иллюстрируется на дисплее 8. В блоке БФГС осуществляется модуляция сформированным групповым сигналом канальной несущей частоты, в результате чего формируется канальный сигнал (дисплей 8). Поскольку групповой сигнал является комплексным для его формирования используется преобразование в квадратурное представление. [131].

24. Блок генератор помехи предназначен для имитации помехи типа «Белый шум» в канале связи.

25. Блок канальный сумматор 5 предназначен для имитации искажения сигнала в линии, как иллюстрируется на дисплее 9.

26. Блок обратного преобразования группового сигнала (БОПГС) предназначен для приема сигнала из линии связи и преобразования группового сигнала из квадратурной формы в последовательность ПСКЧ (комплексный вид).

27. Блок канальный объединитель 1 предназначен для объединения группового сигнала, поступающего с выхода блока БОПГС с копией первой последовательности из состава АМФОКП. С выхода канального объединителя 1 объединенный сигнал поступает в блок коррелятор 1.

28. Блок канальный объединитель 2 предназначен для объединения группового сигнала, поступающего с выхода блока БОПГС с копией второй последовательности из состава АМФОКП. С выхода канального объединителя 2 объединенный сигнал поступает в блок коррелятор 2.

29. Блок канальный объединитель 3 – предназначен для объединения группового сигнала, поступающего с выхода блока БОПГС с копией третьей последовательности из состава АМФОКП. С выхода канального объединителя 3 объединенный сигнал поступает в блок коррелятор 3.

30. Блок канальный объединитель 4 предназначен для объединения группового сигнала, поступающего с выхода блока БОПГС с копией четвертой последовательности из состава АМФОКП. С выхода канального объединителя 4 объединенный сигнал поступает в блок коррелятор 4.

31. Блок коррелятор 1 предназначен для выделения информационной последовательности, поступающей с выхода канального объединителя 1 на основе сравнения группового сигнала и копии последовательности из состава АМФОКП, соответствующей первому информационному каналу.

32. Блок коррелятор 2 предназначен для выделения информационной последовательности, поступающей с выхода канального объединителя 2 на основе сравнения группового сигнала и копии последовательности из состава АМФОКП, соответствующей второму информационному каналу.

33. Блок коррелятор 3 предназначен для выделения информационной последовательности, поступающей с выхода канального объединителя 3 на основе

сравнения группового сигнала и копии последовательности из состава АМФОКП, соответствующей третьему информационному каналу.

34. Блок коррелятор 4 предназначен для выделения информационной последовательности, поступающей с выхода канального объединителя 4 на основе сравнения группового сигнала и копии последовательности из состава АМФОКП, соответствующей четвертому информационному каналу.

35. Блок осциллограф 1 предназначен для визуализации информационных процессов, происходящих на выходах коррелятора каждого канала.

36. Блок осциллограф 2 предназначен для визуализации информационных процессов при передаче на выходах блоков модуляции 1-4.

Более подробно структура и описание модели ССС с КРК на основе стохастического применения АМФОКП описана в [113].

4.3 Моделирование системы спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей

На основе представленной на рисунке 4.6 и рисунке 4.7 модели ССС с КРК на основе стохастического применения АМФОКП, опишем происходящие в ней в процессы. Данная модель подробна описана в [113].

Передающая часть модели ССС с КРК использует стохастическое применение ортогональных кодовых последовательностей.

1. Блок генератор ЭМ 4×4.

Рассматриваемая модель для наглядности представления происходящих в ней процессов базируется на применении четырех информационных трактов. В силу

того, что для генерации и стохастического применения используются АМФОКП, получаемые на основе бидиагональных ЭМ четвертого порядка, то в блоке генератор ЭМ 4×4 для задания значений ЭМ необходимо три комплексных псевдослучайных числа, используемых в качестве диагональных элементов рассматриваемой ЭМ. По указанной выше причине блок генератор ЭМ 4×4 в качестве исходных данных использует ПСКЧ, поступающие от трех ГПСКЧ, на основе которых формируется бидиагональная ЭМ. Правило построения бидиагональной ЭМ заключается в следующем. На основании ПСКЧ, поступающих от ГПСКЧ формируются коэффициенты второй верхней диагонали ЭМ, а затем, с учетом свойств комплексно-сопряженных чисел, достраивается вторая нижняя диагональ ЭМ с комплексно-сопряженными числами второй верхней диагонали ЭМ.

Вид бидиагональной ЭМ, сформированной при помощи блока Генератора ЭМ 4×4 иллюстрируется на дисплее 1, как указано на рисунке 4.8.

0	-3	0	0
-3	0	1 - 1i	0
0	1 + 1i	0	1 + 1i
0	0	1 - 1i	0

1

Рисунок 4.8 – ЭМ размера 4×4

Вид матрицы СВ ЭМ, сформированной на основе бидиагональной ЭМ, представленной на рисунке 4.8, иллюстрируется на дисплее 2, как указано на рисунке 4.9.

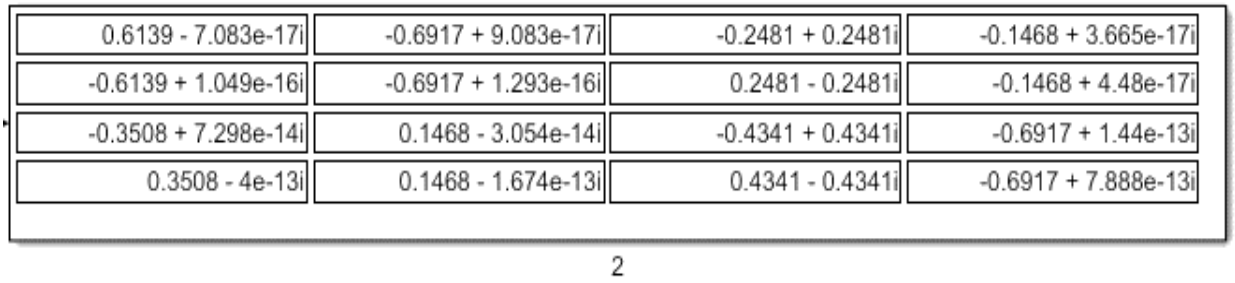


Рисунок 4.9 – Матрица СВ ЭМ, сформированной на основе бидиагональной ЭМ размера 4 × 4

2. Блоки селектор 1-4.

Блок селектор 1 выделяет первый СВ, находящийся в первой строке матрицы СВ ЭМ.

В качестве примера на рисунке 4.10 иллюстрируется дисплей 3, на котором отображается процесс выделения собственного вектора ЭМ из общей матрицы собственных векторов ЭМ, приведенной на рисунке 4.9 с номером, совпадающим с номером селектора. В данном случае иллюстрируется процесс выделения первого собственного вектора ЭМ, выделяемый блоком селектор 1:

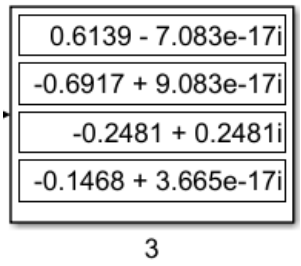


Рисунок 4.10 – Первый собственный вектор ЭМ, выделяемый блоком селектор 1

Аналогичным образом происходит выделение остальных СВ ЭМ из общей матрицы СВ ЭМ с номерами, совпадающими с номерами селекторов. Так блок селектор 2 выделяет второй СВ, находящийся во второй строке матрицы СВ ЭМ, как указано на дисплее 4 рисунка 4.6; блок селектор 3 выделяет третий СВ, находящийся в третьей строке матрицы СВ ЭМ как указано на дисплее 5 рисунка

4.6; блок селектор 4 выделяет четвертый СВ, находящийся в четвертой строке матрицы СВ ЭМ как указано на дисплее 6 рисунка 4.6.

3. Блоки информационный сигнал 1-4 входят в состав блоков модуляции 1-4.

Блок информационный сигнал 1 состоит из следующих элементов: генератор случайных натуральных чисел от 0 до 7, преобразователь в битовую последовательность, буфер и селектор. Блок работает следующим образом. Сначала генерируется десятеричное число от 0 до 7, затем данное число преобразуется в трех битовую последовательность, которая записывается в буфер. В последующем значения последовательности поступают на селектор, который позволяет осуществить побитовое считывание для последующей модуляции в блоке модуляции 1.

Аналогичным образом происходит генерация информационных символов в блоках информационный сигнал 2-4, поступающих в блоки модуляции 2-4.

На рисунке 4.11 представлены осциллограммы информационных последовательностей 1-4 перед подачей их на входы блоков модуляции 1-4.

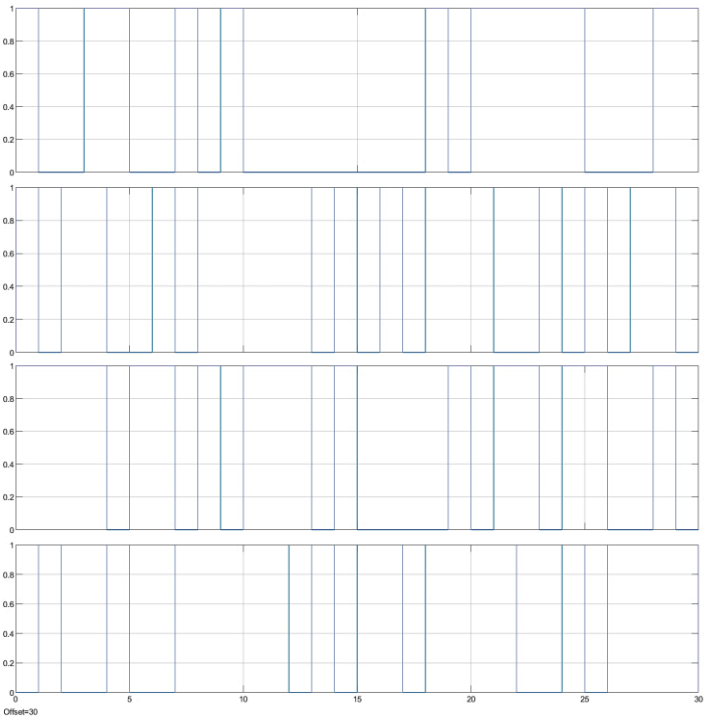


Рисунок 4.11 – Осциллограммы информационных последовательностей 1-4 перед подачей их на входы блоков модуляции 1-4

4. Блоки модуляции 1-4.

Блок модуляции 1 осуществляет фазовую модуляцию собственного ЭМ, представляющего собой МФОКП и выступающую в качестве расширяющей последовательности, при помощи информационного сигнала 1. Если на вход блока модуляции 1 поступает информационный символ «единица», то модулируемая последовательность остается неизменной. Если на вход блока модуляции 1 поступает информационный символ «ноль», то последовательность на выходе инвертируется.

На рисунке 4.12, в качестве примера, иллюстрируется результат фазовой модуляции МФОКП в блоке модуляции 1 информационным символом «единица».

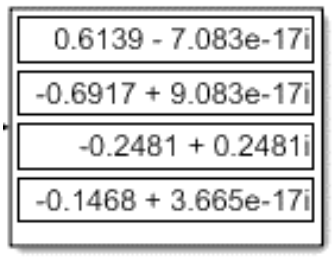


Рисунок 4.12 – Результат фазовой модуляции МФОКП в блоке модуляции 1 информационным символом «единица»

На рисунке 4.13, в качестве примера, иллюстрируется результат модуляции МФОКП в блоке модуляции 1 информационным символом «ноль».

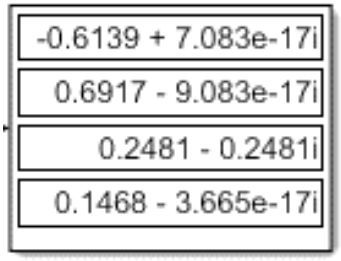


Рисунок 4.13 – Результат фазовой модуляции МФОКП в блоке модуляции 1 информационным символом «ноль»

Аналогичным образом осуществляется фазовая модуляция в блоках модуляции 2-4.

Блок модуляции 2 осуществляет фазовую модуляцию собственного вектора ЭМ, представляющего собой МФОКП, при помощи информационного сигнала 2. Если на вход блока модуляции 2 поступает информационный символ «единица», то сигнал остается неизменным. Если на вход блока модуляции 2 поступает информационный символ «ноль», то сигнал на выходе инвертируется.

Блок модуляции 3 осуществляет фазовую модуляцию собственного вектора ЭМ, представляющего собой МФОКП, при помощи информационного сигнала 3. Если на вход блока модуляции 3 поступает информационный символ «единица», то сигнал остается неизменным. Если на вход блока модуляции 3 поступает информационный символ «ноль», то сигнал на выходе инвертируется.

Блок модуляции 4 осуществляет фазовую модуляцию собственного вектора ЭМ, представляющего собой МФОКП, при помощи информационного сигнала 4. Если на вход блока модуляции 4 поступает информационный символ «единица», то сигнал остается неизменным. Если на вход блока модуляции 4 поступает информационный символ «ноль», то сигнал на выходе инвертируется.

5. Группы блоков разделения векторов 1-16 каналов 1-4.

Группа блоков разделения векторов 1-4 канала 1 разделяет модулированный СВ ЭМ на составные части. На вход каждого блока разделения векторов 1-4 поступает одинаковый сигнал от блока модуляции 1, на выходе блока разделения вектора 1 выходит первый модулированный элемент СВ 1, на выходе блока разделения вектора 2 выходит второй модулированный элемент СВ 1, на выходе блока разделения вектора 3 выходит третий модулированный элемент СВ 1, на выходе блока разделения вектора 4 выходит четвертый модулированный элемент СВ 1.

На рисунке 4.14, в качестве примера, иллюстрируется процесс разделения векторов 1-4 и подачи их на вход блоков сумматор 1-4.

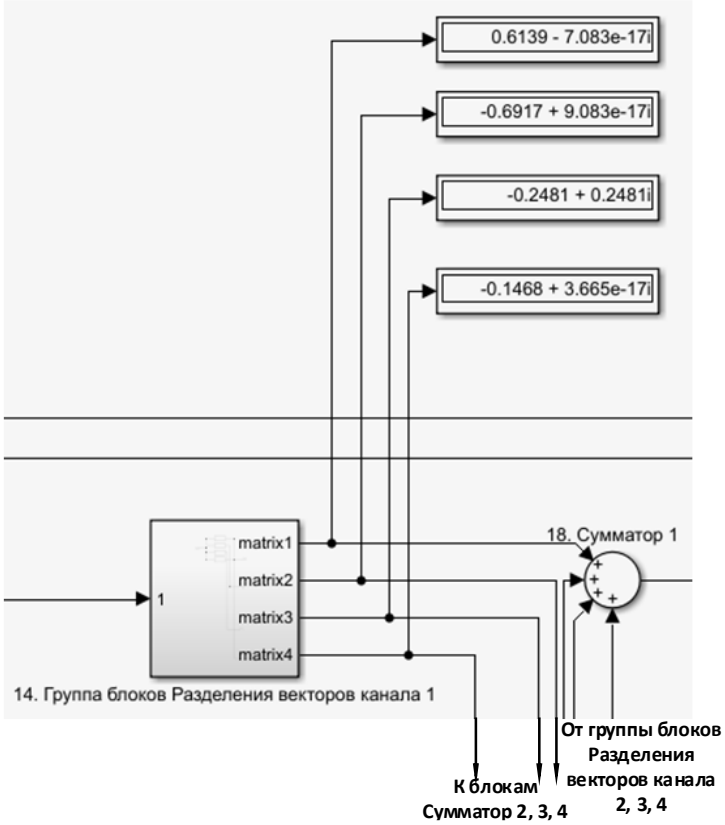


Рисунок 4.14 – Процесс разделения векторов 1-4 и подачи их на вход блоков сумматор 1-4

Аналогичным образом происходит разделение векторов 2-4 в блоках разделения векторов 2-4 и подача их на входы блоков сумматор 1-4.

Группа блоков разделения векторов 5-8 канала 2 разделяет модулированный СВ ЭМ на составные части. На вход каждого блока разделения векторов 5-8 поступает одинаковый сигнал от блока модуляции 2, на выходе блока разделения вектора 5 выходит первый модулированный элемент СВ 2, на выходе блока разделения вектора 6 выходит второй модулированный элемент СВ 2, на выходе блока разделения вектора 7 выходит третий модулированный элемент СВ 2, на выходе блока разделения вектора 8 выходит четвертый модулированный элемент СВ 2.

Группа блоков разделения векторов 9-12 канала 3 разделяет модулированный СВ ЭМ на составные части. На вход каждого блока разделения векторов 9-12 поступает одинаковый сигнал от блока модуляции 3, на выходе блока разделения вектора 9 выходит первый модулированный элемент СВ 3, на выходе блока

разделения вектора 10 выходит второй модулированный элемент СВ 3, на выходе блока разделения вектора 11 выходит третий модулированный элемент СВ 3, на выходе блока разделения вектора 12 выходит четвертый модулированный элемент СВ 3.

Группа блоков разделения векторов 13-16 канала 4 разделяет модулированный СВ ЭМ на составные части. На вход каждого блока разделения векторов 13-16 поступает одинаковый сигнал от блока модуляции 4, на выходе блока разделения вектора 13 выходит первый модулированный элемент СВ 4, на выходе блока разделения вектора 14 выходит второй модулированный элемент СВ 4, на выходе блока разделения вектора 15 выходит третий модулированный элемент СВ 4, на выходе блока разделения вектора 16 выходит четвертый модулированный элемент СВ 4.

6. Блоки сумматор 1-4.

Блок сумматор 1 суммирует первые элементы модулированных СВ 1-4, поступающие с выходов блока разделения векторов 1, 5, 9, 13 и передает их на блок канального объединителя.

Блок сумматор 2 суммирует вторые элементы модулированных СВ 1-4, поступающие с выходов блока разделения вектора 2, 6, 10, 14 и передает их на блок канального объединителя.

Блок сумматор 3 суммирует третьи элементы модулированных СВ 1-4, поступающие с выходов блока разделения вектора 3, 7, 11, 15 и передает их на блок канального объединителя.

Блок сумматор 4 суммирует четвертые элементы модулированных СВ 1-4, поступающие с выходов разделения вектора 4, 8, 12, 16 и передает их на блок канального объединителя.

На рисунке 4.15 иллюстрируется результат суммирования первых элементов СВ ЭМ 1-4 и подачи группового сигнала на блок канальный объединитель.

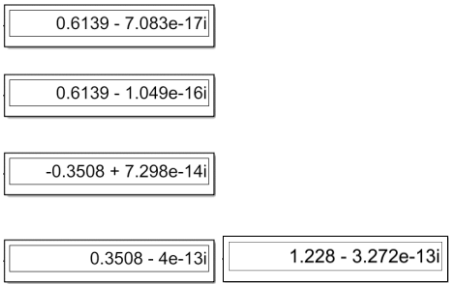


Рисунок 4.15 – Процесс суммирования первых элементов собственных векторов ЭМ 1-4

7. Блок канальный объединитель объединяет сигналы, поступающие на его входы 1-4 от блоков сумматор 1-4 в единый вектор и последовательной передачи суммы первых элементов, модулированных СВ 1-4, затем суммы вторых элементов модулированных СВ 1-4, затем суммы третьих элементов модулированных СВ 1-4, затем суммы четвертых элементов модулированных СВ 1-4 на блок преобразования последовательностей в квадратурную форму и передаче в блок БФГС.

Результат объединения значений выходов блоков сумматор 1-4 в блоке канальный объединитель иллюстрируется на дисплее 7, как указано на рисунке 4.16.

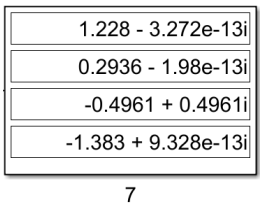


Рисунок 4.16 – Результат объединения значений выходов блоков сумматор 1-4 в блоке канальный объединитель

8. Блок БФГС преобразует групповой сигнал, поступающий с выхода блока канального объединителя в квадратурную форму (дисплей 7) путём модуляции групповым сигналом канальной несущей частоты и подает его на вход 1 блока канальный сумматор 5, имитирующего линию связи (дисплей 8).

На рисунке 4.17 представлена осциллограмма, показывающая групповой сигнал на выходе передатчика (входе линии связи).

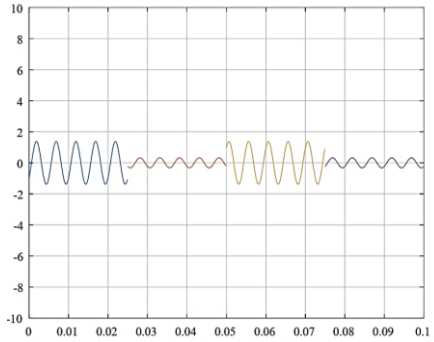


Рисунок 4.17 – Осциллограмма сигнала на выходе передатчика (входе линии связи)

Модель канала связи представляет собой линию связи между передатчиком и приемником, состоящую из блока генератор помехи и блока канальный сумматор 5, предназначенного для сложения группового сигнала, поступающего в линию связи с помехой.

9. Блок генератор помехи формирует помеху в виде шумового сигнала типа «Белый шум» и подает его на вход 2 блока канальный сумматор 5.

Шумовой сигнал используется для имитации помехи в канале связи.

На рисунке 4.18 представлена осциллограмма сигнала с помехой типа «Белый шум» при отношении $\frac{P_{\text{с}}}{P_{\text{ш}}} = 0$ дБ, поступающий из канала связи на вход приемного устройства ССС с КРК.

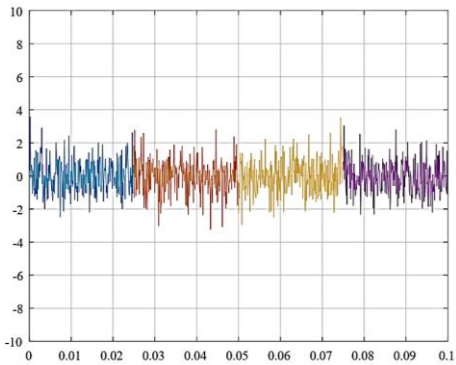


Рисунок 4.18 – Осциллограмма помехи типа «Белый шум» в канале связи

10. Блок канальный сумматор 5 накладывает помеху типа «Белый шум» на групповой сигнал, поступающий в линию связи от блока БФГС. С выхода блока канальный сумматор 5 сигнал с помехой поступают на вход приемной части ССС с КРК (дисплей 9).

На рисунке 4.19 представлена осциллограмма сигнала с помехой типа «Белый шум» в канале связи на входе приемного устройства ССС с КРК.

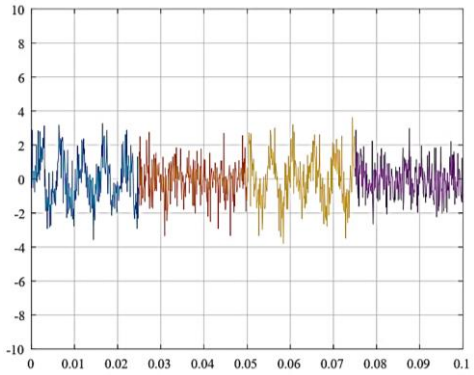


Рисунок 4.19 – Осциллограмма сигнала с помехой типа «Белый шум» в канале связи на входе приемного устройства ССС с КРК

Приемная часть модели ССС с КРК на основе стохастического применения ортогональных кодовых последовательностей предназначена для выделения группового сигнала на фоне помехи и последующей ее обработки в информационных каналах с целью выделения полезного сообщения.

11. Блок БОПГС осуществляет преобразование группового сигнала, поступающего из блока канальный сумматор 5, имитирующего линию связи из квадратурной формы в последовательность комплексных чисел (комплексный вид). С выхода блока БОПГС сигнал в алгебраической форме поступает на входы канальных объединителей 1-4 индивидуальных информационных каналов 1-4.

На рисунке 4.20 представлена визуализация отличия исходного канального сигнала на выходе передатчика, как указано на дисплее 7 и сигнала, испытывающего влияние помехи типа «Белый шум» на входе приемника, как указано на дисплее 8.

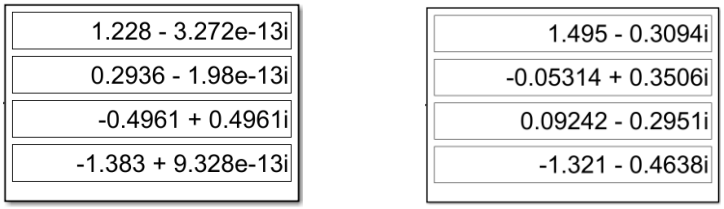


Рисунок 4.20 – Визуализация отличия исходного канального сигнала на выходе передатчика (дисплей 7) и сигнала, испытывающего влияние помехи типа «Белый шум» на входе приемника (дисплей 8)

На рисунке 4.21 представлена осциллограмма, показывающая демодулированный групповой сигнал на выходе демодулятора.

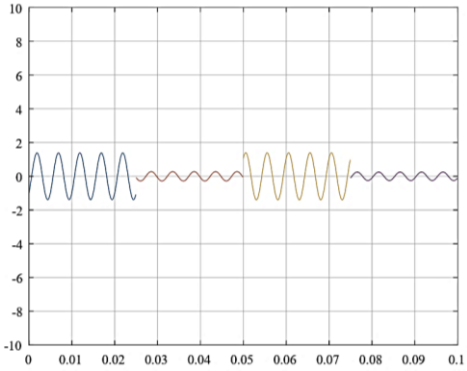


Рисунок 4.21 – Осциллограмма демодулированного группового сигнала на выходе демодулятора

Анализ осциллограммы исходного группового сигнала на выходе передатчика (входе линии связи), представленного на рисунке 4.17, и осциллограммы демодулированного группового сигнала на выходе демодулятора, представленной на рисунке 4.21 указывает на отсутствие ошибок в канале связи при мощности помехи, раной мощности сигнала.

12. Блоки канальный объединитель 1-4.

Блок канальный объединитель 1 осуществляет объединение группового сигнала, поступающего с выхода блока БОПГС с копией первой последовательности из состава АМФОКП. Для упрощения моделирования и

синхронизации передающей и приемной частей ССС с КРК в канальных объединителях приемной части используется АМФОКП, формируемый на передающей части блоков селектор 1-4. С выхода канального объединителя 1 объединенный сигнал поступает в коррелятор 1.

Аналогичным образом в блоках канальный объединитель 2-4 осуществляется объединение группового сигнала, поступающего с выхода блока БОПГС и соответствующего номеру канала выхода блока селектор 2-4.

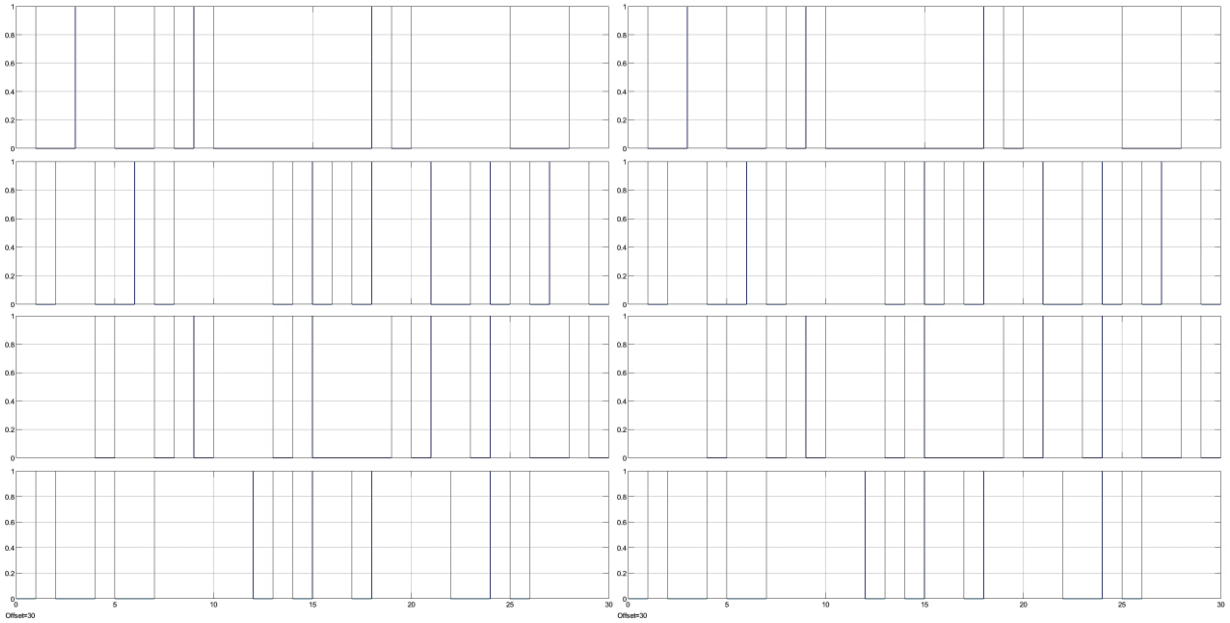
13. Блоки коррелятор 1-4.

Блок коррелятор 1 представляет собой вычислитель корреляционной функции между сигналом, поступающим из блока канальный объединитель 1 и копией первой последовательности из состава АМФОКП. С помощью него осуществляется выделение информационной последовательности, в первом информационном канале.

Аналогичным образом в блоках коррелятор 2-4 осуществляется вычисление корреляционной функции между сигналом, поступающим из блока канальный объединитель 2-4 и копией соответствующей последовательности из состава АМФОКП. С их помощью осуществляется выделение информационной последовательности, в втором-четвертом информационных каналах.

Выходы корреляторов подключены к блоку осциллограф 1. С целью сравнения принятой информационной последовательности с исходной информационной последовательностью, последняя выведена на блок осциллограф 2.

На рисунке 4.22 представлены осциллограммы информационного сигнала на входе каждого канала передающей части ССС с КРК, представленной на рисунке 4.5 (рисунок 4.22 а) и на выходе каждого канала приемной части ССС с КРК, представленной на рисунке 4.6 (рисунок 4.22 б) с целью сравнения достоверности принятого сигнала.



а б

Рисунок 4.22 Осциллограммы информационного сигнала:
а) на входе каждого канала передающей части ССС с КРК;
б) на выходе каждого канала приемной части ССС с КРК

Сравнение указанных осциллограмм позволяет сделать вывод о высокой достоверности принятого сигнала.

При корректной работе модели в условиях помех передаваемые информационные последовательности в канале 1-4 будут соответствовать принятым информационным последовательностям, получаемым на выходах блоков корреляторов 1-4.

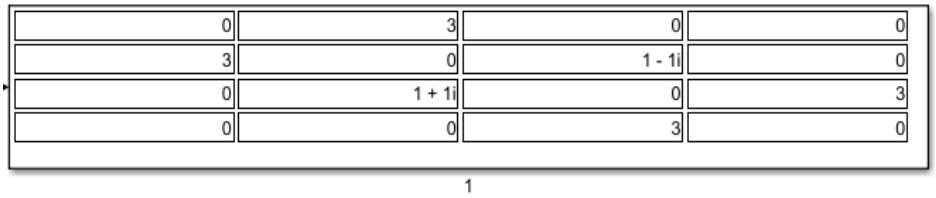
Наблюдая передаваемые информационные последовательности на блоке осциллограф 2 и принятые информационные последовательности на блоке осциллограф 1 можно их сопоставить и сделать вывод о корректности работы ССС с КРК.

Смена АМФОКП в процессе передачи информации.

Через интервал времени, соответствующий передаче одного информационного символа на выходе ГПСКЧ будет сформирован новый набор ПСКЧ, который будет присвоен коэффициентом второй верхней диагонали ЭМ, а затем, с учетом свойств комплексно-сопряженных чисел, будет построена вторая

нижняя диагональ ЭМ с комплексно-сопряженными числами второй верхней диагонали ЭМ.

На рисунке 4.23 представлена ЭМ после смены значений диагональных коэффициентов.

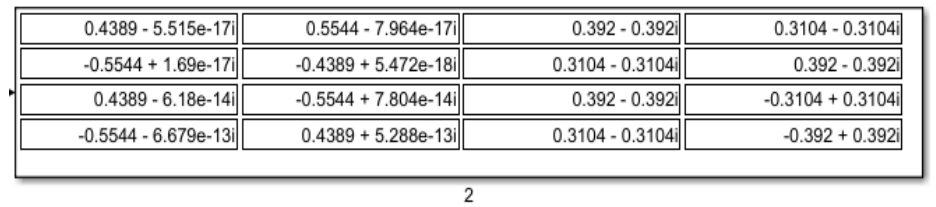


0	3	0	0
3	0	1 - 1i	0
0	1 + 1i	0	3
0	0	3	0

1

Рисунок 4.23 – ЭМ, сформированная после смены значений диагональных коэффициентов

На рисунке 4.24 представлен вид матрицы СВ ЭМ, после ввода коэффициентов, представленных на рисунке 4.21.



0.4389 - 5.515e-17i	0.5544 - 7.964e-17i	0.392 - 0.392i	0.3104 - 0.3104i
-0.5544 + 1.69e-17i	-0.4389 + 5.472e-18i	0.3104 - 0.3104i	0.392 - 0.392i
0.4389 - 6.18e-14i	-0.5544 + 7.804e-14i	0.392 - 0.392i	-0.3104 + 0.3104i
-0.5544 - 6.679e-13i	0.4389 + 5.288e-13i	0.3104 - 0.3104i	-0.392 + 0.392i

2

Рисунок 4.24 – Матрица СВ ЭМ после смены значений диагональных коэффициентов

Таким образом, в процессе передачи информации в рассматриваемой модели ССС с КРК на основе стохастического применения АМФОКП, каждый информационный символ каждого информационного канала будет передаваться при помощи уникальной реализации АМФОКП с неповторяющейся структурой, изменяющейся по одинаковому закону на передающей и приемной стороне. С точки зрения злоумышленника стохастическое изменение ПСКЧ, на основе которых формируется АМФОКП, будут иметь случайный непредсказуемый закон изменения. Для передающей и приемной частей ССС с КРК данные изменения

осуществляются по определенному известному только для них алгоритму [104, 106, 112, 113].

4.4 Выводы по главе

1. Принцип защиты информации от угрозы подмены сообщений в ССС с КРК заключается в том, что каждый информационный символ каждого информационного канала передается при помощи уникальной реализации АМФОКП размерностей $N = 128, 256$ с неповторяющейся структурой, изменяющейся по одинаковому закону на передающей и приемной стороне. Техническое решение предложено в виде стохастического средства защиты информации, включающее генератор ПСКЧ, генератор псевдослучайных АМФОКП, устройство синхронизации и буферный накопитель, которые имеют техническую возможность сформировать множество кодовых последовательностей и использовать их стохастическим образом.

2. Для решения задачи разработки структуры и алгоритма функционирования генератора псевдослучайных АМФОКП за основу выбран Генератор функций Попенко-Турко [11], в силу наличия у него достоинств и универсальности. Для построения генератора псевдослучайных АМФОКП структура исходного ГФПТ дополнена блоком псевдослучайного формирования комплексно-сопряженных коэффициентов ЭМ, состоящим из МК, ГПСКЧ, БН, блока N – разрядного ОЗУ. Кроме того, в ГФПТ исключена обратная 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 СВ ЭМ для исключения цикличности вывода ортогонального базиса.

3. Алгоритм формирования АМФОКП состоит из одиннадцати этапов и позволяет из наборов последовательностей ПСКЧ, формируемых ГПСКЧ, получить наборы соответствующих им АМФОКП.

4. Разработанный генератор формирования АМФОКП может иметь широкую область применения, заключающуюся в генерировании АМФОКП, число которых может быть отлично от 2^m, где m – натуральное число, имеющих широкий набор значений периодов генерируемых функций и большое число значений ортогональных базисных функций за счет автоматизации процесса присвоения псевдослучайных значений диагональным коэффициентам ЭМ A.

5. Для оценки возможности практической реализации была разработана компьютерная модель ССС с КРК на основе стохастического применения АМФОКП в среде Matlab SIMULINK. Модель состоит из передающей части, приемной части и канала связи и экспериментально доказывает возможность практической реализации скрытной передачи информации на основе стохастического применения АМФОКП.

6. Разработанная модель ССС с КРК, в которой в процессе передачи информации на основе стохастического применения АМФОКП, каждый информационный символ каждого информационного канала передается при помощи уникальной реализации АМФОКП с неповторяющейся структурой, изменяющейся по одинаковому закону на передающей и приемной стороне. Результаты компьютерного моделирования ССС с КРК показывают корректность ее работы с учетом стохастического применения АМФОКП при различных отношениях сигнал/шум в канале связи.

ЗАКЛЮЧЕНИЕ

В диссертации решена важная **научная задача** разработки метода противодействия угрозе подмены сообщений для ССС с КРК на основе синтеза, формирования и стохастического применения ансамблей многофазных ортогональных кодовых последовательностей, который включает в себя:

- модель противодействия угрозе подмены сообщений в ССС с КРК на основе стохастического применения АМФОКП;

- модель АМФОКП и алгоритм их синтеза для стохастического применения в ССС с КРК, обеспечивающие требуемый уровень их структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ;

- принцип и техническое решение по противодействию угрозе подмены сообщений в ССС с КРК.

Модель противодействия угрозе подмены сообщений в ССС с КРК содержит четырнадцать этапов и позволяет снизить вероятность разведки структуры сигнала $P_{\text{разв.}}$ от которой зависит успешность реализации злоумышленником угрозы подмены сообщений за счет снижения вероятности раскрытия структуры сигнала при условии его обнаружения $P_{\text{стр.}}$.

Модель АМФОКП основана на использовании множества наборов собственных векторов ЭМ, которые в каждом конкретном случае вычисляются в соответствии с набором значений модулей и аргументов диагональных коэффициентов ЭМ. Используя различные наборы таких коэффициентов, в соответствии с разработанным алгоритмом синтеза, определяются различные по своей структуре ансамбли ортогональных кодовых последовательностей в количестве, превышающем требуемое значение $A_{\text{треб.}} \geq 4{,}54 \cdot 10^{12}$ для размерностей $N = 128, 256$.

Принцип защиты информации от угрозы подмены сообщений в ССС с КРК заключается в том, что каждый информационный символ каждого информационного канала передается при помощи уникальной реализации АМФОКП размерностей $N = 128, 256$ с неповторяющейся структурой, изменяющейся по одинаковому закону на передающей и приемной стороне. Техническое решение предложено в виде стохастического средства защиты информации, включающее генератор ПСКЧ, генератор псевдослучайных АМФОКП, устройство синхронизации и буферный накопитель, которые имеют техническую возможность сформировать множество кодовых последовательностей и использовать их стохастическим образом.

В процессе работы были получены следующие результаты:

1. Разработанная модель противодействия угрозе подмены сообщений в ССС с КРК на основе синхронного генерирования и стохастического применения АМФОКП обеспечивает повышение их структурной скрытности выше требуемого значения $S_{\text{треб.}} \geq 43$ ДИЗ, отличается от известных тем, что при передаче каждого информационного бита используется уникальная неповторяющаяся структура многофазной ортогональной кодовой последовательности синхронно изменяемая на приемной и передающей сторонах.

2. Разработанная модель АМФОКП требуемых размерностей $L = 128, 256$ и алгоритм их синтеза, по сравнению с известной моделью АДОМУС, позволяют увеличить выигрыш в структурной скрытности АМФОКП. Получаемые АМФОКП имеют прирост структурной скрытности по отношению к структурной скрытности АДОМУС, который лежит в пределах для порядка матрицы $n = 128$ от 2,5 до 101,31%, для $n = 256$ от 2,32 до 101,02%. Данный выигрыш обеспечивается при условии, что фазовый сдвиг между элементами кодовой последовательности изменяется на угол $\Delta\varphi_i = 18^{\circ}$ и, соответственно $\Delta\varphi_i = 1^{\circ}$. Значение структурной скрытности АМФОКП для фазового сдвига между элементами кодовой последовательности $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения

структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для L=128 и L=256, что позволяет их использовать в существующих ССС с КРК.

3. Полученные принцип построения и техническое решение генератора псевдослучайных АМФОКП для стохастического средства защиты информации ССС с КРК, в отличие от известных, обеспечивают генерацию ансамблей многофазных ортогональных кодовых последовательностей, описываемых комплексными числами.

Научная новизна полученных результатов диссертационной работы состоит в том, что:

1. Разработанная модель противодействия угрозе подмены сообщений в ССС с КРК, отличающаяся от известных тем, что при передаче каждого информационного бита используется уникальная неповторяющаяся структура ансамбля многофазных ортогональных кодовых последовательностей синхронно изменяемых на приемной и передающей сторонах.

2. Модель АМФОКП требуемых размерностей $N = 128, 256$ и алгоритм их синтеза которые, в отличие от известных, основаны на рассмотрении множества эрмитовых матриц порядка $(n \times n)$, элементы которых являются комплексными числами и задают все возможные ортогональные базисы пространства C^n – комплексных чисел.

3. Принцип построения и техническое решение генератора псевдослучайных АМФОКП для стохастического средства защиты информации системы спутниковой связи с кодовым разделением каналов, позволяющие, в отличие от известных, генерировать псевдослучайные АМФОКП на основе собственных векторов эрмитовых матриц в соответствии с задаваемым набором псевдослучайных комплексных чисел.

Практическая ценность работы состоит в следующем:

- Разработанные технические решения по повышению защищённости информации, защищённые патентами на изобретения и свидетельствами на регистрацию программ для ЭВМ, реализующие предложенные алгоритмы, обеспечивают реализацию модели и алгоритма противодействия угрозе подмены

передаваемых в ССС с КРК сообщений на основе формирования и стохастического применения АМФОКП. В случае использования разработанного алгоритма противодействия угрозе подмены сообщений за счет стохастического применения неповторяющихся псевдослучайных АМФОКП происходит преобразование исходной информации и её передача в канал связи с помощью изменяющихся стохастическим образом ансамблей ортогональных кодовых последовательностей для передачи каждого информационного символа, что обеспечивает повышение их структурной скрытности. Получаемые АМФОКП имеют прирост структурной скрытности по отношению к структурной скрытности АДОМУС, который лежит в пределах для порядка матрицы $n = 128$ от 2,5 до 101,31%, для $n = 256$ от 2,32 до 101,02%. Данный выигрыш обеспечивается при условии, что фаза каждого диагонального коэффициента ЭМ изменяется на угол $\Delta\varphi_i = 18^{\circ}$ и, соответственно $\Delta\varphi_i = 1^{\circ}$. Значение структурной скрытности АМФОКП для $\Delta\varphi_i = 90^{\circ}$ также находится выше требуемого значения структурной скрытности $S_{\text{треб.}} \geq 43$ ДИЗ для L=128 и L=256, что позволяет их использовать в существующих ССС с КРК.

- Структура и алгоритм функционирования генератора псевдослучайных АМФОКП, защищённые патентами на изобретения и свидетельствами на регистрацию программ для ЭВМ, позволяют формировать АМФОКП с изменяющейся структурой на основе СВ ЭМ в соответствии с набором псевдослучайных комплексных чисел, поступающих на вход генератора, и могут быть применены для усовершенствования стохастического средства защиты информации в ССС с КРК.

- Разработанное программное обеспечение для ПЭВМ в пакете Matlab SIMULINK, защищённое свидетельством о государственной регистрации программы для ЭВМ позволяет выполнять исследования процесса передачи информации в модели ССС с КРК на основе стохастического применения АМФОКП при изменении отношения сигнал/шум в канале связи.

- Даны рекомендации по использованию компьютерной модели в пакете Matlab SIMULINK ССС с КРК, реализующей модель противодействия угрозе

подмены сообщений на основе применения стохастического средства защиты информации.

Практическая ценность результатов диссертационной работы подтверждается актами внедрения результатов исследования в ООО «Инфоком-С», ФГАОУ ВО «Северо-Кавказский федеральный университет», в которых использованы результаты исследований.

Основные положения диссертации опубликованы в 14 научных печатных работах в том числе: 5 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК РФ, 9 – в материалах конференций и других изданиях. Получено 4 патента на изобретение, 3 свидетельства о государственной регистрации программ для ЭВМ.

Возможными направлениями дальнейших исследований являются развитие методов скрытного информационного обмена в высокоскоростных сетях на основе различных технологий мультиплексирования с кодовым разделением каналов и стохастическим применением ансамблей ортогональных кодовых последовательностей различных классов, а также новых принципов их формирования с высоким быстродействием и повышенной точностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Макаренко, С. И. Описательная модель системы спутниковой связи Inmarsat / С. И. Макаренко. – Текст : электронный // Системы управления, связи и безопасности. – 2018. – № 4. – С. 64-91. – URL: http://sccs.intelgr.com/archive/2018-04/04-Makarenko.pdf (дата обращения : 23.06.2020).

2. Макаренко, С. И. Описательная модель системы спутниковой связи Iridium / С. И. Макаренко. – Текст : электронный // Системы управления, связи и безопасности. – 2018. – № 4. – С. 1-34. – URL: http://sccs.intelgr.com/archive/2018-04/01-Makarenko.pdf (дата обращения : 24.06.2020).

3. Макаренко, С. И. Описательная модель системы спутниковой связи MUOS / С. И. Макаренко. – Текст : электронный // Системы управления, связи и безопасности. – 2019. – № 3. – С. 89-116. – DOI: 10.24411/2410-9916-2019-10306 (дата обращения : 21.06.2020).

4. Пехтерев, С. В. Описательная модель системы спутниковой связи Starlink / С. В. Пехтерев, С. И. Макаренко, А. А. Ковальский. – Текст : электронный // Системы управления, связи и безопасности. – 2022. – № 4. – С. 190-255. DOI: 10.24412/2410-9916-2022-4-190-255 (дата обращения: 19.06.2020).

5. Антохин, Е. А. Основные требования к беспроводным каналам связи наземных робототехнических комплексов военного назначения / Е. А. Антохин, Н. Н. Панасенко, А. Д. Чернова. – Текст : непосредственный // Робототехника и техническая кибернетика. – 2017. – № 4 (17). – С. 10-14.

6. Дятлов, А. П. Вскрытие временной структуры пакетных фазоманипулированных сигналов / А. П. Дятлов, П. А. Дятлов, А. Н. Шостак. – Текст : непосредственный // Журнал радиотехники. – 2015. – № 3. – С. 16.

7. Жук, А. П. Влияние коэффициентов второй диагонали эрмитовой матрицы на корреляционные и спектральные свойства определяемых ею ортогональных в усиленном смысле сигналов / А. П. Жук, В. В. Сазонов. – Текст :

непосредственный // Физика волновых процессов и радиотехнические системы. – 2007. – Т. 10. – № 6. – С. 52-54.

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

9. Петрович, Н. Т. Системы связи с шумоподобными сигналами / Н. Т. Петрович, М. К. Размахнин. – Москва : Издательство «Советское радио», 1969. – 232 с. – Текст : непосредственный.

10. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью / В. И. Борисов, В. М. Зинчук, А. Е. Лимарев [и др.]; Под редакцией В. И. Борисова. – Москва : «Радио и связь», 2003. – 640 с. – Текст : непосредственный.

11. Патент № 1753464 A1 Российская Федерация, МПК G06F 1/02 (2006.01). Генератор функций Попенко-Турко : № SU 1 753 464 A1 : заявлено 06.03.1990 : опубликовано 07.08.1992 / Попенко В. С., Турко С. А. – Текст : электронный // Яндекс. Патенты. – URL: SU1753464A1 - Генератор функций Попенко-Турко - Яндекс.Патенты (дата обращения 27.06.2020).

12. Попенко, В. С. Оценка ширины спектра дискретных сигналов / В. С. Попенко. – Текст : непосредственный // Радиотехника. – 1996. – № 11. – С. 57-59.

13. Попенко, В. С. Векторный синтез ансамблей ортогональных сигналов. Часть 3 / В. С. Попенко. – Ставрополь, 1993. – 150 с. – Текст : непосредственный.

14. Труханович, А. Л. Разработка модуля передачи данных по радиоканалу / А. Л. Труханович, С. С. Тюшкевич. – Текст : непосредственный // Сборник работ 69-й научной конференции студентов и аспирантов Белорусского государственного университета 14-17 мая 2012 г., Минск. В 3 частях. Часть I. – Минск, 2013. – С. 283-286.

15. Mahdi Sharifi. Using chaotic sequence in direct sequence spread spectrum based on code division multiple access (DS-CDMA) / Mahdi Sharifi, Mohammad Jafar

Pour Jalali. – Text : direct // ARPN Journal of Engineering and Applied Sciences. – 2017. – V. 12. – No. 20. – pp. 5837-5846.

16. Proakis J. Digital Communications / J. Proakis. – New York NY : McGraw-Hill, 2001. – 928 p. – Text : direct.

17. Жук, А. П. Алгоритм синтеза ансамблей многофазных ортогональных кодовых последовательностей для защищённой системы передачи информации с кодовым разделением каналов / А. П. Жук, А. В. Студеникин, Д. Е. Белов. – Текст : непосредственный // Телекоммуникации. – 2021. – № 10. – С. 21-30. – DOI: 10.31044/1684-2588-2021-0-10-21-30.

18. Dixon R. Spread spectrum systems / R. Dixon. – New York NY, Wiley, 1976. – 318 p. – Text : direct.

19. Orel D. A method of forming code sets for CDMA in communication, navigation and control systems / D. Orel, A. Zhuk, , E. Zhuk, L. Luganskaia // CEUR Workshop Proceedings. 2017. – Text : direct.

20. Pashintsev V. P. Formation Algorithms and Properties of Binary Quasi-Orthogonal Code Sequence of Modern Satellite Systems / V. P. Pashintsev, I. A. Kalmykov, A. P. Zhuk, D. V. Orel, E. P. Zhuk // International Journal of Engineering & Technology. – 2018. – Vol. 7 (4.38). – pp. 1205-1209. – Text : direct.

21. Афанасьев, В. В. Вейвлет-анализ сигналов радиоэлектронных систем с динамическим хаосом / В. В. Афанасьев, С. С. Логинов, Ю. Е. Польский. – Текст : непосредственный // Вестник КГТУ имени А. Н. Туполева. – 2013. – № 1. – С. 61-66.

22. Бабкин, А. Н. Защищенные сети радиосвязи органов внутренних дел / А. Н. Бабкин. – Текст : непосредственный // Охрана, безопасность, связь. – 2017. – № 1-1. – С. 34-38.

23. Авраменко, В. С. Модель для количественной оценки защищенности информации от несанкционированного доступа в автоматизированных системах по комплексному показателю / В. С. Авраменко, А. В. Козленко. – Текст : непосредственный // Труды СПИИРАН. – 2010. – Выпуск 2 (13). – С. 172–179.

24. Ажмухамедов, И. М. Модифицированная беспроводная охранная система Wireless Security / И. М. Ажмухамедов, З. А. Носиров. – Текст : непосредственный // Проблемы информационной безопасности: материалы VI Всероссийской научной конференции, (21-22 декабря 2016 года). – Ростов н-на-Дону : Издательско-полиграфический комплекс РГЭУ (РИНХ), 2016. – С. 164-167. Аливер, В. Ю. Хаотические режимы в непрерывных динамических системах / В. Ю. Аливер. – Текст : непосредственный // Вестник МГТУ им. Н. Э. Баумана. Серия: Приборостроение. – 2006. – № 1. – С. 65-84.

25. Алиев, Т. И. Основы моделирования дискретных систем / Т. И. Алиев. – Санкт-Петербург : СПбГУ ИТМО, 2009. – 363 с. – Текст : непосредственный.

26. Pietro Tedeschi, Savio Sciancalepore, Roberto Di Pietro Satellite-based communications security: A survey of threats, solutions, and research challenges // Computer Networks. – 2022. – Vol. 216. – Article no 109246. – DOI 10.1016/j.comnet.2022.109246. (Published 24 October 2022).

27. Brandon Bailey. Cybersecurity Protections for Spacecraft : A Threat Based Approach. Cyber Assessment and Research Department (CARD) Cybersecurity Subdivision (CSS) / Bailey Brandon. – Text : electronic // Prepared for: U.S. GOVERNMENT AGENCY/ April 29, 2021. – URL : https://www.cs2ai.org/ot-cyber-reports-and-papers/cybersecurity-protections-for-spacecraft%3A-a-threat-based-approach-(дата обращения 21.07.2021).

28. Gregory Falco. A Security Risk Taxonomy for Commercial Space Missions / Gregory Falco, Nicolò Boschetti. – Text : direct. ASCEND 2021. November 15-17, 2021, Las Vegas, Nevada & Virtual. DOI: 10.2514/6.2021-4241.

29. Brandon Bailey. Defending Spacecraft in the cyber domain / Brandon Bailey, Ryan J. Speelman, Prashant A. Doshi, Nicholas C. Cohen, Wayne A. Wheeler. – Text : direct // Center for space policy and strategy. Aerospace Corporation. November 2019.

30. Maj Brian Garino, USAF, and Maj Jane Gibson, USAF. Space System Threats. 2009. – URL : https://api.semanticscholar.org/CorpusID:11134785. (дата обращения: 10.08.2022). – Text : electronic.

31. Гришенцев, А. Ю. Защита канала широкополосной связи с применением ортогональных шумоподобных сигнальных символов / А. Ю. Гришенцев, С. А. Арустамов, А. Г. Коробейников, О. В. Козин. – Текст : непосредственный // Научно-технический вестник информационных технологий, механики и оптики. – 2019. – Том 19. – № 2. – С. 280-291.

32. L. Schiff. Design and system operation of GlobalstarTM versus IS-95 CDMA – similarities and differences / Leonard Schiff and A. Chockalingam. – Text : direct // Wireless Networks. – No. 6 – p. 47-57.

33. Урядников, Ю. Ф. Сверхширокополосная связь. Теория и применение / Ю. Ф. Урядников, С. С. Аджемов. – Москва : СОЛОН-Пресс, 2005. – 368 с. – Текст : непосредственный.

34. Кузнецов, А. П. Стабилизация хаоса в системе Рёсслера импульсным и гармоническим сигналом / А. П. Кузнецов, Н. В. Станкевич, Н. Ю. Чернышов. – Текст : непосредственный // Известия вузов «ПНД». – 2010. – Т. 18. – № 4. – С. 3-16.

35. Каневский, З. М. Теория скрытности. Часть 1. Основы теории скрытности : учебное пособие / З. М. Каневский, В. П. Литвиненко, Г. В. Макаров. – Воронеж : Государственный технический университет, 2003. – 92 с. – Текст : непосредственный.

36. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / В. И. Борисов [и др.]. – Москва : «Радио и связь», 2000. – 384 с.– Текст : непосредственный

37. Кандауров, Н. А. Сигнально-кодовые конструкции для низкоэнергетических широкополосных радиолиний декаметрового диапазона : диссертация ... кандидата технических наук : 05.12.13 / Кандауров Николай Александрович ; [Место защиты: Московский технический университет связи и информатики]. – Москва, 2019. – 147 с. – Текст : непосредственный.

38. Метод формирования многопозиционных помехозащищенных сигнальных конструкций / С. В. Дворников, А. В. Пшеничников, С. С. Манаенко, С. С. Дворников // Информационные технологии. – 2017. – Т. 23, № 9. – С. 669-676.

39. Айтмагамбетов, А. З. Системы подвижной спутниковой связи: учебное пособие / А. З. Айтмагамбетов. – Алматы : АИЭС, 2006. – 106 с. – Текст : непосредственный.

40. Golomb S. Digital communications with space applications / S. Golomb/ – Upper Saddle River NJ, Prentice-Hall, 1964. – 210 p. – Text : direct.

41. Зюко, А. Г. Теория передачи сигналов : учебник для вузов / А. Г. Зюко, Д. Д. Кловский, М. В. Назаров, Л. М. Финк. – Москва : «Радио и связь», 1986. – 304 с. – Текст : непосредственный.

42. Мазурков М. И. Системы широкополосной радиосвязи : учебное пособие для студентов вузов / М. И. Мазурков. – Одесса : «Наука и техника», 2009. – 344 с. – Текст : непосредственный.

43. Siamäk Naghian Mobile satellite CDMA system. Licentiate Course on Signal Processing in Communications S-38.220, FALL. – 97 MOBILE SATELLITE CDMA SYSTEM. – Siamäk Naghian P.O. Box 311, FIN-00045 NOKIA GROUP siamak.naghian#ntc.nokia.com. – Date: 4.12.1997 (дата обращения: 26.12.2024). – Text : electronic.

44. Ran Cheng, Wei Wei, Weilin Xie, Yi Dong. Programmable linear frequency modulated signal generation using a compact photonics-based scheme / Ran Cheng, Wei Wei, Weilin Xie, Yi Dong. – Text : direct // 2019 International Topical Meeting on Microwave Photonics (MWP) 2019 г. Conference Paper 7-10 October 2019, Ottawa, ON, Canada. DOI: 10.1109/MWP.2019.8892087.

45. Report Concerning Space Data System Standards «Data transmission and PN ranging for 2 GHz CDMA link via data relay satellite», CCSDS Secretariat, Space Communications and Navigation Office, 7L70, Space Operations Mission Directorate, NASA Headquarters, Washington, DC 20546-0001, USA. – Text : direct.

46. Diakoumis Gerakoulis, Evaggelos Geraniotis, Hsuan-.J ung Su. Network Access and Synchronization Procedures for a CDMA Satellite Communication System / Diakoumis Gerakoulis, Evaggelos Geraniotis, Hsuan-.J ung Su. –Text : direct // MILCOM 1999. IEEE Military Communications. Conference Proceedings (Cat.

No.99CH36341) October 1999 – 03 November 1999. Atlantic City, NJ, USA. DOI: 10.1109/MILCOM.1999.822716.

47. Robert J Finean, Kokusai Denshin. Chapter 7 Satellite Channel Assignment / Robert J Finean, Kokusai Denshin. – URL: https://rfinean. tripod.com/PhD/7ChAlloc.pdf (дата обращения 13.07.2023). – Text : electronic.

48. Стасев, Ю. В. Применение сложных сигналов в командно-телеметрических радиолиниях / Ю. В. Стасев, И. Д. Горбенко, Б. И. Макаренко, А. В. Ивашкин, Д. Н. Воронов. – Текст : непосредственный // Космическая наука и технология. – 1997. – Том 3. – № 5/6. – С. 104-108.

49. Andreas Springer, Mario Huemer, Wolfgang Gugler, Leo Reindl. Spread spectrum communications using chirp signals / Andreas Springer, Mario Huemer, Wolfgang Gugler, Leo Reindl. – Text : electronic // Conference Paper May 2000, DOI: 10.1109/EURCOM.2000.874794. Source: IEEE Xplore. – URL: https://www.researchgate.net/publication/3867801 (дата обращения: 12.05.2022).

50. Рекомендации МСЭ-R. – Москва. – с. 67-70. – URL: https://standardsclub.com/product/itu-r-m-1850-2. (дата обращения: 10.02.2021). – Текст : электронный.

51. NASA. – URL :https://trends.rbc.ru/trends/industry/614da42d9a7947b3101372 b3 (дата обращения: 09.03.2023). – Text : electronic.

52. Сухарев, Е. М. Общесистемные вопросы защиты информации : коллективная монография / Е. М. Сухарев [и др.]. Книга 1. – Москва : «Радиотехника», 2003. – 296 с. – Текст : непосредственный.

53. Осмоловский, С. А. Стохастические методы защиты информации / С. А. Осмоловский. – Москва : «Радио и связь», 2003. – 320 с. – Текст : непосредственный.

54. Варакин, Л. Е. Системы связи с шумоподобными сигналами / Л. Е. Варакин. – Москва : «Радио и связь», 1985. – 384 с. – Текст : непосредственный.

55. Зачиняев, Ю. В. Формирование наносекундных ЛЧМ-радиосигналов на волоконно-оптических структурах / Ю. В. Зачиняев, К. Е. Румянцев, А. В.

Кукуяшный. – Текст : непосредственный // Электротехнические и информационные комплексы и системы. – Уфа : Уфимский государственный нефтяной технический университет, 2011. – № 3. – Том 7. – С. 32-37.

56. Spread Spectrum Satcom Hacking Attacking the Globalstar Simplex Data Service Colby Moore – URL: https://www.blackhat.com/docs/us-15/materials/us-15-Moore-Spread-Spectrum-Satcom-Hacking-Attacking-The-GlobalStar-Simplex-Data-Service.pdf (дата обращения: 26.12.2024). – Text : electronic.

57. Черняк, З. В. Математическое моделирование ансамблей дискретных ортогональных многоуровневых сигналов с требуемыми корреляционными характеристиками : диссертация ... кандидата технических наук : 05.13.18 / Черняк Захар Владимирович ; [Место защиты : Ставропольский государственный университет]. – Ставрополь, 2010. – 120 с. – Текст : непосредственный.

58. Быховский, М. А. Эффективные методы передачи сигналов в спутниковых системах связи / М. А. Быховский. – Текст : непосредственный // Цифровая обработка сигналов. – 2020. – № 2. – С. 27-33.

59. Rahman M. Study of the cyclostationarity properties of various signals of opportunity / M. Rahman. – Text : direct // Master of Science Thesis. – 2014. – 119 p.

60. Taboada Fernando L., Detection and classification of low probability of intercept radar signals using parallel filter arrays and higher order statistics / Fernando L. Taboada. – Monterey, California. Naval Postgraduate School. – 2002. – 298 p. – Text : direct.

61. Lima Antonio F. Analysis of low probability of intercept (LPI) radar signals using cyclostationary processing / Antonio F. Lima. – Monterey California. Naval Postgraduate School. – 2002. – 187 p. – Text : direct.

62. Шеннон, К. Математическая теория связи / К. Шеннон. – Текст : непосредственный // Работы по теории информации и кибернетике. – Москва : ИИЛ, 1963. – С. 243-322.

63. Шеннон, К. Теория связи в секретных системах / К. Шеннон. – Текст : электронный // Работы по теории информации и кибернетике. – Москва : ИИЛ, 1963. [По изданию: К. Шеннон «Работы по теории информации и кибернетике»,

Москва : ИЛ, 1963, С. 333-369 (перевод В. Ф. Писаренко) с корректировкой терминологии переводчика]. – URL : https://techlibrary.ru/b1/ 3g1f1o1o1p1o_2s._3a1f1p1r1j2g_1s1c2g1i1j_1c_1s1f1l1r1f1t1o2c1w_1s1j1s1t1f1n1a1 w.pdf (дата обращения 25.07.2022).

64. Финк, Л. М. Псевдостохастическое кодирование для обнаружения ошибок / Л. М. Финк, С. А. Мухаметшина. – Текст : непосредственный // Проблемы передачи информации. – 1979. – Том XV. – Выпуск 2. – С. 76-79.

65. Флейшман, Б. С. Конструктивные методы оптимального кодирования для каналов с шумами / Б. С. Флейшман. – Москва : Издательство Академии наук СССР, 1963. – 244 с. – Текст : непосредственный.

66. Ватрухин, Е. М. Новые возможности применения коротковолновой радиосвязи при решении боевой авиацией задач воздушно-космической обороны / Е. М. Ватрухин. – Текст : непосредственный // Вестник Концерна ВКО «Алмаз – Антей». – 2020. – № 4. – С. 6-14.

67. Ватрухин, Е. М. Комплексная защита информации в каналах «земля-борт» / Е. М. Ватрухин. – Текст : непосредственный // Вестник Концерна ВКО «Алмаз – Антей». 2017. – № 2. – С. 16-20.

68. Патент № 2 428 795 (13) C1 Российская Федерация, МПК H04B 7/216 H04J 13/00 H04L 9/22. Способ передачи информации на основе хаотически формируемых ансамблей дискретных многоуровневых ортогональных сигналов : № 2 428 795 (13) : заявлено 24.02.2010 : опубликовано 10.09.2011 / Жук А. П., Иванов А. С., Голубь Ю. С., Орел Д. В. // Яндекс. Патенты. – URL: https://patents.s3.yandex.net/ RU2428795C1_ 20110910.pdf (дата обращения 23.08.2023). – Текст : электронный.

69. Столингс, В. Беспроводные линии связи и сети = Wireless Communications and Networking / В.Столлингс ; [Перевод с английского А. В. Высоцкого и др.]. – Москва [и др.] : Вильямс, 2003. – 638 с. – Текст : непосредственыний.

70. National Institute of Standards and Technology Special Publication 800-22 revision 1a. Natl. Inst. Stand. Technol. Spec. Publ . 800-22rev1a, 131 pages (April 2010). – Text : direct.

71. National Institute of Standards and Technology Special Publication 800-90A Revision 1. Natl. Inst. Stand. Technol. Spec. Publ. 800-90A Rev. 1, 109 pages (June 2015). CODEN: NSPUE2. http://dx.doi.org/10.6028/NIST.SP.800-90Ar (дата обращения: 26.12.2024). – Text : electronic.

72. Жук, А. П. Анализ подходов к моделированию радиоэлектронного подавления радиосигналов спутниковых систем связи с помощью организации радиопомех / А. П. Жук, Д. В. Орел, Е. П. Жук, А. В. Студеникин. – Текст : непосредственный // Прорывные научные исследования как двигатель науки: сборник статей Международной научно-практической конференции (Магнитогорск, 4 декабря 2018 года). – Магнитогорск : МЦИИ ОМЕГА САЙНС, 2018. – № 3. – С. 45-50.

73. Жук, А. П. Способ повышения структурной скрытности спутниковой системы связи на основе стохастического использования систем двоичных квазиортогональных кодовых последовательностей в качестве расширяющих кодов / А. П. Жук, А. В. Студеникин, И. А. Калмыков. – Текст : непосредственный // Актуальные вопросы развития научных исследований: теоретический и практический взгляд : сборник статей Национальной (Всероссийской) научно-практической конференции (Тюмень, 22 декабря 2020 года). – Тюмень : МЦИИ ОМЕГА САЙНС, 2020. – № 1. – С. 38-41.

74. Жук, А. П. Проблематика радиосвязи в отдаленных районах России / А. П. Жук, А. В. Студеникин. – Текст : непосредственный // Проблемы современной системотехники : сборник научных статей. – Таганрог: ИП Ступин С. А., 2018. – № 12. – С. 3-9.

75. Студеникин, А. В. Алгоритм скрытного информационного обмена в системах передачи информации с кодовым разделением каналов на основе хаотического применения ортогональных кодовых последовательностей / А. В. Студеникин. – Текст : непосредственный // Современная наука: актуальные

проблемы теории и практики. Серия Естественные и технические науки. – 2021. – № 11. – С. 102-107. DOI: 10.37882/2223-2966.2021.11.31.

76. Студеникин, А. В. Метод защиты информации в системах связи с кодовым разделением каналов на основе хаотического применения ортогональных кодовых последовательностей / А. В. Студеникин. – Текст : непосредственный // Теория и практика обеспечения информационной безопасности : сборник научных трудов по материалам всероссийской научно-теоретической конференции (Москва, 3 декабря 2021 года). – Москва : Московский технический университет связи и информатики, 2021. – С. 303-310.

77. Жук, А. П. Алгоритм повышения структурной скрытности систем передачи информации с кодовым разделением каналов / А. П. Жук, А. В. Студеникин, А. В. Кузин, Д. А. Лебедев. – Текст : непосредственный // Радиоэлектронные устройства и системы для инфокоммуникационных технологий ("РЭУС-2022"). Доклады Всероссийской конференции (с международным участием). – Москва : Российское научно-техническое общество радиотехники, электроники и связи им. А. С. Попова, 2022. – С. 175-180.

78. Варакин, Л. Е. Теория сложных сигналов / Л. Е. Варакин. – Москва : Советское радио, 1970. – 375 с. – Текст : непосредственный.

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

80. Пашинцев, В. П. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн : монография / В. П. Пашинцев, О. П. Малофей, А. П. Жук [и др.]. – Москва : ООО Издательская фирма «ФМЛ», 2010. – 196 с. – Текст : непосредственный.

81. Сазонов, В. В. Разработка методики синтеза ансамблей дискретных ортогональных в усиленном смысле сигналов для коротковолновых систем радиосвязи / В. В. Сазонов, С. С. Манаенко. Текст : электронный // Информация и

космос. – 2017. – № 3. – С. 31-36. – URL: https://infokosmo.ru/file/ article/16553.pdf (дата обращения : 19.06.2021).

82. Гайчук, Д. В. Метод синтеза ансамблей дискретных ортогональных в усиленном смысле сигналов для радиолиний декаметрового диапазона системы : диссертация ... кандидата технических наук / Гайчук Дмитрий Викторович. – Ставрополь, 2010. – 120 с. – Текст : непосредственный.

83. Трошков, М. А. Методика синтеза помехоустойчивых ансамблей дискретных ортогональных сигналов с расширенной базой и усовершенствованным алгоритмом криптографической защиты информации для радиолиний УКВ диапазона : диссертация ... кандидата технических наук : 20.01.09 / Трошков Михаил Александрович ; [Место защиты : Ставропольское высшее военное инженерное училище связи]. – Ставрополь, 2007. – 214 с. – Текст : непосредственный.

84. Вержбицкий, В. М. Численные методы. Линейная алгебра и нелинейные уравнения : учебное пособие / В. М. Вержбицкий. – Москва : Издательский дом ОНИКС 21 век, 2005. – 432 с. – Текст : непосредственный.

85. Головина, Л. И. Линейная алгебра и некоторые ее приложения / Л. И. Головина. – Москва : Наука, 1971. – 340 с. – Текст : непосредственный.

86. Линейная алгебра : учебное пособие для студентов вуза / Н. В. Гредасова, М. А. Корешникова, Н. И. Желонкина [и др.] ; научный редактор А. Н. Сесекин ; Уральский федеральный университет им. первого президента России Б. Н. Ельцина, Уральский энергетический институт. – Екатеринбург : Издательство Уральского университета, 2019. – 88 с. – Текст : непосредственный.

87. Жук, А. П. Разработка методики повышения структурной скрытности сигналов спутниковых радионавигационных систем / А. П. Жук, Д. В. Орёл. – Текст : непосредственный // Вестник Ставропольского государственного университета. – 2010. – № 5. – С. 44-52.

88. Жук, А. П. О целесообразности использования ансамблей ортогональных сигналов с изменяющейся размерностью в системе CDMA / А. П.

Жук, З. В. Черняк, В. В. Сазонов. – Текст : непосредственный // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 190-195.

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

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

91. Zhuk A. Simulation of the Information Transmission System with Code Division of Channels with Increased Structural Stealth / Zhuk, A., Studenikin, A., Orel, D., Zhuk, E. – Text : direct // Lecture Notes in Networks and Systems, 2024, 1044 LNNS. – С. 295-304.

92. Студеникин, А. В. Моделирование дискретных ортогональных кодовых последовательностей для систем передачи информации / А. В. Студеникин, А. П. Жук. – Текст : непосредственный // Наукоемкие технологии в космических исследованиях Земли. – 2021. – № 1(27). – С. 36-43. DOI: 10.36724/2409-5419-2021-13-1-36-43.

93. Гантмахер, Ф. Р. Теория матриц / Ф. Р. Гантмахер. – 5-е издание – Москва : Физматлит, 2010. – 559 с. – Текст : непосредственный.

94. Сборник задач по линейной алгебре. Второй семестр: учебное пособие для вузов / Е. А. Ивин, Ф. Ю. Попеленский ; Московский государственный университет имени М. В. Ломоносова, Московская школа экономики, Кафедра эконометрики и математических методов экономики. – Вологда : ВолНЦ РАН, 2021. – 104 с. – Текст : непосредственный.

95. Сазонов, В. В. О влиянии коэффициентов второй диагонали эрмитовой матрицы на автокорреляционные свойства определяемых ею ортогональных в

усвоенном смысле сигналов / В. В. Сазонов. – Текст : непосредственный // Проблемы эффективности и безопасности функционирования сложных технических и информационных систем : труды XXV Межрегиональной научно-технической конференции. Сборник №4. – Серпухов 2006 – С. 200-203.

96. Студеникин, А. В. Математическое моделирование ансамблей дискретных ортогональных последовательностей / А. В. Студеникин, А. П. Жук, Е. П. Жук. – Текст : непосредственный // Инновационные векторы цифровизации экономики и образования в регионах России – 2021 : сборник материалов Всероссийской научно-практической конференции (Ставрополь, 10-11 марта 2021 года). – Ставрополь : Ставропольский государственный аграрный университет, 2021. – С. 714-717.

97. Студеникин, А. В. Программная модель синтеза увеличенных объемов систем дискретных ортогональных кодовых последовательностей / А. В. Студеникин, А. П. Жук, Е. С. Тран. – Текст : непосредственный // Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации – 2020 : сборник докладов II Всероссийской научной конференции (с приглашением зарубежных ученых) (Ставрополь, 30 ноября 2020 года). – Ставрополь : Северо-Кавказский федеральный университет, 2020. – С. 227-232.

98. Свидетельство о государственной регистрации программы для ЭВМ № 2020665609 Российская Федерация. Программа генерации стохастических ортогональных сигналов «Stochastic orthogonal signal generator (SOSG)» : № 2020664575 : заявлено 20.11.2020 : опубликовано 27.11.2020 / С. Ю. Сухоруков, А. П. Жук, Е. С. Тран, Я. В. Шуляк, Е. П. Жук, А. В. Студеникин ; правообладатель: ФГАОУ ВО «Северо-Кавказский федеральный университет». –1 с. – Текст : непосредственный.

99. Pashintsev, V. P. Malofey, O. P., Zhuk A. P. et al. Development of the theory of synthesis and methods of formation of ensembles of discrete signals for promising radio communication systems of various radio wave ranges : Monograph / Pashintsev, V. P. Malofey, O. P., Zhuk A. P. et al. – Moskow : Publishing Company «FML», 2010. – 196 p. – Text : direct.

100. Демидович, Б. П. Основы вычислительной математики / Б. П. Демидович, И. А. Марон. – Москва : Наука, 1970. – 664 с. – Текст : непосредственный.

101. Андерсон, Дж. А. Дискретная математика и комбинаторика / Джеймс А. Андерсон. – Москва : Вильямс, 2003. – 957 с. – Текст : непосредственный.

102. Жук, А. П. Оценка вычислительной сложности алгоритмов формирования систем кодовых последовательностей / А. П. Жук, Д. В. Орел, А. В. Студеникин, А. Ю. Муравьев. – Текст : непосредственный // Роль и значение науки и техники для развития современного общества : сборник статей Международной научно-практической конференции (Волгоград, 26 ноября 2018 года). – Волгоград: МЦИИ ОМЕГА САЙНС, 2018. – № 1. – С. 81-85.

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

104. Студеникин, А. В. Экспериментальное моделирование защищенного информационного обмена в системе передачи информации с кодовым разделением каналов / А. В. Студеникин, А. П. Жук. – Текст : непосредственный // Глобальные тенденции и перспективы цифровизации экономики, образования и науки – 2021 : сборник материалов международной научно-практической конференции (Ставрополь, 19–20 мая 2021 года). – Ставрополь : Ставропольский государственный аграрный университет, 2021. – С. 572-577.

105. Жук, А. П. Универсальный алгоритм формирования ансамблей псевдослучайных ортогональных кодовых последовательностей / А. П. Жук, А. В. Студеникин, Д. В. Лебедев, А. В. Кузин. – Текст : непосредственный // Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2021 : сборник научных докладов по материалам Всероссийской конференции (Москва, 02-04 июня 2021 года). – Москва : РНТОРЭС имени А.С. Попова, 2021. – № LXXVI. – С. 108-113.

106. Студеникин, А. В. Моделирование системы передачи информации с кодовым разделением каналов на основе хаотического применения ортогональных кодовых последовательностей / А. В. Студеникин. – Текст : непосредственный // Проблемы передачи информации в инфокоммуникационных системах: сборник докладов и тезисов XI Всероссийской научно-практической конференции (Волгоград, 28 мая 2021 года). – Волгоград : Издательство ВолГУ, 2021. – С. 98-101.

107. Жук, А. П. Универсальный формирователь дискретных ортогональных последовательностей / А. П. Жук, А. В. Студеникин, Е. П. Жук. – Текст : непосредственный // Радиоэлектронные устройства и системы для инфокоммуникационных технологий – РЭУС-2020 – 2020 : сборник трудов конференции (Ставрополь, 27-29 мая 2020 года). – Москва : Российское научно-техническое общество радиотехники, электроники и связи им. А. С. Попова, 2020. – С. 46-48.

108. Жук, А. П. Формирователь дискретных ортогональных последовательностей для стохастического использования / А. П. Жук, А. В. Студеникин, А. В. Суханов, А. А. Жарнов. – Текст : непосредственный. // Проблемы эффективности и безопасности функционирования сложных технических и информационных систем : сборник трудов XLI Всероссийской научно-технической конференции (Серпухов, 23-24 июня 2022 года). – Серпухов : филиал ВА РВСН, 2022. – С. 131-135.

109. Свидетельство о государственной регистрации программы для ЭВМ № 2021661193 Российская Федерация. Генератор стохастических ортогональных кодовых последовательностей : № 2021619557 : заявлено 21.06.2021 : опубликовано 07.07.2021 / А. П. Жук, Е. С. Тран, А. В. Студеникин, Я. В. Шуляк, А. А. Апурин ; правообладатель: ФГАОУ ВО «Северо-Кавказский федеральный университет» – 1 с. – Текст : непосредственный.

110. Патент № 2 780 418 C1 Российская Федерация. МПК H04B 7/216 / Система передачи информации с применением стохастических ортогональных кодов : № 2 021 129 144 : заявлено 06.10.2021 : опубликовано 22.09.2022 / Жук А.

П., Степанян Н. Э., Студеникин А. В., и др.; заявитель и патентообладатель ФГАОУ ВО «Северо-Кавказский федеральный университет». – 39 с. – Текст : непосредственный.

111. Патент № 2 773 107 C1 Российская Федерация. МПК G06F 1/02, G06F 7/58 Устройство формирования стохастических ортогональных кодов : № 2021117997 : заявлено 21.06.2021 : опубликовано 30.05.2022 / Жук А. П., Степанян Н. Э., Студеникин А. В., и др.; заявитель и патентообладатель ФГАОУ ВО «Северо-Кавказский федеральный университет». – 50 с. – Текст : непосредственный.

112. Патент № 2 106 31 U1 Российская Федерация. МПК H03M 13/43 Модифицированное устройство коррекции ошибок с расширенным набором решающих правил и учетом адаптивного сигнала стирания : № 2021133067 : заявлено 25.02.2021 : опубликовано 22.04.2022 / Малофей О. П., Жук А. П., Студеникин А. В., и др.; заявитель и патентообладатель ФГАОУ ВО «Северо-Кавказский федеральный университет». – 24 с. – Текст : непосредственный.

113. Свидетельство о государственной регистрации программы для ЭВМ № 2023682120. Российская Федерация. Модель системы передачи информации с кодовым разделением каналов на основе псевдослучайного применения ортогональных кодовых последовательностей : № 2023681642/69 : заявлено 20.10.2023 : опубликовано 23.10.2023 / И. В. Макаров, А. П. Жук, А. В. Студеникин; правообладатель: ФГАОУ ВО «Северо-Кавказский федеральный университет». – 1 с. – Текст : непосредственный.

114. Патент № 2 801 172 C1 Российская Федерация. МПК H04B 7/216, H04J 11/00, H04L 9/26, H04L 27/26 Система непрерывной передачи информации ансамблями стохастических ортогональных кодов : № 2022132306 : заявлено 09.12.2022 : опубликовано 02.08.2023 / Жук А. П., Степанян Н. Э., Студеникин А. В., и др.; заявитель и патентообладатель ФГАОУ ВО «Северо-Кавказский федеральный университет». – 33 с. – Текст : непосредственный.

115. Патент № 2 787 561 C1 Российская Федерация. МПК G06F 1/102, H04J 13/12 Формирователь ансамблей стохастических ортогональных кодов с отсутствующей временной задержкой : № 2022111972 : заявлено 04.05.2022 :

опубликовано 10.01.2023 / Жук А. П., Степанян Н. Э., Студеникин А. В., и др. ; заявитель и патентообладатель ФГАОУ ВО «Северо-Кавказский федеральный университет». – 12 с. – Текст : непосредственный.

116. Жук, А. П. Оценка структурной скрытности ансамблей многофазных ортогональных кодовых последовательностей / А. П. Жук, А. В. Студеникин, И. В. Макаров, А. А. Беседин. – Текст : непосредственный // Телекоммуникации. – 2024. – № 3. – С. 13-21. DOI: 10.31044/1684-2588-2024-0-3-13-21.

117. Основы теории скрытности : учебное пособие / З. М. Каневский, В. П. Литвиненко, Г. В. Макаров, Д. А. Максимов; [под редакцией З. М. Каневского], Воронежский государственный технический университет. – Воронеж : ГОУ ВПО «Воронежский государственный технический университет», 2006. – 202 с. – Текст : непосредственный.

118. Литюк, В. И. Методы цифровой многопроцессорной обработки ансамблей радиосигналов / В. И. Литюк, Л. В. Литюк. – Москва : Солон-Пресс, 2007. – 592 с. – Текст : непосредственный.

119. Иванов, М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. Книга 2 / М. А. Иванов, И. В. Чугунков. – Москва : КУДИЦ-ОБРАЗ, 2003, – 240 с. – Текст : непосредственный.

120. Защита информации. Основные термины и определения = Protection of information. Basic terms and definitions : Protection of information. Basic terms and definitions : национальный стандарт Российской Федерации ГОСТ Р 50922-2006 : взамен ГОСТ Р 50922-96 : введен 2008-02-01 / Федеральное агентство по техническому регулированию и метрологии. – Москва : Стандартинформ, 2008. – IV, 7 с. – Текст : непосредственный.

121. Патент № 2 740 339 C1 Российская Федерация. МПК G06F 7/58. Генератор псевдослучайных чисел : № 2020109726 : заявлено 05.03.2020 : опубликовано 13.01.2021 / Иванов М. А., Саликов Е. А. ; заявитель и патентообладатель ФГАОУ ВО «Национальный исследовательский ядерный университет МИФИ». – 13 с. – Текст : непосредственный.

122. Патент № 2 774 812 C1 Российская Федерация. МПК G06F 7/58. Устройство для генерации псевдослучайных чисел : № 2021120046 : заявлено 08.07.2021 : опубликовано 23.06.2022 / Козлов А. А., Иванов М. А. ; заявитель и патентообладатель ФГАОУ ВО «Национальный исследовательский ядерный университет МИФИ». – 10 с. – Текст : непосредственный.

123. Патент № 2 776 346 C1 Российская Федерация. МПК G06F 7/58. Генератор псевдослучайных чисел : № 2021120045 : заявлено 08.07.2021 : опубликовано 19.07.2022 / Иванов М. А., Саликов Е. А., Козлов А. А. и др. ; заявитель и патентообладатель ФГАОУ ВО «Национальный исследовательский ядерный университет МИФИ». – 15 с. – Текст : непосредственный.

124. Патент № 2 800 190 C1 Российская Федерация. МПК G06F 7/58. Устройство формирования псевдослучайных комплексных чисел : № 2022126403 : заявлено 10.10.2022 : опубликовано 19.07.2023 / Апруда А. В., Самойленко Д. В., Диченко С. А. и др.; заявитель и патентообладатель ФГКОУ ВО «Краснодарское военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко». – 17 с. – Текст : непосредственный.

125. Патент на полезную модель № 108167 U1 Российская Федерация. МПК G06F 12/14, G06F 13/12. Портативный накопитель информации с функцией защиты данных от несанкционированного доступа : № 2011124344/08 : заявлено 06.06.2011 : опубликовано 10.09.2011 / Котляревский В. В., Цапура Е. Е.; заявитель и патентообладатель Общество с ограниченной ответственностью «Рантех». – 3 с. – Текст : непосредственный.

126. Патент на полезную модель № 184681 U1 Российская Федерация. МПК G06F 12/08. Устройство хранения данных : № 2018114139 : заявлено 18.04.2018 : опубликовано 02.11.2018 / Людвиг В. А., Васькин А. А.; заявитель и патентообладатель Общество с ограниченной ответственностью «Булат». – 9 с. – Текст : непосредственный.

127. Патент № 2 017 241 C1 Российская Федерация. МПК G11C 11/00. Запоминающее устройство : № 404353124 : заявлено 10.06.1991 : опубликовано

30.07.1994 / Берсон Ю. Я., Марголин Е. Я.; заявитель и патентообладатель ЦНИИ «Гранит». – 13 с. – Текст : непосредственный.

128. Патент № 2 790 533 C1 Российская Федерация. МПК G06F 12/08, G06F 3/06, H03M 7/30. Устройство обработки и хранения данных : № 2022124458 : заявлено 15.09.2022 : опубликовано 22.02.2023 / Анохин Д. В., Измайлов Д. А., Семилетов А. Д. и др.; заявитель и патентообладатель АО НПЦ «Электронные вычислительно-информационные системы». – 13 с. – Текст : непосредственный.

129. Патент № 2 359 405 C2 Российская Федерация. МПК H04B 1/00. Способ формирования наборов ортогональных псевдослучайных последовательностей с использованием свойств фрактальных отображений : № 2006143688/09 : заявлено 10.06.2008 : опубликовано 20.06.2009 / Сахно И. В., Симонов А. Б., Ткачев Е. А. ; заявитель и патентообладатель Сахно И. В., Симонов А. Б., Ткачев Е. А. – 10 с. – Текст : непосредственный.

130. Патент № 2 615 322 C1 Российская Федерация. МПК G06F 1/02, G06F 7/58. Генератор стохастических ортогональных кодов : № 2016110664 : заявлено 22.03.2016 : опубликовано 04.04.2017 / Жук А. П., Петренко В. И., Осипов Д. Л. и др. ; заявитель и патентообладатель ФГАОУ ВО «Северо-Кавказский федеральный университет». – 3 с. – Текст : непосредственный.

131. Сергиенко, А. Б. Цифровая обработка сигналов : учебное пособие / А. Б. Сергиенко. – 3-е издание. – Санкт-Петербург : БХВ-Петербург, 2011. – 756 с. – Текст : непосредственный.

132. Черноусов, А. В. Имитостойкость спутниковых систем связи на основе W ШПС / А. В. Черноусов, А. В. Кузовников, В. Г. Сомов. – Текст : непосредственный // Решетневские чтения. Том 1. – 2012. – С. 165-166.

133. Воронов, Д. Н. Критерии оценки имитостойкости командно-телеметрических радиолиний / Д. Н. Воронов. – Текст : непосредственный // Системы обработки информации. – 2007. – Выпуск 4 (62). – С. 14-16.

134. Globalstar : сайт компании [Электронный ресурс]. – URL: https://global-star.ru/sms.html (дата обращения: 04.05.2022).

135. Globalstar-ZORA CO, LTD Морские радио и навигационные системы : сайт компании [Электронный ресурс]. – URL: https://zora.ru/?page_id=380.html (дата обращения: 04.05.2022).

136. Махов, Д. С. Анализ некриптографических методов защиты информации в радиоканалах информационных систем / Д. С. Махов. – Текст : электронный // Вопросы кибербезопасности. – 2024. – № 1(59). – С. 82-88. DOI: 10.21681/2311-3456-2024-1-82-88.

137. Толковый словарь живого великорусского языка Владимира Даля : в 4 томах. Том 1. А-З / В. И. Даль ; под редакцией И. А. Бодуэна-Де-Куртенэ. – 3-е издание, исправленное и значительно дополненное. – Санкт-Петербург ; Москва : Товарищество М. О. Вольфъ, 1903. – XI с., 1744 стб., VI с. – Текст : непосредственный.

138. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: "Триумф", 2002 – 816 с.: ил.

139. Мао Венбо. Современная криптография: теория и практика. : Пер. с англ. – М. : Издательский дом "Вильямс", 2005. – 768 с. : ил.

140. Джу, А. В. Исследование зависимостей между диагональными коэффициентами Эрмитовых матриц и свойсвами их собственных векторов / А. В. Джу, И. В. Макаров, А. А. Беседин // Студенческая наука - для развития информационного общества : Сборник научных трудов по материалам XIV Всероссийской научно-технической конференции, Ставрополь, 18 мая 2023 года. – Ставрополь: Северо-Кавказский федеральный университет, 2023. – С. 117-120.

141. Помехозащищенность радиосистем со сложными сигналами. / Г.И. Тузов, В.А Сивов, В.И. Прытков и др.; Под ред. Г.И. Тузова. – М.: Радио и связь, 1985. – 264 с.

142. Рекомендация МСЭ-R M.1850 (01/2010). Подробные спецификации радиоинтерфейсов для спутниковой компоненты Международной подвижной электросвязи (IMT-2000).

143. Магазинников Л. И. Высшая математика III. Функции комплексного переменного. Ряды. Интегральные преобразования. — Томск: Томский

государственный университет систем управления и радиоэлектроники, 2012. — 206 с.

144. Осмоловский С. А. Стохастическая информатика: инновации в информационных системах / С.А. Осмоловский. - Москва : Горячая Линия–Телеком, 2012. - 320 с.

145. Микушин, А. В. Схемотехника современных телекоммуникационных устройств : Учебное пособие в 2 частях / А. В. Микушин. Том Часть 1. – Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2022. – 136 с.

ОСНОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

3GPP – 3rd Generation Partnership Project.

CDMA – Code Division Multiple Access, кодовый многостанционный доступ.

CDMA-DS – доступ с кодовым разделением каналов и прямым расширением спектра.

DS – direct-sequence, функция расширения спектра прямой последовательностью

DVB-T – наземное цифровое видеовещание.

IMT-2000 – International Mobile Telecommunications-2000, Международная подвижная электросвязь.

FDMA – Frequency Division Multiple Access, частотный многостанционный доступ.

FCC – Федеральная комиссия по связи.

GEO – геостационарная орбита.

GNSS – Global Navigation Satellite System, Глобальная навигационная спутниковая система.

HAPS – High-Altitude Platform Station, Высотные платформенные системы.

HEO – негеостационарная эллиптическая орбита.

LEO – негеостационарная низковысотная орбита.

MC-CDMA – множественный доступ с кодовым разделением с несколькими несущими.

MEO – негеостационарная средневысотная орбита.

NCC – Network Control Center Центр управления сетью.

NMC – центр управления сетью Network Management Center.

OFDM – мультиплексирование с ортогональным частотным разделением.

OVSF – Orthogonal Variable Spreading Factor.

QAM – Quadrature Amplitude Modulation.

QPSK – Quadrature phase shift keying, квадратурная фазовая манипуляция.

SDMA – пространственный многостанционный доступ, space-division multiple access.

TDMA – Time Division Multiple Access, временной многостанционный доступ.

TT&C – данные телеуправления-телесигнализации.

АДОМУС – ансамбли дискретных ортогональных многоуровневых сигналов.

АДОП – ансамбли дискретных ортогональных последовательностей

АДОС – ансамбли дискретных ортогональных сигналов.

АМФОКП – ансамбли многофазных ортогональных кодовых последовательностей.

АОКП – ансамбли ортогональных кодовых последовательностей.

БЛА – беспилотный летательный аппарат.

БН – блок накопителя.

БОПГС – блок обратного преобразования группового сигнала.

ВКФ – взаимокорреляционная функция.

ГПСКЧ – генератор псевдослучайных комплексных чисел.

ГФПТ – генератор функций Попенко – Турко.

ДИЗ – двоичное измерение.

ЕКА – Европейское космическое агентство.

КРК – кодовое разделение каналов.

ЛОС – линейная обратная связь.

ЛЧМ – линейная частотная модуляция.

МК – микроконтроллер.

МСЭ – Международный союз электросвязи.

МСЭ-R М.1850 – Подвижная спутниковая служба, спутниковая служба радиоопределения, любительская спутниковая служба и относящиеся к ним спутниковые службы.

ОЗУ – оперативное запоминающее устройство.

ПСКЧ – псевдослучайное комплексное число.

ПСП – псевдослучайная последовательность.

ПСХП – псевдослучайные хаотические последовательности.

РЭБ – радиоэлектронная борьба.

СВ – собственный вектор.

СПИ – система передачи информации.

ССС – система спутниковой связи.

ШПС – широкополосный сигнал.

ЭМ – эрмитова матрица.

ПРИЛОЖЕНИЕ А

Программы синтеза ансамблей многофазных ортогональных кодовых последовательностей на основе собственных векторов эрмитовых матриц

Программа синтеза АМФОКП на основе СВ ЭМ четвертого порядка

```
clc;
clear;
rng('shuffle', 'simdTwister');
S=rand(1,10)+1i*rand(1,10);

A=zeros(4);
A(1,1)=real(S(1));
A(1,2)=S(2);
A(1,3)=S(3);
A(1,4)=S(4);
A(2,1)=conj(S(2));
A(2,2)=real(S(5));
A(2,3)=S(6);
A(2,4)=S(7);
A(3,1)=conj(S(3));
A(3,2)=conj(S(6));
A(3,3)=real(S(8));
A(3,4)=S(9);
A(4,1)=conj(S(4));
A(4,2)=conj(S(7));
A(4,3)=conj(S(9));
A(4,4)=real(S(10));

[V, N]=eig(A);

A
V=V'
```

Программа синтеза АМФОКП на основе СВ ЭМ 128-го порядка

```
% Количество значений в диагонали матрицы определяется произвольно
(сколько
% будет введено, исходя из этого определится порядком матрицы n)
S = [100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
    0.0001;
```

```
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.000001+10i;
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.0001;
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;];
      % Углы в исходной строке S
      S_angle = rad2deg (angle(S));
      % Порядок матрицы собственных векторов
      n = length(S) + 1;
      % Строим матрицу нулей размера (n; n)
      A = zeros(n);
      % Заполняем коэффициенты матрицы над главной диагональю
      for j = 1:n-1
          v = complex(zeros(1,n));
          v(j+1) = S(j);
          A(j,:) = v;
      end
      % Делаем матрицу комплексно-сопряженной
      A = A + ctranspose(A);
      % Вычисляем матрицу собственных векторов сохраняя их в переменную
eigen_vectors
      [eigen_vectors, ~]=eig(A);
      % Функция перевода комплексной матрицы собственных векторов в матрицу
углов
      % в градусах
      angles_deg = rad2deg(angle(eigen_vectors));
      writematrix(round(angles_deg), '128.csv', "Delimiter", ';');
      % Построение графического изображения матрицы собственных векторов
      imagesc(angles_deg);
      colorbar;
```

Программа синтеза АМФОКП на основе СВ ЭМ 256-го порядка

```
      % Количество значений в диагонали матрицы определяется произвольно
(сколько
      % будет введено, исходя из этого определится порядком матрицы n)
      S = [100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.0001;
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.000001;
```

```
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.0001;
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.00000001+10i;
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.0001;
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.000001;
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;
          0.0001;
          100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05; 100;
1; 100; 0.0001; 100; 1; 100; 0.05; 100; 1; 100; 0.0025; 100; 1; 100; 0.05;
100; 1; 100;];
     % Углы в исходной строке S
     S_angle = rad2deg (angle(S));
     % Порядок матрицы собственных векторов
     n = length(S) + 1;
     % Строим матрицу нулей размера (n; n)
     A = zeros(n);
     % Заполняем коэффициенты матрицы над главной диагональю
     for j = 1:n-1
         v = complex(zeros(1,n));
         v(j+1) = S(j);
         A(j,:) = v;
     end
     % Делаем матрицу комплексно-сопряженной
     A = A + ctranspose(A);
     % Вычисляем матрицу собственных векторов сохраняя их в переменную
eigen_vectors
     [eigen_vectors, ~]=eig(A);
     % Функция перевода комплексной матрицы собственных векторов в матрицу
углов
     % в градусах
     angles_deg = rad2deg(angle(eigen_vectors));
     writematrix(round(angles_deg), '256.csv', "Delimiter", ';');
     % Построение графического изображения матрицы собственных векторов
     imagesc(angles_deg);
     colorbar;
```

ПРИЛОЖЕНИЕ Б

Эксперименты по решению задач синтеза ансамблей многофазных ортогональных кодовых последовательностей размерности $N = 4$

Рассмотрим примеры решения задач синтеза ансамблей многофазных ортогональных кодовых последовательностей размерности $N = 4$ на основе рассмотрения собственных векторов бидиагональных эрмитовых матриц.

Задача 1

Дано:

1. Бидиагональная эрмитова матрица четвертого порядка $N = 4$.
2. Модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения $a_{1,2} = 100;\ a_{2,3} = 0.01;\ a_{3,4} = 100$.
3. Диагональные коэффициенты эрмитовой матрицы третьей и четвертой диагонали равны нулю.
4. Коэффициенты главной диагонали равны нулю $d_{1,1} = 0; d_{2,2} = 0;\ d_{3,3} = 0;\ d_{4,4} = 0$.
5. Аргументы диагональных коэффициентов второй диагонали $a_{2,3}$ и $a_{3,4}$ имеют фиксированное значений $\varphi_{2,3} = \varphi_{3,4} = 0°$.
6. Аргументы коэффициента $a_{1,2}$ второй диагонали имеют следующий набор значений $\varphi_{1,2} = 0°, 45°, 90°, 135°, 180°, 225°, 270°, 315°$.

Найти:

Матрицы собственных векторов V, удовлетворяющих условию задачи 1.

Решение 1.1

Данное решение представим для случая, когда аргумент коэффициента $a_{1,2}$ второй диагонали имеют следующее значение $\varphi_{1,2} = 0°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2 = 0{,}01e^{i0°} = 0{,}01;$

$a_{3,4} = S_3 = 100e^{i0°} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.5 & -0.5 & 0.5 & -0.5 \\ 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & -0.5 \\ 0.5 & 0.5 & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.1)}$$

Представим матрицу собственных векторов (Б.1) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{i0^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i0^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.2)}$$

Для наглядности изобразим ортогональные последовательности (Б.2) во временной области на рисунке Б.1.

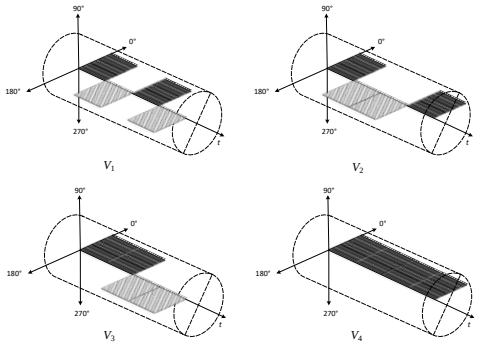


Рисунок Б.1 – Представление ортогональных последовательностей (Б.2) во временной области

Решение 1.2

Данное решение представим для случая, когда аргумент коэффициента $a_{1,2}$ второй диагонали имеют следующее значение $\varphi_{1,2} = 45°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i45^\circ} = 70.711 + 70.711\text{i}$;

$a_{2,3} = S_2$=0,01$e^{i0^\circ} = 0{,}01$;

$a_{3,4} = S_3$=$100e^{i0^\circ} = 100$.

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.36 + 0.36\text{i} & 0.51 & -0.48 & 0.48 \\ -0.34 + 0.34\text{i} & 0.48 & 0.51 & -0.51 \\ -0.34 + 0.34\text{i} & -0.48 & 0.51 & 0.51 \\ -0.36 + 0.36\text{i} & -0.51 & -0.48 & -0.48 \end{bmatrix}. \quad \text{(Б.3)}$$

Представим матрицу собственных векторов (Б.3) в показательной форме

$$V = \begin{bmatrix} 0.51e^{-i45^\circ} & 0.51e^{i180^\circ} & 0.49e^{i0^\circ} & 0.49e^{i180^\circ} \\ 0.49e^{-i45^\circ} & 0.49e^{i180^\circ} & 0.51e^{i180^\circ} & 0.51e^{i0^\circ} \\ 0.49e^{-i45^\circ} & 0.49e^{i0^\circ} & 0.51e^{i180^\circ} & 0.51e^{i180^\circ} \\ 0.51e^{-i45^\circ} & 0.51e^{i0^\circ} & 0.49e^{i0^\circ} & 0.49e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.4)}$$

Для наглядности изобразим ортогональные последовательности (Б.4) во временной области на рисунке Б.2.

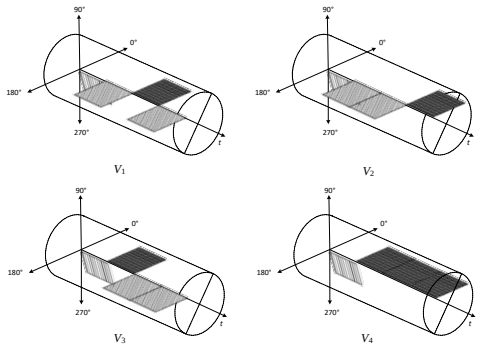


Рисунок Б.2 - Представление ортогональных последовательностей (Б.4) во временной области

Решение 1.3

Данное решение представим для случая, когда аргумент коэффициента $a_{1,2}$ второй диагонали имеют следующее значение $\varphi_{1,2} = 90°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i90^\circ} = 100i$;

$a_{2,3} = S_2$=0,01$e^{i0^\circ} = 0{,}01$;

$a_{3,4} = S_3$=100$e^{i0^\circ} = 100$.

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.5\mathrm{i} & -0.5 & 0.5 & -0.5 \\ -0.5\mathrm{i} & -0.5 & -0.5 & 0.5 \\ -0.5\mathrm{i} & 0.5 & -0.5 & -0.5 \\ -0.5\mathrm{i} & 0.5 & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.5)}$$

Представим матрицу собственных векторов (Б.5) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i90^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i90^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{-i90^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i90^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.6)}$$

Для наглядности изобразим ортогональные последовательности (Б.6) во временной области на рисунке Б.3.

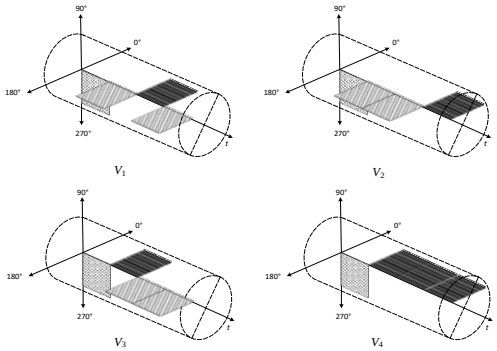


Рисунок Б.3 - Представление ортогональных последовательностей (Б.6) во временной области

Решение 1.4

Данное решение представим для случая, когда аргумент коэффициента $a_{1,2}$ второй диагонали имеют следующее значение $\varphi_{1,2} = 135°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i135^\circ} = -70{,}711 + 70{,}711i;$

$a_{2,3} = S_2 = 0{,}01e^{i0^\circ} = 0{,}01;$

$a_{3,4} = S_3 = 100e^{i0^\circ} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.36 - 0.36\mathrm{i} & -0.5 & 0.5 & -0.5 \\ -0.34 - 0.34\mathrm{i} & -0.5 & -0.5 & 0.5 \\ -0.34 - 0.34\mathrm{i} & 0.5 & -0.5 & -0.5 \\ -0.36 - 0.36\mathrm{i} & 0.5 & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.7)}$$

Представим матрицу собственных векторов (Б.7) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i135^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i135^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{-i135^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i135^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.8)}$$

Для наглядности изобразим ортогональные последовательности (Б.8) во временной области на рисунке Б.4.

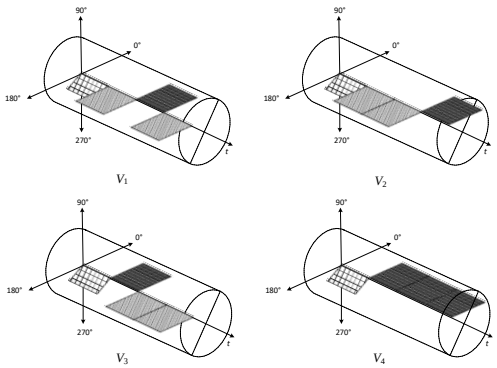


Рисунок Б.4 - Представление ортогональных последовательностей (Б.8) во временной области

Решение 1.5

Данное решение представим для случая, когда аргумент коэффициента $a_{1,2}$ второй диагонали имеют следующее значение $\varphi_{1,2} = 180°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i180°} = -100;$

$a_{2,3} = S_2$=$0{,}01e^{i0°} = 0{,}01;$

$a_{3,4} = S_3$=$100e^{i0°} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.5 & -0.5 & 0.5 & -0.5 \\ -0.5 & -0.5 & -0.5 & 0.5 \\ -0.5 & 0.5 & -0.5 & -0.5 \\ -0.5 & 0.5 & 0.5 & 0.5 \end{bmatrix}. \quad (Б.9)$$

Представим матрицу собственных векторов (Б.9) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i180°} & 0.5e^{i180°} & 0.5e^{i0°} & 0.5e^{i180°} \\ 0.5e^{i180°} & 0.5e^{i180°} & 0.5e^{i180°} & 0.5e^{i0°} \\ 0.5e^{i180°} & 0.5e^{i0°} & 0.5e^{i180°} & 0.5e^{i180°} \\ 0.5e^{i180°} & 0.5e^{i0°} & 0.5e^{i0°} & 0.5e^{i0°} \end{bmatrix}. \quad (Б.10)$$

Для наглядности изобразим ортогональные последовательности (Б.10) во временной области на рисунке Б.5.

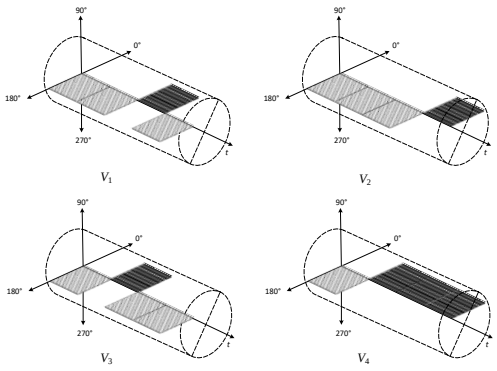


Рисунок Б.5 - Представление ортогональных последовательностей (Б.10) во временной области

Решение 1.6

Данное решение представим для случая, когда аргумент коэффициента $a_{1,2}$ второй диагонали имеют следующее значение $\varphi_{1,2} = 225°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i225°} = -70{,}711 - 70{,}711i$;

$a_{2,3} = S_2 = 0{,}01e^{i0°} = 0{,}01$;

$a_{3,4} = S_3 = 100e^{i0°} = 100$.

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.36 + 0.36\text{i} & -0.5 & 0.5 & -0.5 \\ -0.34 + 0.34\text{i} & -0.5 & -0.5 & 0.5 \\ -0.34 + 0.34\text{i} & 0.5 & -0.5 & -0.5 \\ -0.36 + 0.36\text{i} & 0.5 & 0.5 & 0.5 \end{bmatrix}. \quad (Б.11)$$

Представим матрицу собственных векторов (Б.11) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i225°} & 0.5e^{i180°} & 0.5e^{i0°} & 0.5e^{i180°} \\ 0.5e^{-i225°} & 0.5e^{i180°} & 0.5e^{i180°} & 0.5e^{i0°} \\ 0.5e^{-i225°} & 0.5e^{i0°} & 0.5e^{i180°} & 0.5e^{i180°} \\ 0.5e^{-i225°} & 0.5e^{i0°} & 0.5e^{i0°} & 0.5e^{i0°} \end{bmatrix}. \quad (Б.12)$$

Для наглядности изобразим ортогональные последовательности (Б.12) во временной области на рисунке Б.6.

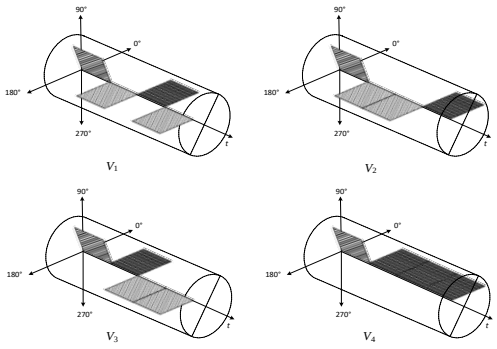


Рисунок Б.6 - Представление ортогональных последовательностей (Б.12) во временной области

Решение 1.7

Данное решение представим для случая, когда аргумент коэффициента $a_{1,2}$ второй диагонали имеют следующее значение $\varphi_{1,2} = 270°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i270°} = -100i$;

$a_{2,3} = S_2$=0,01$e^{i0°} = 0{,}01$;

$a_{3,4} = S_3$=$100e^{i0°} = 100$.

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.5\text{i} & -0.5 & 0.5 & -0.5 \\ 0.5\text{i} & -0.5 & -0.5 & 0.5 \\ 0.5\text{i} & 0.5 & -0.5 & -0.5 \\ 0.5\text{i} & 0.5 & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.13)}$$

Представим матрицу собственных векторов (Б.13) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i270°} & 0.5e^{i180°} & 0.5e^{i0°} & 0.5e^{i180°} \\ 0.5e^{-i270°} & 0.5e^{i180°} & 0.5e^{i180°} & 0.5e^{i0°} \\ 0.5e^{-i270°} & 0.5e^{i0°} & 0.5e^{i180°} & 0.5e^{i180°} \\ 0.5e^{-i270°} & 0.5e^{i0°} & 0.5e^{i0°} & 0.5e^{i0°} \end{bmatrix}. \quad \text{(Б.14)}$$

Для наглядности изобразим ортогональные последовательности (Б.14) во временной области на рисунке Б.7.

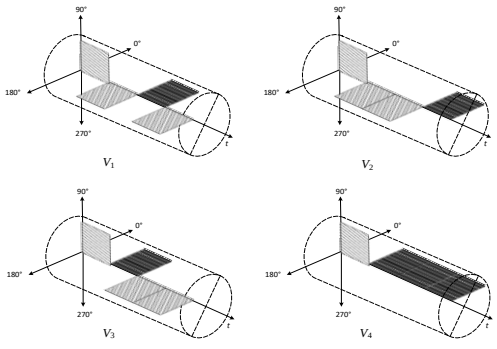


Рисунок Б.7 - Представление ортогональных последовательностей (Б.14) во временной области

Решение 1.8

Данное решение представим для случая, когда аргумент коэффициента $a_{1,2}$ второй диагонали имеют следующее значение $\varphi_{1,2} = 315°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i315°} = 70.711 - 70.711i$;

$a_{2,3} = S_2$=0,01$e^{i0°} = 0{,}01$;

$a_{3,4} = S_3$=$100e^{i0°} = 100$.

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.36 + 0.36\text{i} & -0.5 & 0.5 & -0.5 \\ 0.34 + 0.34\text{i} & -0.5 & -0.5 & 0.5 \\ 0.34 + 0.34\text{i} & 0.5 & -0.5 & -0.5 \\ 0.36 + 0.36\text{i} & 0.5 & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.15)}$$

Представим матрицу собственных векторов (Б.15) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i315°} & 0.5e^{i180°} & 0.5e^{i0°} & 0.5e^{i180°} \\ 0.5e^{-i315°} & 0.5e^{i180°} & 0.5e^{i180°} & 0.5e^{i0°} \\ 0.5e^{-i315°} & 0.5e^{i0°} & 0.5e^{i180°} & 0.5e^{i180°} \\ 0.5e^{-i315°} & 0.5e^{i0°} & 0.5e^{i0°} & 0.5e^{i0°} \end{bmatrix}. \quad \text{(Б.16)}$$

Для наглядности изобразим ортогональные последовательности (Б.16) во временной области на рисунке Б.8.

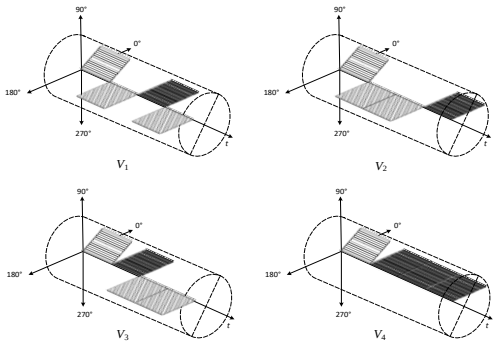


Рисунок Б.8 - Представление ортогональных последовательностей (Б.16) во временной области

Вывод по задаче 1:

Из результатов экспериментальных расчетов собственных векторов эрмитовых бидиагональных матриц четвертого порядка, имеющих фиксированные значения модулей всех диагональных коэффициентов $a_{1,2}, a_{2,3}, a_{3,4}$, а также фиксированное значение фаз (аргументов) диагональных коэффициентов $a_{2,3} = 0°$ и $a_{3,4} = 0°$, установлено, что изменение фазы (аргумента) у диагонального коэффициента $a_{1,2}$ эрмитовой бидиагональной матрицы на угол $\varphi_{1,2}$, изменяющийся в диапазоне от 0° до 360° $\varphi_{1,2}$ =0°…360° приводит к изменению фаз (аргументов) первых координат системы собственных векторов получаемой при этом эрмитовой матрицы на такой же угол, но с противоположным знаком, т.е. $-\varphi_{1,2}$.

Задача 2

Дано:

1. Бидиагональная эрмитова матрица четвертого порядка $N = 4$.
2. Модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения $a_{1,2} = 100;\ a_{2,3} = 0.01;\ a_{3,4} = 100$.
3. Диагональные коэффициенты эрмитовой матрицы третьей и четвертой диагонали равны нулю.
4. Коэффициенты главной диагонали равны нулю $d_{1,1} = 0; d_{2,2} = 0;\ d_{3,3} = 0;\ d_{4,4} = 0$.
5. Аргументы диагональных коэффициентов второй диагонали $a_{1,2}$ и $a_{3,4}$ имеют фиксированное значение $\varphi_{1,2} = \varphi_{3,4} = 0°$.
6. Аргументы коэффициента $a_{2,3}$ второй диагонали имеют следующий набор значений $\varphi_{2,3} = 0°, 45°, 90°, 135°, 180°, 225°, 270°, 315°$.

Найти:

Матрицы собственных векторов V, удовлетворяющих условию задачи 2.

Решение 2.1

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют следующее значение $\varphi_{2,3} = 0°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0^\circ} = 100;$

$a_{2,3} = S_2$=0,01$e^{i0^\circ} = 0{,}01;$

$a_{3,4} = S_3$=100$e^{i0^\circ} = 100.$

Данное решение совпадает с решением 1.1, поэтому его подробно описывать не будем.

Решение 2.2

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют значение $\varphi_{2,3} = 45^\circ$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0^\circ} = 100;$

$a_{2,3} = S_2$=0,01$e^{i45^\circ} = 0{,}01 + 0{,}01\text{i};$

$a_{3,4} = S_3$=100$e^{i0^\circ} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.35 + 0.35\text{i} & 0.35 - 0.35\text{i} & -0.5 & 0.5 \\ -0.35 + 0.35\text{i} & 0.35 - 0.35\text{i} & 0.5 & -0.5 \\ 0.35 - 0.35\text{i} & 0.35 - 0.35\text{i} & -0.5 & -0.5 \\ 0.35 - 0.35\text{i} & 0.35 - 0.35\text{i} & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.17)}$$

Представим матрицу собственных векторов (Б.17) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i135^\circ} & 0.5e^{-i45^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i135^\circ} & 0.5e^{-i45^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{-i45^\circ} & 0.5e^{-i45^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i45^\circ} & 0.5e^{-i45^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.18)}$$

Для наглядности изобразим ортогональные последовательности (Б.18) во временной области на рисунке Б.9.

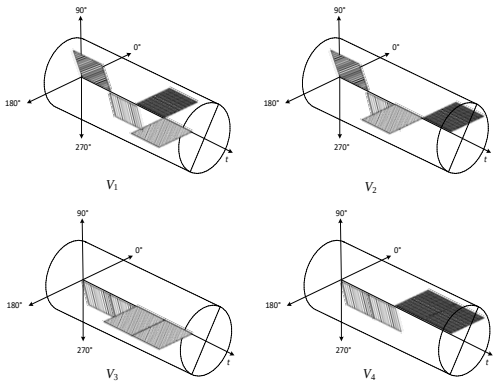


Рисунок Б.9 - Представление ортогональных последовательностей (Б.18) во временной области

Решение 2.3

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют значение $\varphi_{2,3} = 90°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=$0{,}01e^{i90°} = 0{,}01\text{i};$

$a_{3,4} = S_3$=$100e^{i0°} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.5\text{i} & -0.5\text{i} & -0.5 & 0.5 \\ 0.5\text{i} & -0.5\text{i} & 0.5 & -0.5 \\ -0.5\text{i} & -0.5\text{i} & -0.5 & -0.5 \\ -0.5\text{i} & -0.5\text{i} & 0.5 & 0.5 \end{bmatrix}. \quad (Б.19)$$

Представим матрицу собственных векторов (Б.19) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i90°} & 0.5e^{-i90°} & 0.5e^{i180°} & 0.5e^{i0°} \\ 0.5e^{i90°} & 0.5e^{-i90°} & 0.5e^{i0°} & 0.5e^{i180°} \\ 0.5e^{-i90°} & 0.5e^{-i90°} & 0.5e^{i180°} & 0.5e^{i180°} \\ 0.5e^{-i90°} & 0.5e^{-i90°} & 0.5e^{i0°} & 0.5e^{i0°} \end{bmatrix}. \quad (Б.20)$$

Для наглядности изобразим ортогональные последовательности (Б.20) во временной области на рисунке Б.10.

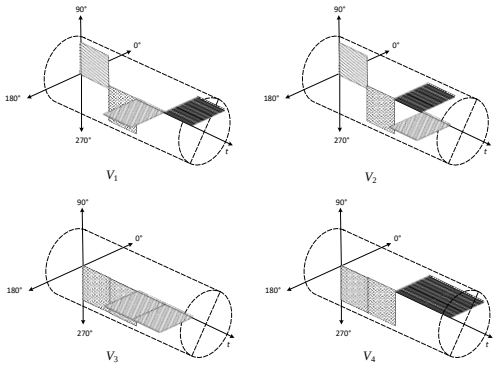


Рисунок Б.10 - Представление ортогональных последовательностей (Б.20) во временной области

Решение 2.4

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют значение $\varphi_{2,3} = 135°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=0,01$e^{i135°} = -0.01 + 0{,}01\text{i};$

$a_{3,4} = S_3$=$100e^{i0°} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.35 + 0.35\text{i} & -0.35 - 0.35\text{i} & -0.5 & 0.5 \\ 0.35 + 0.35\text{i} & -0.35 - 0.35\text{i} & 0.5 & -0.5 \\ -0.35 - 0.35\text{i} & -0.35 - 0.35\text{i} & -0.5 & -0.5 \\ -0.35 - 0.35\text{i} & -0.35 - 0.35\text{i} & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.21)}$$

Представим матрицу собственных векторов (Б.21) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i45°} & 0.5e^{-i135°} & 0.5e^{i180°} & 0.5e^{i0°} \\ 0.5e^{i45°} & 0.5e^{-i135°} & 0.5e^{i0°} & 0.5e^{i180°} \\ 0.5e^{-i135°} & 0.5e^{-i135°} & 0.5e^{i180°} & 0.5e^{i180°} \\ 0.5e^{-i135°} & 0.5e^{-i135°} & 0.5e^{i0°} & 0.5e^{i0°} \end{bmatrix}. \quad \text{(Б.22)}$$

Для наглядности изобразим ортогональные последовательности (Б.22) во временной области на рисунке Б.11.

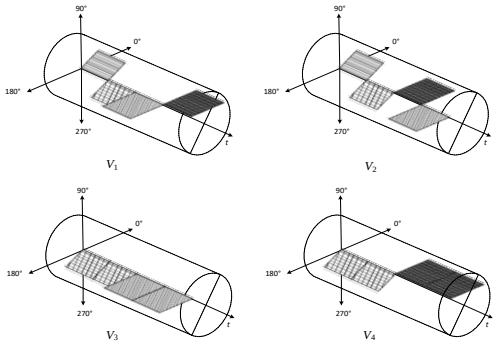


Рисунок Б.11 - Представление ортогональных последовательностей (Б.22) во временной области

Решение 2.5

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют значение $\varphi_{2,3} = 180°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=$0{,}01e^{i180°} = -0{,}01;$

$a_{3,4} = S_3$=$100e^{i0°} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.5 & -0.5 & -0.5 & 0.5 \\ 0.5\text{i} & -0.5 & 0.5 & -0.5 \\ -0.5 & -0.5 & -0.5 & -0.5 \\ -0.5 & -0.5 & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.23)}$$

Представим матрицу собственных векторов (Б.23) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.24)}$$

Для наглядности изобразим ортогональные последовательности (Б.24) во временной области на рисунке Б.12.

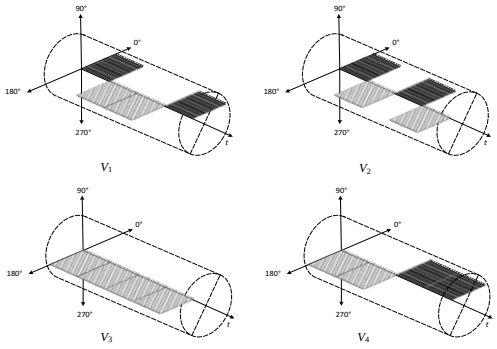


Рисунок Б.12 - Представление ортогональных последовательностей (Б.24) во временной области

Решение 2.6

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют значение $\varphi_{2,3} = 225°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0^\circ} = 100;$

$a_{2,3} = S_2$=$0{,}01e^{i225^\circ} = -0{,}01 - 0.01i;$

$a_{3,4} = S_3$=$100e^{i0^\circ} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.35 - 0.35\text{i} & -0.35 + 0.35\text{i} & -0.5 & 0.5 \\ 0.35 - 0.35\text{i} & -0.35 + 0.35\text{i} & 0.5 & -0.5 \\ -0.35 + 0.35\text{i} & -0.35 + 0.35\text{i} & -0.5 & -0.5 \\ -0.35 + 0.35\text{i} & -0.35 + 0.35\text{i} & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.25)}$$

Представим матрицу собственных векторов (Б.25) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i45^\circ} & 0.5e^{-i225^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{-i45^\circ} & 0.5e^{-i225^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i225^\circ} & 0.5e^{-i225^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i225^\circ} & 0.5e^{-i225^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.26)}$$

Для наглядности изобразим ортогональные последовательности (Б.26) во временной области на рисунке Б.13.

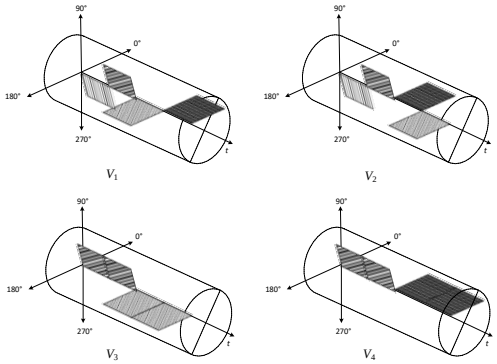


Рисунок Б.13 - Представление ортогональных последовательностей (Б.26) во временной области

Решение 2.7

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют значение $\varphi_{2,3} = 270°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0^\circ} = 100;$

$a_{2,3} = S_2$=0,01$e^{i270^\circ} = -0{,}01\text{i};$

$a_{3,4} = S_3$=$100e^{i0^\circ} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.5\text{i} & -0.5\text{i} & 0.5 & -0.5 \\ 0.5\text{i} & -0.5\text{i} & -0.5 & 0.5 \\ -0.5\text{i} & -0.5\text{i} & 0.5 & 0.5 \\ -0.5\text{i} & -0.5\text{i} & -0.5 & -0.5 \end{bmatrix}. \quad \text{(Б.27)}$$

Представим матрицу собственных векторов (Б.27) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i270^\circ} & 0.5e^{-i270^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{i270^\circ} & 0.5e^{-i270^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i270^\circ} & 0.5e^{-i270^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i270^\circ} & 0.5e^{-i270^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.28)}$$

Для наглядности изобразим ортогональные последовательности (Б.28) во временной области на рисунке Б.14.

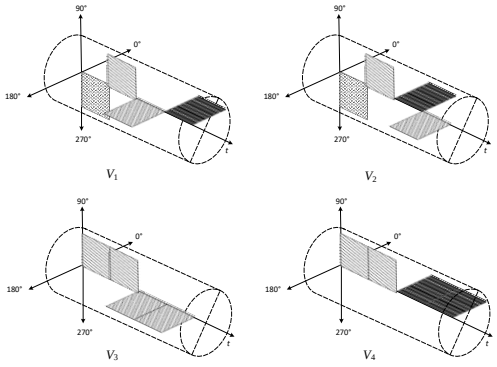


Рисунок Б.14 - Представление ортогональных последовательностей (Б.28) во временной области

Решение 2.8

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют значение $\varphi_{2,3} = 315°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0^\circ} = 100;$

$a_{2,3} = S_2$=$0{,}01e^{i315^\circ} = 0{,}01 - 0{,}01\text{i};$

$a_{3,4} = S_3$=$100e^{i0^\circ} = 100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.35 - 0.35\text{i} & 0.35 + 0.35\text{i} & -0.5 & 0.5 \\ -0.35 - 0.35\text{i} & 0.35 + 0.35\text{i} & 0.5 & -0.5 \\ 0.35 + 0.35\text{i} & 0.35 + 0.35\text{i} & -0.5 & -0.5 \\ 0.35 + 0.35\text{i} & 0.35 + 0.35\text{i} & 0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.29)}$$

Представим матрицу собственных векторов (Б.29) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i225^\circ} & 0.5e^{-i315^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{i225^\circ} & 0.5e^{-i315^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i315^\circ} & 0.5e^{-i315^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i315^\circ} & 0.5e^{-i315^\circ} & 0.5e^{i0^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.30)}$$

Для наглядности изобразим ортогональные последовательности (Б.30) во временной области на рисунке Б.15.

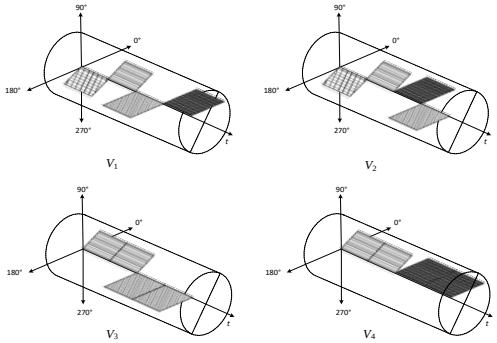


Рисунок Б.15 - Представление ортогональных последовательностей (Б.30) во временной области

Вывод по задаче 2:

Из результатов экспериментальных расчетов собственных векторов эрмитовых бидиагональных матриц четвертого порядка, имеющих фиксированные значения модулей всех диагональных коэффициентов $a_{1,2}, a_{2,3}, a_{3,4}$, а также фиксированное значение фаз (аргументов) диагональных коэффициентов $a_{1,2} = 0°$ и $a_{3,4} = 0°$, установлено, что изменение фазы (аргумента) у диагонального коэффициента $a_{2,3}$ эрмитовой бидиагональной матрицы на угол $\varphi_{2,3}$, изменяющийся в диапазоне от 0° до 360° $\varphi_{2,3} = 0° \ldots 360°$, приводит одновременно к изменению фаз (аргументов) первых и вторых координат системы собственных векторов получаемой при этом эрмитовой матрицы на такой же угол, но с противоположным знаком, т.е. $-\varphi_{2,3}$.

Задача 3

Дано:

1. Бидиагональная эрмитова матрица четвертого порядка $N = 4$.

2. Модули диагональных коэффициентов второй диагонали эрмитовой матрицы имеют следующие значения $a_{1,2} = 100;\ a_{2,3} = 0.01;\ a_{3,4} = 100$.

3. Диагональные коэффициенты эрмитовой матрицы третьей и четвертой диагонали равны нулю.

4. Коэффициенты главной диагонали равны нулю $d_{1,1} = 0; d_{2,2} = 0;\ d_{3,3} = 0;\ d_{4,4} = 0$.

5. Аргументы диагональных коэффициентов второй диагонали $a_{1,2}$ и $a_{2,3}$ имеют фиксированное значение $\varphi_{1,2} = \varphi_{2,3} = 0°$.

6. Аргументы коэффициента $a_{3,4}$ второй диагонали имеют следующий набор значений $\varphi_{3,4} = 0°, 45°, 90°, 135°, 180°, 225°, 270°, 315°$.

Найти:

Матрицы собственных векторов V, удовлетворяющих условию задачи 3.

Решение 3.1

Данное решение представим для случая, когда аргумент коэффициента $a_{3,4}$ второй диагонали имеют значение $\varphi_{3,4} = 0°$. При этом остальные коэффициенты второй диагонали имеют следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=0,01$e^{i0°} = 0{,}01;$

$a_{3,4} = S_3$=$100e^{i0°} = 100.$

Данное решение совпадает с решением 1.1, поэтому его повторно рассматривать не будем.

Решение 3.2

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют следующее значение $\varphi_{3,4} = 45°$. При этих условиях коэффициенты второй диагонали будут иметь следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=0,01$e^{i0°} = 0{,}01;$

$a_{3,4} = S_3$=$100e^{i45°} = 70.71 + 70.71i.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.34 + 0.34\mathrm{i} & 0.34 - 0.34\mathrm{i} & -0.36 + 0.36\mathrm{i} & 0.51 \\ -0.36 + 0.36\mathrm{i} & 0.36 - 0.36\mathrm{i} & 0.34 - 0.34\mathrm{i} & -0.48 \\ -0.36 + 0.36\mathrm{i} & -0.36 + 0.36\mathrm{i} & 0.34 - 0.34\mathrm{i} & 0.48 \\ 0.34 - 0.34\mathrm{i} & 0.34 - 0.34\mathrm{i} & 0.36 - 0.36\mathrm{i} & 0.51 \end{bmatrix} \quad \text{(Б.31)}$$

Проинвертируем первую последовательность, чтобы вторая координата поворачивалась на угол -45°, как и у остальных последовательностей.

$$V = \begin{bmatrix} 0.34 - 0.34\mathrm{i} & -0.34 + 0.34\mathrm{i} & 0.36 - 0.36\mathrm{i} & -0.51 \\ -0.36 + 0.36\mathrm{i} & 0.36 - 0.36\mathrm{i} & 0.34 - 0.34\mathrm{i} & -0.48 \\ -0.36 + 0.36\mathrm{i} & -0.36 + 0.36\mathrm{i} & 0.34 - 0.34\mathrm{i} & 0.48 \\ 0.34 - 0.34\mathrm{i} & 0.34 - 0.34\mathrm{i} & 0.36 - 0.36\mathrm{i} & 0.51 \end{bmatrix}. \quad \text{(Б.32)}$$

Представим матрицу собственных векторов (Б.32) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i45^\circ} & 0.5e^{i135^\circ} & 0.5e^{-i45^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i135^\circ} & 0.5e^{-i45^\circ} & 0.5e^{-i45^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i135^\circ} & 0.5e^{i135^\circ} & 0.5e^{-i45^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{-i45^\circ} & 0.5e^{-i45^\circ} & 0.5e^{-i45^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.33)}$$

Для наглядности изобразим ортогональные последовательности (Б.33) во временной области на рисунке Б.16.

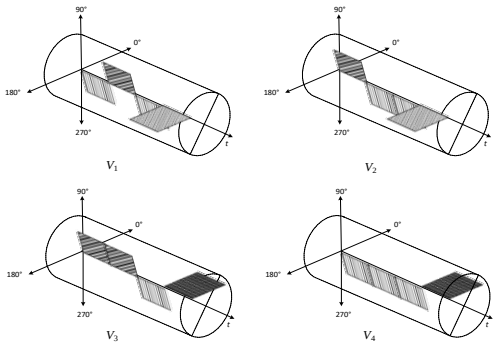


Рисунок Б.16 - Представление ортогональных последовательностей (Б.33) во временной области

Решение 3.3

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют следующее значение $\varphi_{3,4} = 90°$. При этих условиях коэффициенты второй диагонали будут иметь следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=0,01$e^{i0°} = 0{,}01;$

$a_{3,4} = S_3$=100$e^{i90°} = 100i.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.5\text{i} & 0.5\text{i} & -0.5\text{i} & -0.5 \\ -0.5\text{i} & 0.5\text{i} & 0.5\text{i} & 0.5 \\ 0.5\text{i} & 0.5\text{i} & -0.5\text{i} & 0.5 \\ 0.5\text{i} & 0.5\text{i} & 0.5\text{i} & -0.5 \end{bmatrix}. \quad \text{(Б.34)}$$

Проинвертируем вторую и четвертую последовательность, чтобы третья координата поворачивалась на угол -90°, как и у остальных последовательностей.

$$V = \begin{bmatrix} -0.5\text{i} & 0.5\text{i} & -0.5\text{i} & -0.5 \\ 0.5\text{i} & -0.5\text{i} & -0.5\text{i} & -0.5 \\ 0.5\text{i} & 0.5\text{i} & -0.5\text{i} & 0.5 \\ -0.5\text{i} & -0.5\text{i} & -0.5\text{i} & 0.5 \end{bmatrix}. \quad \text{(Б.35)}$$

Представим матрицу собственных векторов (Б.35) в показательной форме [140]

$$V = \begin{bmatrix} 0.5e^{-i90°} & 0.5e^{i90°} & 0.5e^{-i90°} & 0.5e^{i180°} \\ 0.5e^{i90°} & 0.5e^{-i90°} & 0.5e^{-i90°} & 0.5e^{i180°} \\ 0.5e^{i90°} & 0.5e^{i90°} & 0.5e^{-i90°} & 0.5e^{i0°} \\ 0.5e^{-i90°} & 0.5e^{-i90°} & 0.5e^{-i90°} & 0.5e^{i0°} \end{bmatrix}. \quad \text{(Б.36)}$$

Для наглядности изобразим ортогональные последовательности (Б.36) во временной области на рисунке Б.17

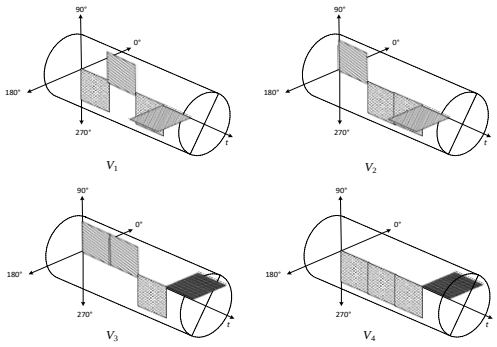


Рисунок Б.17 - Представление ортогональных последовательностей (Б.36) во временной области

Решение 3.4

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют следующее значение $\varphi_{3,4} = 90°$. При этих условиях коэффициенты второй диагонали будут иметь следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=$0{,}01e^{i0°} = 0{,}01;$

$a_{3,4} = S_3$=$100e^{i135°} = -70.71 + 70.71i.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.37 - 0.37\text{i} & 0.37 + 0.37\text{i} & -0.33 - 0.33\text{i} & -0.47 \\ -0.33 - 0.33\text{i} & 0.33 + 0.33\text{i} & 0.37 + 0.37\text{i} & 0.52 \\ -0.33 - 0.33\text{i} & -0.33 - 0.33\text{i} & 0.37 + 0.37\text{i} & -0.52 \\ 0.37 + 0.37\text{i} & 0.37 + 0.37\text{i} & 0.33 + 0.33\text{i} & -0.47 \end{bmatrix}. \quad \text{(Б.37)}$$

Проинвертируем вторую, третью и четвертую последовательность, чтобы третья координата поворачивалась на угол -135°, как и у первой последовательности.

$$V = \begin{bmatrix} -0.37 - 0.37\text{i} & 0.37 + 0.37\text{i} & -0.33 - 0.33\text{i} & -0.47 \\ 0.33 + 0.33\text{i} & -0.33 - 0.33\text{i} & -0.37 - 0.37\text{i} & -0.52 \\ 0.33 + 0.33\text{i} & 0.33 + 0.33\text{i} & -0.37 - 0.37\text{i} & 0.52 \\ -0.37 - 0.37\text{i} & -0.37 - 0.37\text{i} & -0.33 - 0.33\text{i} & 0.47 \end{bmatrix}. \quad \text{(Б.38)}$$

Представим матрицу собственных векторов (Б.38) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i135^\circ} & 0.5e^{i45^\circ} & 0.5e^{-i135^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i45^\circ} & 0.5e^{-i135^\circ} & 0.5e^{-i135^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i45^\circ} & 0.5e^{i45^\circ} & 0.5e^{-i135^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{-i135^\circ} & 0.5e^{-i135^\circ} & 0.5e^{-i135^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.39)}$$

Для наглядности изобразим ортогональные последовательности (Б.39) во временной области на рисунке Б.18.

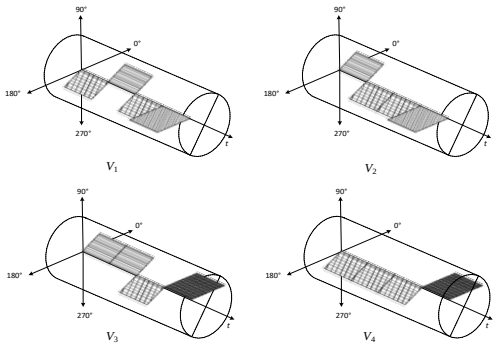


Рисунок Б.18 - Представление ортогональных последовательностей (Б.39) во временной области

Решение 3.5

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют следующее значение $\varphi_{3,4} = 90°$. При этих условиях коэффициенты второй диагонали будут иметь следующие значения:

$a_{1,2} = S_1 = 100e^{i0^\circ} = 100;$

$a_{2,3} = S_2$=$0{,}01e^{i0^\circ} = 0{,}01;$

$a_{3,4} = S_3$=$100e^{i180^\circ} = -100.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.5 & -0.5 & 0.5 & 0.5 \\ 0.5 & -0.5 & -0.5 & -0.5 \\ 0.5 & 0.5 & -0.5 & 0.5 \\ -0.5 & -0.5 & -0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.40)}$$

Проинвертируем первую последовательность, чтобы третья координата поворачивалась на угол -180°, как и у остальных последовательностей.

$$V = \begin{bmatrix} -0.5 & 0.5 & -0.5 & -0.5 \\ 0.5 & -0.5 & -0.5 & -0.5 \\ 0.5 & 0.5 & -0.5 & 0.5 \\ -0.5 & -0.5 & -0.5 & 0.5 \end{bmatrix}. \quad \text{(Б.41)}$$

Представим матрицу собственных векторов (Б.41) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i180^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{i0^\circ} & 0.5e^{i0^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i180^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.42)}$$

Для наглядности изобразим ортогональные последовательности (Б.42) во временной области на рисунке Б.19.

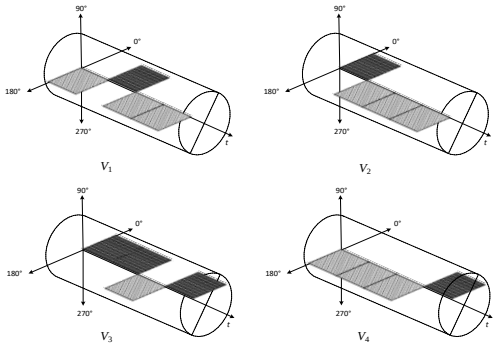


Рисунок Б.19 - Представление ортогональных последовательностей (Б.42) во временной области

Решение 3.6

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют следующее значение $\varphi_{3,4} = 225°$. При этих условиях коэффициенты второй диагонали будут иметь следующие значения:

$a_{1,2} = S_1 = 100e^{i0^\circ} = 100$;

$a_{2,3} = S_2$=0,01$e^{i0^\circ} = 0{,}01$;

$a_{3,4} = S_3$=$100e^{i225°} = -70.71 - 70.71i.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.37 + 0.37\text{i} & 0.37 - 0.37\text{i} & -0.33 + 0.33\text{i} & -0.47 \\ -0.33 + 0.33\text{i} & 0.33 - 0.33\text{i} & 0.37 - 0.37\text{i} & 0.52 \\ -0.33 + 0.33\text{i} & -0.33 + 0.33\text{i} & 0.37 - 0.37\text{i} & -0.52 \\ 0.37 - 0.37\text{i} & 0.37 - 0.37\text{i} & 0.33 - 0.33\text{i} & -0.47 \end{bmatrix}. \quad \text{(Б.43)}$$

Проинвертируем вторую, третью и четвертую последовательность, чтобы третья координата поворачивалась на угол -225°, как и у первой последовательности.

$$V = \begin{bmatrix} -0.37 + 0.37\text{i} & 0.37 - 0.37\text{i} & -0.33 + 0.33\text{i} & -0.47 \\ 0.33 - 0.33\text{i} & -0.33 + 0.33\text{i} & -0.37 + 0.37\text{i} & -0.52 \\ 0.33 - 0.33\text{i} & 0.33 - 0.33\text{i} & -0.37 + 0.37\text{i} & 0.52 \\ -0.37 + 0.37\text{i} & -0.37 + 0.37\text{i} & -0.33 + 0.33\text{i} & 0.47 \end{bmatrix}. \quad \text{(Б.44)}$$

Представим матрицу СВ (Б.44) в показательной форме

$$V = \begin{bmatrix} 0.5e^{i135°} & 0.5e^{-i45°} & 0.5e^{-i225°} & 0.5e^{i180°} \\ 0.5e^{-i45°} & 0.5e^{i135°} & 0.5e^{-i225°} & 0.5e^{i180°} \\ 0.5e^{-i45°} & 0.5e^{-i45°} & 0.5e^{-i225°} & 0.5e^{i0°} \\ 0.5e^{i135°} & 0.5e^{i135°} & 0.5e^{-i225°} & 0.5e^{i0°} \end{bmatrix}. \quad \text{(Б.45)}$$

Для наглядности изобразим ортогональные последовательности (Б.45) во временной области на рисунке Б.20.

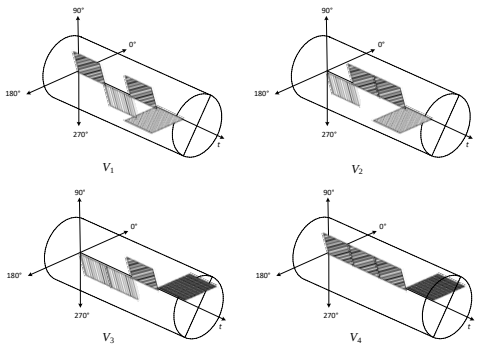


Рисунок Б.20 - Представление ортогональных последовательностей (Б.45) во временной области

Решение 3.7

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют следующее значение $\varphi_{3,4} = 270°$. При этих условиях коэффициенты второй диагонали будут иметь следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=0,01$e^{i0°} = 0{,}01;$

$a_{3,4} = S_3$=$100e^{i270°} = -100i.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} 0.5\text{i} & -0.5\text{i} & 0.5\text{i} & -0.5\text{i} \\ 0.5\text{i} & -0.5\text{i} & -0.5\text{i} & 0.5\text{i} \\ -0.5\text{i} & -0.5\text{i} & 0.5\text{i} & 0.5\text{i} \\ -0.5\text{i} & -0.5\text{i} & -0.5\text{i} & -0.5\text{i} \end{bmatrix}. \quad \text{(Б.46)}$$

Проинвертируем первую последовательность, чтобы третья координата поворачивалась на угол -270°, как и у остальных последовательностей.

$$V = \begin{bmatrix} 0.5\text{i} & -0.5\text{i} & 0.5\text{i} & -0.5\text{i} \\ -0.5\text{i} & 0.5\text{i} & 0.5\text{i} & -0.5\text{i} \\ -0.5\text{i} & -0.5\text{i} & 0.5\text{i} & 0.5\text{i} \\ 0.5\text{i} & 0.5\text{i} & 0.5\text{i} & 0.5\text{i} \end{bmatrix}. \quad \text{(Б.47)}$$

Представим матрицу собственных векторов (Б.47) в показательной форме [140]

$$V = \begin{bmatrix} 0.5e^{i90°} & 0.5e^{-i90°} & 0.5e^{-i270°} & 0.5e^{i180°} \\ 0.5e^{-i90°} & 0.5e^{i90°} & 0.5e^{-i270°} & 0.5e^{i180°} \\ 0.5e^{-i90°} & 0.5e^{-i90°} & 0.5e^{-i270°} & 0.5e^{i0°} \\ 0.5e^{i90°} & 0.5e^{i90°} & 0.5e^{-i270°} & 0.5e^{i0°} \end{bmatrix}. \quad \text{(Б.48)}$$

Для наглядности изобразим ортогональные последовательности (Б.48) во временной области на рисунке Б.21.

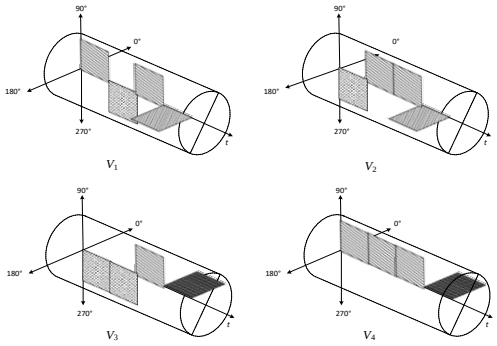


Рисунок Б.21 - Представление ортогональных последовательностей (Б.48) во временной области

Решение 3.8

Данное решение представим для случая, когда аргумент коэффициента $a_{2,3}$ второй диагонали имеют следующее значение $\varphi_{3,4} = 315°$. При этих условиях коэффициенты второй диагонали будут иметь следующие значения:

$a_{1,2} = S_1 = 100e^{i0°} = 100;$

$a_{2,3} = S_2$=0,01$e^{i0°} = 0{,}01;$

$a_{3,4} = S_3$=$100e^{i315°} = 70.71 - 70.71i.$

С помощью программы получим матрицу собственных векторов следующего вида

$$V = \begin{bmatrix} -0.37 - 0.37\text{i} & 0.37 + 0.37\text{i} & -0.33 - 0.33\text{i} & 0.47 \\ 0.33 + 0.33\text{i} & -0.33 - 0.33\text{i} & -0.37 - 0.37\text{i} & 0.52 \\ 0.33 + 0.33\text{i} & 0.33 + 0.33\text{i} & -0.37 - 0.37\text{i} & -0.52 \\ -0.37 - 0.37\text{i} & -0.37 - 0.37\text{i} & -0.33 - 0.33\text{i} & -0.47 \end{bmatrix}. \quad \text{(Б.49)}$$

Проинвертируем все последовательности, чтобы третья координата соответствовала углу -315°.

$$V = \begin{bmatrix} 0.37 + 0.37\text{i} & -0.37 - 0.37\text{i} & 0.33 + 0.33\text{i} & -0.47 \\ -0.33 - 0.33\text{i} & 0.33 + 0.33\text{i} & 0.37 + 0.37\text{i} & -0.52 \\ -0.33 - 0.33\text{i} & -0.33 - 0.33\text{i} & 0.37 + 0.37\text{i} & 0.52 \\ 0.37 + 0.37\text{i} & 0.37 + 0.37\text{i} & 0.33 + 0.33\text{i} & 0.47 \end{bmatrix}. \quad \text{(Б.50)}$$

Представим матрицу собственных векторов (Б.50) в показательной форме

$$V = \begin{bmatrix} 0.5e^{-i315^\circ} & 0.5e^{-i135^\circ} & 0.5e^{-i315^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i135^\circ} & 0.5e^{-i315^\circ} & 0.5e^{-i315^\circ} & 0.5e^{i180^\circ} \\ 0.5e^{-i135^\circ} & 0.5e^{-i135^\circ} & 0.5e^{-i315^\circ} & 0.5e^{i0^\circ} \\ 0.5e^{-i315^\circ} & 0.5e^{-i315^\circ} & 0.5e^{-i315^\circ} & 0.5e^{i0^\circ} \end{bmatrix}. \quad \text{(Б.51)}$$

Для наглядности изобразим ортогональные последовательности (Б.51) во временной области на рисунке Б.22.

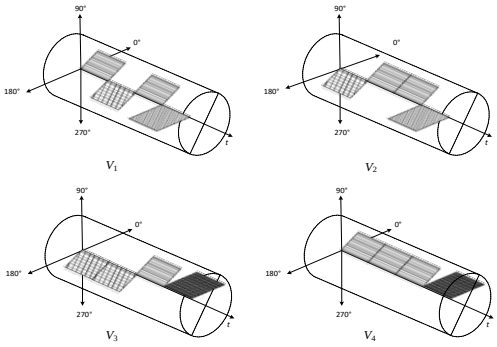


Рисунок Б.22 - Представление ортогональных последовательностей (Б.51) во временной области

Вывод по задаче 3:

Из результатов экспериментальных расчетов собственных векторов эрмитовых бидиагональных матриц четвертого порядка, имеющих фиксированные значения модулей всех диагональных коэффициентов $a_{1,2}, a_{2,3}, a_{3,4}$, а также фиксированное значение фаз (аргументов) диагональных коэффициентов $a_{1,2}$ и $a_{2,3}$ $\varphi_{1,2} = 0°$ и $\varphi_{2,3} = 0°$, установлено, что изменение фазы (аргумента) у диагонального коэффициента $a_{3,4}$ эрмитовой бидиагональной матрицы на угол $\varphi_{3,4}$, изменяющийся в диапазоне от 0° до 360° $\varphi_{3,4} = 0° \ldots 360°$, приводит одновременно к изменению фаз (аргументов) первых, вторых и третьих координат системы собственных векторов получаемой при этом эрмитовой матрицы на такой же угол, но с противоположным знаком, т.е. $-\varphi_{3,4}$.

ПРИЛОЖЕНИЕ В

Акты внедрения результатов диссертационного исследования

Infocom
28.05.2021 № 457/6
На №_____от_____

Общество с ограниченной ответственностью
«Инфоком-С»
355035, г. Ставрополь, ул. Суворова, 7
info@infocom-s.ru www.infocom-s.ru
+7 (8652) 20-58-20
ИНН : 2635811319 ОКПО : 38852042
КПП: 263501001 ОГРН: 1122651011559
+7 (495) 700-00-65

УТВЕРЖДАЮ
Генеральный директор
ООО «Инфоком-С»
д-р техн. наук, профессор_____ В.В. Копытов
«28» мая 2021 г.

АКТ
внедрения результатов диссертации
Студеникина А.В. «Метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей»

Комиссия в составе:
председателя – генерального директора ООО «Инфоком-С», д-ра техн. наук, профессора, Копытова В.В., членов – директора по проектам ООО «Инфоком-С», канд. техн. наук, доцента, Демурчева Н.Г., руководителя департамента разработки комплексных систем безопасности ООО «Инфоком-С» Касимова Р.И.

подтверждает, что основные результаты диссертационного исследования А.В. Студеникина «Метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей» нашли применение в научно-практической работе ООО «Инфоком-С», а именно:

1. Метод информационного обмена в системах передачи информации с кодовым разделением каналов на основе стохастического применения ортогональных кодовых последовательностей.
2. Практические рекомендации по использованию ортогональных кодовых последовательностей в системах передачи информации с кодовым разделением каналов.

Полученные результаты использованы в научно-практических исследованиях по созданию новых и совершенствованию существующих методов и алгоритмов скрытного информационного обмена в беспроводных системах передачи данных между распределёнными объектами на базе программной платформы «Дарвис» для цели повышения скрытности от деструктивных воздействий информации, передаваемой в беспроводных каналах связи. Разработанные метод информационного обмена в системах

передачи информации с кодовым разделением каналов на основе стохастического применения ортогональных кодовых последовательностей и рекомендации по его практическому применению использованы в научно-практических исследованиях для повышения скрытности информационного обмена существующих и перспективных беспроводных систем передачи данных распределённых объектов.

В результате использования основных результатов диссертационного исследования А.В. Студеникина «Метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей» удалось сократить время получения, анализа, интерпретации первичных данных и уменьшить трудоемкость проводимых научно-исследовательских работ по созданию новых и совершенствованию существующих методов и алгоритмов скрытного информационного обмена в беспроводных системах передачи данных между распределёнными объектами на базе программной платформы «Дарвис» для цели повышения защищенности от деструктивных воздействий на информацию, передаваемую в беспроводных каналах связи.

Председатель _____ (подпись) Копытов В.В. (ФИО)

Члены комиссии _____ (подпись) Демурчев Н.Г. (ФИО)

_____ (подпись) Касимов Р.И. (ФИО)

Утверждаю
И.о. проректора по образовательной деятельности СКФУ
канд. физ.-мат. наук., доцент
_____О.С. Мезенцева
«__13__» ___января___ 2025 г.

АКТ

об использовании результатов диссертационной работы Студеникина Андрея Владимировича на тему «Метод противодействия угрозе подмены сообщений для систем спутниковой связи с кодовым разделением каналов на основе стохастического применения ансамблей многофазных ортогональных кодовых последовательностей» в учебном процессе кафедры организации и технологии защиты информации факультета математики и компьютерных наук имени профессора Н.И. Червякова ФГАОУ ВО «Северо-Кавказский федеральный университет»

Настоящий акт составлен о том, что результаты диссертационного исследования Студеникина А.В. использованы в учебном процессе студентов на кафедре организации и технологии защиты информации факультета математики и компьютерных наук имени профессора Н.И. Червякова ФГАОУ ВО «Северо-Кавказский федеральный университет» в рамках дисциплин «Информационная безопасность автоматизированных и телекоммуникационных систем» и «Сети и системы передачи информации», изучаемых студентами по направлению подготовки 10.03.01 «Информационная безопасность», направленности (профилю) «Организация и технология защиты информации».

Использованы следующие материалы:

– структура и алгоритм функционирования системы передачи информации с кодовым разделением каналов на основе с стохастического применения ортогональных кодовых последовательностей;

– программа моделирования процесса защищенного информационного обмена в системах беспроводной связи;

– программа для ЭВМ «Программа для генерации стохастических ортогональных кодов «Stochastic orthogonal signal generator (SOSG)».

Использование в учебном процессе результатов диссертационной работы Студеникина А.В. позволило повысить наглядность обучения и качество освоения студентами дисциплин «Информационная безопасность автоматизированных и телекоммуникационных систем» и «Сети и системы

передачи информации», а также получить навыки по исследованию процесса генерации стохастических ортогональных кодов.

Заведующий кафедрой организации и технологии защиты информации факультета математики и компьютерных наук имени профессора Н.И. Червякова
канд. техн. наук, доцент _____ В.И. Петренко

И.о. декана
факультета математики и компьютерных наук имени профессора Н.И. Червякова
канд. физ.-мат. наук, доцент _____ Т.А. Гробова