МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ УКРАИНЫ
ХАРЬКОВСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ
имени В.Н. КАРАЗИНА

На правах рукописи

ЗАМУЛА АЛЕКСАНДР АНДРЕЕВИЧ

УДК 621.391

МОДЕЛИ И МЕТОДЫ СИНТЕЗА СЛОЖНЫХ СИГНАЛОВ С НЕОБХОДИМЫМИ СВОЙСТВАМИ ДЛЯ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

05.12.02 – Телекоммуникационные системы и сети

Диссертация на соискание ученой степени
доктора технических наук

Научный консультант
Горбенко Иван Дмитриевич
доктор технических наук, профессор

ХАРЬКОВ – 2016

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АКФ	–	авто-корреляционная функция
АФАК	–	апериодическая функция автокорреляции
АФВК	–	апериодическая функция взаимной корреляции
БСШ	–	блочный симметричный шифр
ВКФ	–	взаимно-корреляционная функция
ВФН	–	взаимная функция неопределенности
ДГСП	–	детерминированный генератор случайных последовательностей
CDMA	–	система множественного доступа с кодовым разделением
ИС	–	информационные системы
КП	–	криптографические последовательности
КС	–	криптографические сигналы
МСС	–	модулярная система счисления
ПСП	–	псевдослучайная последовательность
ПФАК	–	периодическая функция автокорреляции
ПФВК	–	периодическая функция взаимной корреляции
ПНС	–	производный нелинейный сигнал
СС	–	система счисления
ТЛКС		телекоммуникационная система
УП	–	управляющая последовательность
ХДС	–	характеристический дискретный сигнал
ЧМ	–	частотная модуляция
ФМ ШПС	–	фазово- манипулированные широкополосные сигналы
ФМ	–	фазовая модуляция
ЧФМ	–	частотно-фазоманипулированные сигналы
ЭЦП	–	электронная цифровая подпись

ВВЕДЕНИЕ

Уровень информатизации государства, степень его привлечения к глобальному информационному сообществу определяются, прежде всего, развитием инфотелекоммуникаций, как совокупности сетевых ресурсов, предназначенных для производства и предоставления телекоммуникационных, информационных и других услуг. Основу инфотелекоммуникаций составляют информационные сети, которые в свою очередь, базируются на телекоммуникационных сетях. С появлением новых телекоммуникационных технологий, ориентированных на пакетный способ передачи информации, использование различных сред передачи (оптическое волокно, радиочастотный ресурс), и обеспечение мобильности связи, появилась возможность существенно повысить производительность, эффективность и качество обслуживания телекоммуникационных сетей, а также расширить диапазон услуг, которые ими предоставляются [130]. Современный етап развития телекоммуникационных систем и сетей, это, по сути, этап телекоммуникационно-компьютерной интеграции. Создание высокопроизводительных, малогабаритных и относительно недорогих компьютеров, интеграция их с телекоммуникациями в качестве терминальных и коммутационных устройств, а так же достижения в области информационных технологий стали основой создания информационных сетей. Указанное дало возможность накапливать в электронном виде, сохранять и обрабатывать значительные объемы информации и предоставлять ее пользователям по их запросу в необходимые временные интервалы [129]. Появились десятки фундаментальных работ в сфере науки и техники, которая охватывает теоретические и методологические основы построения телекоммуникационных систем. Это фундаментальные работы зарубежных авторов: Hsiao-Hwa Chen, K. Fazel, S. Kaiser, Christopher Cox, Hooshang Chafouri-Shiraz, M. Massoud Karbassian, а также ученых нашей страны: Бондаренко О.В. [49-50], Климаш М.Н. [47,115-116], Кучук Г.А. [121-125] и др.

К основным показателям эффективности телекоммуникационной системы относят: надежность, живучесть, пропускную способность сети, качество обслу-

живания, рентабельность и стоимость, помехозащищенность, информационная безопасность и др. [49-50,80,115-118].

Задачи обеспечения требуемых показателей помехозащищенности (помехоустойчивости и скрытности функционирования) на уровне источника сигналов традиционно решаются на основе увеличения отношения мощности сигнала к мощности помехи на входе приемного устройства, а также улучшения направленности антенн передатчика и приемника. Интенсивность сигнала или отношение сигнал – шум является ключевым параметром, определяющим характеристику любой задачи приема. Однако энергетические параметры системы могут быть ограничены, в том числе, международными и национальными правилами, за исполнением которых следят соответствующие службы.

Среди основных направлений улучшения помехозащищенности и скрытности телекоммуникационной системы можно выделить направления, связанные с применением каналов с большой избыточностью, высокой пространственной, структурной, энергетической и временной скрытностью. Одним из путей решения данной проблемы является применение радиоканалов с частотной избыточностью (широкополосных каналов). Для ее обеспечения в настоящее время на физическом уровне используются фазоманипулированные широкополосные сигналы (ФМ ШПС) и частотно-фазоманипулированные (ЧФМ) сигналы.

Решение проблем обеспечения необходимых значений показателей помехозащищенности (помехоустойчивость, скрытность), информационной безопасности привело к идее сложных широкополосных систем. К основным достоинствам таких систем можно отнести [9,15]:

- достижение высокой помехоустойчивости по отношению к узкополосной помехе без увеличения энергии сигнала и пиковой мощности;

- возможность повышения защищенности системы от заградительной помехи (спектр помехи покрывает спектр сигнала) в условиях ограничений как на пиковую мощность полезного сигнала, так и на мощностной ресурс постановщика помех на основе использования сигналов с большим значением частотно-временного произведения полосы частот сигнала (F) на его длительность (T);

- возможность системы предотвращать обнаружение своего сигнала потенциальным перехватчиком на основе использования сигналов с распределенным спектром, обладающих максимально возможным значением выигрыша от обработки FT. Физическое обоснование данного тезиса состоит в следующем: расширение спектра сигнала с постоянной энергией и длительностью уменьшает уровень его спектральной плотности мощности, скрывая ее под спектром;

- возможность применения сигналов с практически не раскрываемой структурой и многое другое.

К числу первых наиболее важных результатов в области широкополосных или распределенных систем следует отнести результаты глубоких исследований, проведенные Р. Вудвордом. Опубликованные Р. Вудвордом результаты базировались на фундаментальных работах Шеннона [28,29]. Работы Zierler [34-36], Golomb [14], R. Gold [13], T. Kasami [21], D.V. Sarvate, M.P. Pursley [27], M. Simon [30] и других ученых в области синтеза дискретных сигналов со специальными корреляционными свойствами имели важное значение для развития теории и практики широкополосных систем. Значительный вклад в развитие широкополосной идеологии внесли отечественные ученые Я.Д. Ширман, И.М. Амиантов, Л.Е. Варакин, М.Б. Свердлик, В.Б. Пестряков, И.Д. Горбенко, В.П. Ипатов и многие другие.

В конце 70- годов прошлого столетия стали активно развиваться системы мобильной телефонной связи. Такие системы, как и многие другие современные беспроводные системы (например, спутниковые системы), относятся к многопользовательским. При проектировании таких систем основной проблемой является выбор способа множественного доступа, т. е возможности одновременного использования многими абонентами канала связи с минимальным взаимным влиянием. При необходимости обслуживания большого числа абонентов частотно-временной ресурс должен быть значительным, и если каждый пользовательский сигнал занимает как всю доступную полосу, так и весь временной интервал, то есть необходимость применения ортогональной схемы множественного доступа, в которой все пользовательские сигналы широкополосны. Такая многопользовательская система будет обладать всеми достоинствами широкополосной технологии. Если передача ин-

формации организована таким образом, что каждому абоненту «назначается» свой широкополосный сигнал (сигнатура) из множества ортогональных сигналов, и каждый сигнал занимает всю полосу и весь временной интервал, передавая $\log_2 M$ бит информации, то такой способ разделения абонентов называют множественным доступом с кодовым разделением (CDMA) [5,20,22,31-32]. Такой способ доступа является основой физического слоя «вниз» в сотовых сетях с CDMA второго (IS – 95) и 3-го (UMTS, cdma 2000) поколений. Необходимым условием для обеспечения ортогональности и разделения абонентов на приемной стороне является синхронизация сигнатур (для синхронного метода с CDMA). При асинхронном способе множественного доступа с CDMA задержки различных сигналов на входе приемного устройства могут изменяться в широком диапазоне. В этом случае процедура синхронизации широкополосных сигналов (сигнатур) становится проблематичной. Примером такого положения дел может служить канал «вверх» системы мобильной сотовой связи, в которой потребители передвигаются внутри соты [15], из-за чего происходит изменение расстояния между ними и базовой станцией, а значит, и времени поступления пользовательских сигналов на приемник базовой станции. В этом случае сигнатуры различных абонентов, обладая перекрывающимися спектрами, не могут оставаться ортогональными в широком диапазоне взаимных задержек. Следствием указанного является возникновение межпользовательского мешающего воздействия (помехи множественного доступа), проявлением которого служит ненулевой отклик приемника, настроенного на j-го абонента, от сигналов других абонентов. Для приложений телекоммуникационных систем, в которых используется асинхронный метод с CDMA, требуются особенные свойства взаимно корреляционных функций сигналов (сигнатур).

Актуальность темы. Основные теоретические положения теории широкополосных сигналов сформировались к концу семидесятых и началу восьмидесятых годов. Широкое применение получили дискретные сигналы, в которых манипулируемые параметры (амплитуда, фаза, частота) изменяются через строго фиксированные интервалы времени. Закон изменения манипулируемого параметра дискретных сигналов задается дискретными последовательностями, которые полно-

стью определяют свойства дискретных сигналов и часто отождествляются с ними [27]. Именно поэтому внимание ученых оказалось сосредоточенным на анализе, синтезе и обработке дискретных последовательностей.

Анализ методов информационного обмена в телекоммуникационных системах (ТКС) показывает, что для передачи данных в таких системах используют дискретные сигналы с линейными законами их формирования. Однако применение указанных систем сигналов в ТКС, не обеспечивают требуемые показатели по помехозащищенности и скрытности их функционирования [82]. Сигналы с линейным законом формирования обладают весьма ограниченными ансамблевыми характеристиками и низкой кодовой устойчивостью против раскрытия законов их формирования (низкой структурной скрытностью). Кроме того, повышение помехозащищенности, скрытности функционирования телекоммуникационных систем может быть достигнуто за счет изменения длительности (числа символов) сигналов. Однако при использовании данных классов сигналов корреляционные, спектральные, ансамблевые и структурные свойства сигналов существенно ухудшаются, что, в свою очередь, приводит к ухудшению указанных выше характеристик функционирования телекоммуникационных систем [85].

Кроме того, применяемые в ТКС методы цикловой синхронизации и управления предполагают, что в течение продолжительного времени в канале синхронизации передается один и тот же широкополосный сигнал линейной формы, а в информационном канале, т.е. на физическом уровне, соответствие: бит (m бит) сообщения - сигнал линейной формы (2^m сигналов) с течением времени остается фиксированным. Такой метод информационного обмена в ТКС позволяет нарушителю на основе определения параметров используемых в системе сигналов, осуществить постановку преднамеренных помех с минимальными энергетическими затратами. Такие помехи с точки зрения нарушителя являются оптимальными и могут быть созданы при некоторой априорной определенности станции разведки и противодействия нарушителя относительно пространства состояний канала передачи данных (несущие частоты, формы используемых сигналов и др.). Для рассматриваемого случая, помехи представляют собой либо ретранслирован-

ные, либо имитационные помехи, обработка которых совместно с полезным сигналом, приводит к энергетическому подавлению последнего.

В указанных условиях в процессе информационного противодействия нарушитель, с большой вероятностью, может осуществить подавление радиоканала, применяя станции помех с энергетическим потенциалом, соизмеримым с энергетикой радиоканала, а также осуществить навязывание режимов работы системы (режима синхронизации, ложных сообщений), что может привести к существенному ухудшению показателей функционирования телекоммуникационной системы (помехозащищенности, информационной безопасности, имитостойкости, вероятносто-временных показателей передачи сообщений, живучести и др.).

Приведенные выше доводы позволяют утверждать, что применяемые в ТКС методы информационного обмена, основанные на фиксированном соответствии: бит сообщения (n бит) – сложный сигнал (2^n сигналов) в информационном канале, и использование (в течение продолжительного времени) в канале синхронизации одного и тот же широкополосного сигнала (причем используемые сигналы построены с применением линейных законов), не позволяют обеспечить необходимые значения помехозащищенности и информационной безопасности функционирования телекоммуникационной системы.

Основными путями решения указанного противоречия является повышение помехозащищенности (в частности, энергетической, структурной и информационной скрытности) и информационной безопасности (в частности, имитостойкости) телекоммуникационной системы на основе усовершенствования методологических основ построения ТКС путем разработки методов информационного обмена, синтеза новых классов нелинейных дискретных сложных сигналов с необходимыми ансамблевыми, корреляционными и структурными свойствами.

Становится все более актуальным вопрос о создании комплексной системы защиты информации, в том числе, и о управлении рисками информационной безопасности, в ТКС компании, учреждении, организации. Основной задачей данного направления является использование совокупности организационных и программно-технических средств защиты от несанкционированных воздействий в

целях повышения эффективности функционирования ТКС [7, 72,87-88,95,97,99,101,106,113].

Связь работы с научными программами, планами, темами.

Направления исследований тесно связаны с рядом научно-исследовательских и опытно-конструкторских работ, выполненных в соответствии с планами научной и научно-технической деятельности Харьковского Национального университета имени В. Н. Каразина, Харьковского национального университета радиоэлектроники. Результаты исследований получены в ходе решения отдельных вопросов следующих НИР:

- «Обоснование требований, разработка и внедрение инфраструктуры электронной цифровой подписи в МОНУ» (№ Госрегистрации 0106U006221);

- «Направления, методы и средства совершенствования и развития национальной инфраструктуры открытых ключей (№Госрегистрации 0109U002573);

- «Развитие, стандартизация, унификация, совершенствование и внедрение инфраструктуры открытых ключей, включая национальную систему электронной цифровой подписи (ЭЦП)» (№Госрегистрации 0111U002628);

- «Анализ состояния, определение направлений развития, стандартизация, совершенствование, разработка и внедрение криптографических систем, включая систему электронной цифровой подписи (ЭЦП)» (№Госрегистрации 0113U000363);

- «Методы, системы и средства криптографической защиты информации с гарантированным уровнем стойкости и повышенным быстродействием» (№Госрегистрации 0115U002431);

- «Математическое и компьютерное моделирование информационных процессов в сложных естественных и технических системах" (№Госрегистрации 0112U002098).

При выполнении указанных НИР соискателем разработаны теоретические основы информационного обмена, а так же ряд методов синтеза систем сложных нелинейных сигналов и методов обработки данных, для реализации в ТКС в условиях внешних и внутренних воздействий. Проведено математическое и физиче-

ское моделирование методов синтеза и исследования свойств сложных сигналов. На основе разработанных и усовершенствованных в диссертации методов синтеза систем сигналов, а также методов быстрой реализации модульных операций представлены алгоритмы для их реализации, в соответствии с которыми синтезирован класс средств синтеза сигналов и обработки данных в телекоммуникационных системах, на которые получено 14 патентов Украины.

Цель и задачи исследований. Целью диссертационной работы является улучшение показателей помехозащищенности и информационной безопасности телекоммуникационной системы в условиях внешних и внутренних воздействий на основе развития теории синтеза новых классов сложных нелинейных дискретных сигналов с необходимыми свойствами, а также развития теории и практики информационного обмена в телекоммуникационной системе.

Для достижения поставленной цели необходимо найти новые решения научной проблемы взаимодействия удаленных информационных объектов – повышения помехозащищенности и информационной безопасности телекоммуникационной системы в условиях внешних и внутренних воздействий за счет усовершенствования методологических основ построения телекоммуникационной системы путем разработки методов синтеза сложных нелинейных дискретных сигналов с необходимыми ансамблевыми, структурными и корреляционными свойствами, а также методов обработки данных в телекоммуникационной системе. Нахождение новых решений сформулированной научной проблемы возможно на основе постановки и решения ряда взаимосвязанных научных задач. К основным задачам исследований диссертационной работы относятся следующие.

1. Исследование проблемы защищенности информационного обмена в телекоммуникационных системах. Выявление причин, порождающих указанную научную проблему, выбор критериев оценки и показателей эффективности исследуемых процессов и обоснование направлений исследований.

2. Математическое обоснование, разработка и исследование методов синтеза нелинейных дискретных сложных сигналов в конечных полях с улучшенными

ансамблевыми, корреляционными, структурными свойствами в целях повышения помехозащищенности и информационной безопасности ТКС.

3. Разработка модели структуры сложных нелинейных дискретных сигналов в конечных полях в целях определения структурной скрытности данного класса сигналов для оценки показателей помехозащищенности и информационной безопасности ТКС.

4. Разработка и исследование методов синтеза нелинейных криптографических дискретных сложных сигналов с улучшенными ансамблевыми, корреляционными, структурными свойствами в целях повышения помехозащищенности и информационной безопасности ТКС.

5. Исследование свойств новых синтезированных классов нелинейных дискретных сложных сигналов для использования в ТКС в качестве физического переносчика информации.

6. Разработка методов оценки свойств нелинейных дискретных сложных сигналов, которые позволят снизить вычислительные затраты на реализацию процесса нахождения (отбора) сложных сигналов с улучшенными ансамблевыми, корреляционными и структурными свойствами.

7. Разработка программных моделей, реализующих педложенные методы синтеза нелинейных дискретных сложных сигналов и исследование свойств синтезированных систем сигналов.

8. Разработка и усовершенствование методов быстрой реализации модульных операций.

9. Усовершенствование методов информационного обмена в ТКС в целях улучшения показателей помехозащищенности и информационной безопасности ТКС.

Объект исследования: процессы информационного обмена и управление этим обменом, протекающих в ТКС и сетях.

Предмет исследования. Модели и методы повышения помехозащищенности и информационной безопасности ТКС на основе синтеза новых классов нелиней-

ных дискретных сигналов с необходимыми ансамблевыми, структурными и корреляционными свойствами.

Методы исследований определены сущностью решаемых задач и включают положения: теории информации, теории систем сигналов, методы теории вероятностей и случайных процессов, теории криптографической защиты информации, которые использованы в аналитической разработке методов управления информационной безопасностью (реализация динамического режима работы системы); теории систем сигналов, теории групп, колец, полей при решении задач разработки моделей и методов синтеза систем сложных сигналов в конечных полях; методы теории цифровых автоматов и методы анализа и синтеза сложных технических систем при разработке методов реализации арифметических операций в модулярной системе счисления; методы для нахождения оптимальных решений различных задач дискретной и комбинаторной оптимизации при разработке усовершенствованного метода синтеза сигналов с заданными свойствами.

Получены следующие **научные результаты**.

Развиты теория синтеза новых систем сложных нелинейных дискретных сигналов, теория информационного обмена, теория арифметических модульных операций для улучшения показателей эффективности ТКС.

Научная новизна полученных результатов обусловлена решением, на основе проведенных теоретических и экспериментальных исследований, актуальной научной проблемы повышения помехозащищенности и информационной безопасности телекоммуникационной системы в условиях внешних и внутренних воздействий за счет усовершенствования методологических основ построения телекоммуникационной системы путем разработки моделей и методов синтеза новых классов нелинейных дискретных сигналов с необходимыми ансамблевыми, структурными и корреляционными свойствами, методов информационного обмена, а также методов реализации арифметических операций в модулярной системе счисления.

К основным новым научным результатам следует отнести следущие.

Впервые получены:

- метод синтеза сложных нелинейных дискретных криптографических сигналов, который использует случайные (псевдослучайные) процессы, и позволяет создавать сигналы с необходимыми ансамблевыми, структурными и корреляционными свойствами, что дает возможность улучшить показатели помехозащищенности и информационной безопасности телекоммуникационной системы в условиях внешних и внутренних воздействий;

- математическая модель структуры сложных нелинейных дискретных сигналов в конечных полях, определяющей зависимость характеров элементов мультипликативной группы поля Галуа и символов дискретных последовательностей, синтезированных с использованием характеров элементов мультипликативной группы поля, что позволяет определить значения показателей помехозащищенности (структурной скрытности) дискретных сигналов;

- метод реализации арифметических модульных операций сложения и вычитания, основанный на табличном принципе реализации арифметических операций посредством использования специального кода табличного умножения, что позволяет повысить быстродействие выполнения модульных операций сложения и вычитания;

- метод реализации арифметической модульной операции умножения, основанный на использовании табличного принципа путем использования процедуры поразрядного определения результата операции, что позволяет повысить быстродействие выполнения модульных операций модульного умножения.

Усовершенствованы:

- метод синтеза нелинейных дискретных сложных сигналов, в котором, в отличие от известных, используется зависимость между элементами и индексами элементов конечного поля, что позволяет повысить быстродействие синтеза сигналов;

- метод синтеза нелинейных криптографических дискретных сложных сигналов, в котором, в отличие от известных, используются механизмы направленного (ограниченного) перебора сигналов для отбора сигналов, отвечающих определен-

ным требованиям, что позволяет повысить производительность синтеза системы сигналов с необходимыми свойствам;

- метод оценки свойств нелинейных дискретных сложных сигналов, в котором, в отличие от известных, использованы алгебраические свойства элементов конечного поля, что позволяет увеличить быстродействие процесса исследования свойств сигналов, и, таким образом, повысить производительность синтеза системы сигналов с необходимыми свойствами;

- метод синтеза всей системы нелинейных дискретных сигналов, в котором, в отличие от известных, используется процедура считывания символов изоморфизма нелинейного сигнала по правилу, задаваемому коэффициентами децимации и образования, таким образом, всего множества сигналов, относящегося к этому классу сигналов, что позволяет повысить производительность синтеза сигналов;

- метод информационного обмена данными, в котором, в отличие от известных, применяется изменение соответствия: бит сообщения - сложный сигнал и, в качестве сложных сигналов, применяются нелинейные дискретные сигналы с необходимыми ансамблевыми, структурными и корреляционными свойствами, что позволяет улучшить показатели информационной безопасности и помехозащищенности;

- метод реализации арифметических модульных операций сложения и вычитания, который, в отличие от известных, основан на использовании принципа кольцевого сдвига, посредством представления остатков числа двоичным кодом, за счет использования свойств циклических перестановок содержания кольцевого регистра, что позволяет повысить быстродействие выполнения модульных операций.

Практическое значение диссертационных исследований заключается в следующем.

Впервые получен метод синтеза нелинейных криптографических дискретных сигналов, который использует случайные или псевдослучайные процессы, и создает последовательности символов (сигналов) определенного алфавита, которые удовлетворяют требованиям необратимости, неразличимости, непредсказуемости,

и обладают необходимыми ансамблевыми и корреляционными свойствами. Практическое использование данной системы сигналов позволит повысить скрытность функционирования ТКС. Так, для периода сигналов порядка 1000 элементов структурная скрытность криптографических сигналов превышает данный показатель для линейных классов сигналов (М последовательностей) более чем в 30 раз. Характеристики корреляционных функций синтезированных КС не уступают, а в ряде случаев превосходят, соответствующие характеристикам линейных сигналов. В частности, КП обладают улучшенными по сравнению с М последовательностями, взаимно корреляционными свойствами. Применение синтезированных систем нелинейных криптографических сигналов (КС) позволит, например, при использовании КС с периодом 256 элементов в качестве синхронизирующих последовательностей, более чем на 3 дБ повысить помехоустойчивость приема сигналов. За счет улучшенных ансамблевых свойств КС, появляется возможность улучшить показатели информационной безопасности. Так, имитостойкость системы при применении КС с периодом сигнала 1023 элемента на пять порядков выше, чем при применении линейных классов сигналов (например, М – последовательностей). При этом необходимо подчеркнуть, что при увеличении имитостойкости системы обеспечивается высокий уровень помехоустойчивости приема сигналов. Улучшенные по сравнению с линейными классами сигналов ансамблевые свойства КС позволяют повысить информационную скрытность системы.

Усовершенствован метод синтеза системы КС на основе направленного (ограниченного) перебора всех возможных сигналов для отбора таких, которые удовлетворяют заданным требованиям, что позволяет повысить быстродействие процесса синтеза системы таких сигналов (от 45 до 60 процентов).

Усовершенствованные методы синтеза систем нелинейных сигналов в конечных полях позволяют повысить (за счет улучшенных корреляционных свойств сигналов) помехоустойчивость приема. Так при использовании указанных нелинейных сигналов в качестве синхропоследовательностей (при периоде сигнала 256 элементов) помехоустойчивость приема КС на 4 дБ выше, чем в случае использования линейных классов сигналов. Кроме того полученные методы позво-

ляют повысить производительность синтеза системы сигналов для практической реализации динамического режима передачи данных. Так для периода нелинейного сигнала 10098 элементов (объем системы составляет 2880 сигналов) выигрыш при использовании разработанного метода синтеза сигналов по сравнению с известным составляет более 720 раз.

Разработаны методы табличной реализации модульных операций в МСС с использованием специального кода табличного представления операндов, которые позволяют, в зависимости от величины l-байтового ($l=\overline{1-4,8}$) машинного слова, например, при выполнении операции модульного умножения от 64 до 4096 раз сократить время выполнения операций, по сравнению с использованием сумматорного метода в позиционной системе счисления.

На основе разработанных и усовершенствованных в диссертации методов синтеза систем НС, быстрой реализации модульных операций в работе представлены алгоритмы для их реализации, в соответствии с которыми синтезирован класс аппаратных средств формирования и обработки сигналов в ТКС, на которые получено 14 патентов Украины, что подтверждает мировую новизну и практическую значимость полученных в диссертации научных результатов работы.

Разработаны модели и методы синтеза систем нелинейных дискретных сигналов с необходимыми для тех или иных приложений телекоммуникационных систем свойствами, получены вычислительные алгоритмы и программная реализация указанных моделей и методов, а также исследования свойств новых классов нелинейных сигналов. Созданный программный комплекс позволяет: генерировать криптографические последовательности символов практически любой длительности; получать значения минимальных и максимальных боковых выбросов корреляционных функций; сравнивать полученные значения с известными граничными значениями; считывать отобранные, удовлетворяющие границам, последовательности; присваивать выбранным последовательностям уникальные идентификаторы (специальные радио данные); исследовать ансамблевые, статистические и корреляционных свойства синтезированных сигналов; генерировать параметры, используемые в процессе синтеза и исследования свойств сигналов

(первообразные элементы конечного поля, примитивные полиномы заданной степени, значения функции Эйлера для заданного периода синтезируемой последовательности, числа взаимно простые с значением периода последовательности и др.).

Разработан метод информационного обмена данными, в котором, по определенному закону изменяется с течением времени соответствие: бит сообщения - сложный сигнал, и в качестве сложных сигналов применяются сигналы с необходимыми ансамблевыми, структурными и корреляционными свойствами, что позволяет повысить помехозащищенность и информационную скрытность ТКС. Так при реализации динамического режима функционирования системы и использовании множества нелинейных дискретных сигналов с периодом 10000 элементов, имитостойкость системы на три порядка выше, чем при использовании линейных дискретных сигналов с трехуровневой функцией корреляции, которые являются лучшими с точки зрения ансамблевых и корреляционных свойств в данном классе сигналов.

Полученные в работе результаты нашли практическое внедрение и использование:

- при построении телекоммуникационной системы в Приватном акционерном обществе «Институт информационных технологий» (г. Харьков), в соответствие с Договором №0003/01-15 от 08.07.15. (Акт использования от 28.09. 2015г.);

- при выполнении научно-исследовательских работ по разработке перспективных средств связи и определении путей модернизации «Малогабаритной помехозащищенной коротковолновой радиостанции малой мощности», которая разработана и изготовлена в Государственном предприятии «Центральное конструкторское бюро «Протон» (г. Харьков) (Акт внедрения от 23.09. 2015г.);

- при выполнении научно-исследовательских и опытно-конструкторских работ: «Построение моделирующего комплекса для управления функционированием корабельного соединения»; «Исследование и разработка методов обеспечения живучести компьютерных информационных сетей для высокотехнологических

объектов» в Институте проблем регистрации информации Национальной Академии наук Украины (г. Киев), (Акт внедрения от 07.09. 2015г.);

- в учебном процессе кафедры национального университета им. В.Н. Каразина при изложении дисциплин « Управление информационной безопасностью», «Комплексные системы защиты информации: проектирование, внедрение, сопровождение», «Нормативно-правовое обеспечение информационной безопасности», что подтверждается Актом использования от 21.09. 2015г.

Акты, подтверждающие практическое значение работы, представлены в Приложении Ж.

Личный вклад соискателя. Все основные научные положения, результаты, выводы и рекомендации диссертации получены автором самостоятельно. Из перечня основных публикаций работы [74,78,82-84,87,93-94,96,102,110,111-112] выполнены без соавторов. Личным вкладом автора диссертации в работы, написанные в соавторстве, был определяющим. В работах, выполненных в соавторстве и опубликованных в научных специализированных изданиях Украины, а также в зарубежных изданиях, которые входят в научно-метрические базы, личный вклад автора в статьи состоит в следующем.

В работе [48] представлены концепция и политика безопасности информации в телекоммуникационных системах, в которых решаются задачи обеспечения информационной безопасности; в работе [89] приведен анализ методов аутентификации объектов данных и субъектов телекоммуникационной сети; в работе [90] определены условия обеспечения абсолютной стойкости при реализации услуг целостности и подлинности сообщений; в работе [120] предложены алгоритмы реализации операций сложения, умножения на основе сжатия цифровых данных таблиц; в работе [46] предложен метод повышения производительности обработки данных в автоматизированных системах управления; в работе [87] приведен сравнительный анализ методов анализа и управления рисками информационной безопасности, сформулированы предложения по использованию методов оценки рисков (воздействий) в телекоммуникационных системах; в работе [45] предложена структура процесса обработки информации на основе применения модуляр-

ной системы счисления; в работе [128] разработан метод реализации операции сложения в модульных системе счисления; в работе [119] разработан метод обработки информации в модулярной системе счисления; в работе [127] предложен метод реализации операции сложения и вычитания за счет унитарного кодирования остатков чисел на основе принципа кольцевого сдвига в модульной системе счисления; в работе [113] сформулированы принципы проектирования систем защиты информации в ТКС; в работе [61] приводится математическая модель построения структуры дискретной последовательности, которая позволяет получить оценку структурной скрытности нелинейных сигналов; в работе [88] приводится анализ несанкционированных воздействий на ТКС и формулируются предложения по применению методов оценки рисков информационной безопасности; в работе [85] разработан метод синтеза нелинейных дискретных сигналов в конечных полях; в работе [84] разработан метод синтеза всей системы нелинейных дискретных сигналов в конечных полях; в работе [60] разработан метод синтеза производных нелинейных дискретных сигналов в конечных полях и приводятся результаты исследований корреляционных, ансамблевых и структурных свойств этих сигналов; в работе [77] приводится анализ возможных внутренних воздействий (угроз) на ТКС и формулируются предложения по применению методов защиты от воздействий; в работе [7] проведен сравнительный анализ методов оценки воздействия на ТКС и разработаны предложения по применению методов оценки воздействий на основе теории нечетких множеств; в работе [79] проведены исследования методов поиска и противодействия внешним воздействиям на ресурсы ТКС; в работе [73] исследованы методы генерации случайных и псевдослучайных последовательностей для реализации динамического режима функционирования ТКС; в работе [62] определены критерии и показатели синтеза систем сигналов с заданными свойствами для использования сигналов в защищенной ТКС; в работе [80] вводятся и обосновываются показатели оценки защищенности ТКС от внешних и внутренних угроз; в работе [75] приводится анализ угроз информационной безопасности, помехозащищенности, энергетической и структурной скрытности ТКС, обосновываются показатели защищенности и методы противодействия от

соответствующих угроз, в том числе, на уровне источника сложных сигналов; в работе [98] введены показатели и критерии оценки решения одной из задач теории оптимального приема сигналов - оценка параметров сигналов, а именно, задержки сигнала, выдвигаются требования относительно корреляционных свойств сигналов синхронизации; в работе [76] разработан метод генерации псевдослучайных последовательностей символов, который может быть использован для реализации динамического режима функционирования канала ТКС; в работе [100] предложены показатели оценки защищенности информации от внешних угроз, и предложены меры и методы противодействия угрозам нарушения целостности и конфиденциальности данных абонентов ТКС; в работе [91] разработан метод построение генератора псевдослучайных последовательностей на основе параллельных вычислений с использованием графических процессоров и приводятся показатели статистических свойств данного метода; в работе [105] приведен сравнительный анализ систем обнаружения и перекрытия несанкционированных воздействий на ресурсы ТКС, сформулированы предложения по применению методов и средств противодействия в современных ТКС; в работе [63] разработан метод синтеза нелинейных криптографических дискретных сигналов с заданными свойствами; в работе [64] разработан усовершенствованный метод информационного обмена информации на основе динамического изменения соответствия: бит сообщения - сложный сигнал, определены необходимые и достаточные условия обеспечения в ТКС показателей помехозащищенности и информационной безопасности; в работе [109] определены критерии и показатели свойств генераторов случайных (псевдослучайных) последовательностей символов, используемых для формирования дискретных сигналов и генераторов управляющих сигналов в ТКС; в работе [101] приводится анализ международных стандартов в области управления информационной безопасностью и сформулированы предложения по применению международных стандартов при создании систем защиты информации для различных приложений ТКС; в работе [69] предложены возможные сферы использования нелинейных сигналов в приложениях ТКС; в работе [57] приводятся результаты исследований свойств нелинейных дискретных сигналов, методы син-

теза которых разработаны в диссертационной работе; в работе [58] введены критерии и показатели оценки эффективности функционирования информационной системы и сформулированы предложения по реализации требуемых значений показателей на уровне источника сложных сигналов; в работе [59] проведен анализ возможности минимизации значений боковых лепестков функции неопределенности на основе синтеза нелинейных систем сигналов; в работе [81] представлены критерии оценки свойств генераторов псевдослучайных последовательностей для практического применения в качестве генераторов управляющих последовательностей при реализации динамического принципа передачи данных в ТКС; в работе [86] представлен метод синтеза системы нелинейных дискретных сигналов в базисе конечных полей Галуа; в работе [95] представлена разработанная в ходе исследований модель оценки рисков информационной безопасности в ТКС; в работе [97] приведен анализ методов обнаружения воздействий на ТКС и сформулированы предложения по практическому применению методов для критичных приложений систем; в работе [99] приведен анализ методов оценивания рисков информационной безопасности для ряда приложений ТКС; в работе [103] приводится характеристика и возможности разработанного в ходе исследований программного комплекса синтеза и исследования свойств новых классов сигналов; в работе [104] представлен разработанный метод оценки рисков информационной безопасности на основе ранжирования угроз; в работе [106] рассмотрена возможность применения математического аппарата нечеткой логики для оценивания рисков информационной безопасности; в работе [108] предложены принципы создания комплексных систем защиты информации современных ТКС.

Апробация результатов диссертации. Основные результаты исследований докладывались и были одобрены на 14 международных форумах и международных научно-технических конференциях: I-я международная конференция «Глобальные информационные системы. Проблемы и тенденции развития». – Харьков. ХНУРЭ. – 2006, [94]; XIII Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах. - Запорожье, 2010 г. Классический приватный университет, Запорожский нацио-

нальный технический университет, Академия наук высшей школы Украины. – 2010 [110]; XIII Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2010 [108]; Международная научно-практическая конференция «Перспективы развития информационных и транспортно – таможенных технологий в таможенном деле, внешнеэкономической деятельности и управлении организациями», г. Днепропетровск. – 2011 [78]; 14 -я Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2011 [99]; 4 –й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития». - Харьков, АНПРЭ. 2011 [58-59,86]; 15–я Юбилейная Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Киев. - 2012. [81,104]; 16-я Международная научно-практическая конференция. Киев. – 2013 [92]; Международная научно-техническая конференция «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2014). Харьков, ХНУ имени Каразина В.Н.- 2014 [97]; «РТ – 2014». 10-я международная научно – техническая конференция. Современные проблемы радиотехники и телекоммуникаций. - Севастополь, 2014) [95]; Пятая международная научно-техническая конференция «Современные направления развития информационно-коммуникационных технологий и средств управления». - Полтава: ПНТУ; Баку; ВА ЗС АР; Кировоград; КЛА НАУ; Харков; ДП «ХНДИ ТМ» - 2015 [93]; Научно-техническая конференция: Информационная безопасность Украины. г. Киев. - 2015 [82,103]; IV международная научно-техническая конференция «Защита информации и безопасность информационных систем», Львов. – 2015 [111].

Публикации. Результаты диссертации опубликованы в 73 научных работах (из них 13 выполнены без соавторства) [74,78,82-84,87,93-94,96,102,110-112,], в том числе, 1 – монография, 40 – статей, тезисы докладов и тексты выступлений опубликованы в 14 сборниках трудов международных форумов и международных научно-практических конференций. Результаты исследований отражены в отчетах

о НИР: «Обоснование требований, разработка и внедрение инфраструктуры электронной цифровой подписи в МОНУ» (№ Госрегистрации 0106U006221); «Направления, методы и средства совершенствования и развития национальной инфраструктуры открытых ключей (№Госрегистрации 0109U002573); «Развитие, стандартизация, унификация, совершенствование и внедрение инфраструктуры открытых ключей, включая национальную систему электронной цифровой подписи (ЭЦП)» (№Госрегистрации 0111U002628); «Анализ состояния, определение направлений развития, стандартизация, совершенствование, разработка и внедрение криптографических систем, включая систему электронной цифровой подписи (ЭЦП)» (№Госрегистрации 0113U000363); «Методы, системы и средства криптографической защиты информации с гарантированным уровнем стойкости и повышенным быстродействием» (№Госрегистрации 0115U002431); «Математическое и компьютерное моделирование информационных процессов в сложных естественных и технических системах" (№Госрегистрации 0112U002098).

Диссертация содержит введение, шесть разделов, выводы, список использованных источников, шесть приложений. Полный объем диссертации составляет 436 страниц, в том числе 10 страниц рисунков и таблиц, 17 страниц списка использованных источников в количестве 150 наименований, 123 страниц приложений. Автор выражает глубокую признательность научному консультанту профессору И.Д. Горбенко, заведующему кафедрой безопасности информационных систем и технологий ХНУ им. В. Н. Каразина профессору Рассомахину С.Г. за бесценную помощь и полезные советы при написании и оформлении работы.

РАЗДЕЛ 1
СОСТОЯНИЕ ПРОБЛЕМЫ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

1.1 Анализ защищенности информационного обмена в телекоммуникационных системах в условиях внутренних и внешних воздействий

Информационный обмен в ряде приложений телекоммуникационных систем осуществляется условиях внутренних и внешних негативных воздействий [75,77,97,104]. Примером внутренних воздействий являются помехи, создаваемые соседними станциями многопользовательских систем. Внешние воздействия, связывают с преднамеренными помехами, создаваемыми станцией противодействия. При этом станция – постановщик преднамеренных помех, ставит перед собой, в том числе, цели лишить легальные станции надежного информационного обмена и минимизировать собственные затраты. Задача построения защищенной ТКС – создать систему, устойчивую к воздейсвию множества различны, актуальных для данной системы, воздействий (помех) [48,108,110]. При решении указанной задачи, необходимо априори полагать, что станции противодействия известны основные параметры системы (частотный диапазон, время сеансов связи, объем передаваемой информации, класс сигналов-переносчиков данных и др.). Информационный обмен должен быть организован таким образом, чтобы единственной стратегией станции противодействия была стратегия подавления системы путем постановки заградительной помехи.

Будем полагать, что в канале действует наиболее характерный вид помехи, описываемый гауссовским случайным процессом, спектр которого перекрывается со спектром сигнала. В этом случае, вероятность ошибки зависит только от отношения мощности сигнала к общему мешающему воздействию. Необходимо подчеркнуть, что в ряде случаев возможность аппроксимации помехи гауссовским законом не так очевидна, поскольку показатели качества решения таких задач, как

оценка параметров, М – ичная передача, зависят не только от отношения указанных мощностей.

Вероятность ошибки в канале связи является функцией помех. Причем помеха представляет собой сумму теплового шума (N_0) и помехи, создаваемой станцией противодействия. Таким образом, отношение сигнал /шум можно записать как $(E/(N_o + N_п))$ где $N_п$ - спектральная плотность мощности преднамеренных помех. Будем полагать, что

$$N_п = \frac{P_п}{F}, \qquad (1.1)$$

где $P_п$ – мощность преднамеренных помех; F – ширина полосы частот сигнала.

Как правило, мощность станции – постановщика помех значительно больше мощности теплового шума. Поэтому величину отношения сигнал/шум принимают равной $\frac{E_с}{N_0}$. Известно, что энергия сигнала определяется из соотношения [51]

$$E_с = P_с T = \frac{P}{R}, \qquad (1.2)$$

где: P – мощность полезного сигнала; T – время передачи бита; R – скорость передачи данных (бит/с).

Тогда требуемое, для обеспечения заданного значения вероятности ошибки в канале, отношение энергии бита данных к спектральной плотности мощности помехи, может быть найдено из соотношения:

$$(\frac{E_с}{N_п})_{треб.} = (\frac{P/R}{P_п/F})_{треб.} = (\frac{F/R}{P_п/P_с})_{треб.} = \frac{B}{(P_п/P_с)_{треб.}}, \qquad (1.3)$$

где $B = F/R$ – коэффициент расширения спектра сигнала (база сигнала).

Отношение мощности помехи к мощности сигнала может быть записано в виде:

$$(\frac{P_п}{P_с})_{треб.} = \frac{B}{(E_с/N_п)_{треб.}}, \qquad (1.4)$$

Выражение (1.4) можно интерпретировать следующим образом. В целях подавления сигналов станция постановщик помех стремиться увеличить значение

$(\frac{E_с}{N_п})_{треб.}$ посредством уменьшения $N_п$. Указанное приводит к уменьшению значения $(\frac{P_п}{P_с})_{треб.}$. Однако защищенная система в этом случае может прибегнуть к увеличению базы сигнала, усложняя задачу станции противодействия по постановке помех.

Рассмотрим воздействие преднамеренной помехи в виде заградительной помехи (помеха в виде стационарного гауссова шума с нулевым средним и равномерным распределением спектральной плотности мощности, по крайней мере, в области частот, занимаемой сигналом). Спектральная плотность мощности энергии станции противодействия равна

$$N_{п\ =}P_п\ /\ F, \tag{1.5}$$

где F – ширина полосы диапазона, в которой создаются помехи.

Вероятность ошибки на бит сообщения P_0 при некогерентной обработке сигнала равна [51]

$$P_0 = Q(\frac{\sqrt{2E_c}}{N_0}), \tag{1.6}$$

где Q - интеграл вероятности.

Полная спектральная плотность мощность, вследствие наличия помех, увеличивается до значения $N_0 + N_п$. Тогда средняя вероятность ошибки на бит сообщения при когерентной обработке при наличии широкополосного шума равна

$$P_0 = Q\left(\frac{\sqrt{2E}}{N_0 + N_п}\right) = Q(\sqrt{\frac{2E / N_0}{1+\left(\frac{E}{N_0}\right)(\frac{P_п}{P_с}) / B}}) \tag{1.7}$$

Графики зависимости P_0 от $\frac{E_0}{N_0}$ при фиксированном отношении $\frac{P_п}{P_с}$ приведены на рис. 1.1 [31]. Анализ приведенных на рисунке кривых показывает, что вероятность ошибки существенно может быть уменьшена при увеличении коэффициента расширения спектра сигнала.

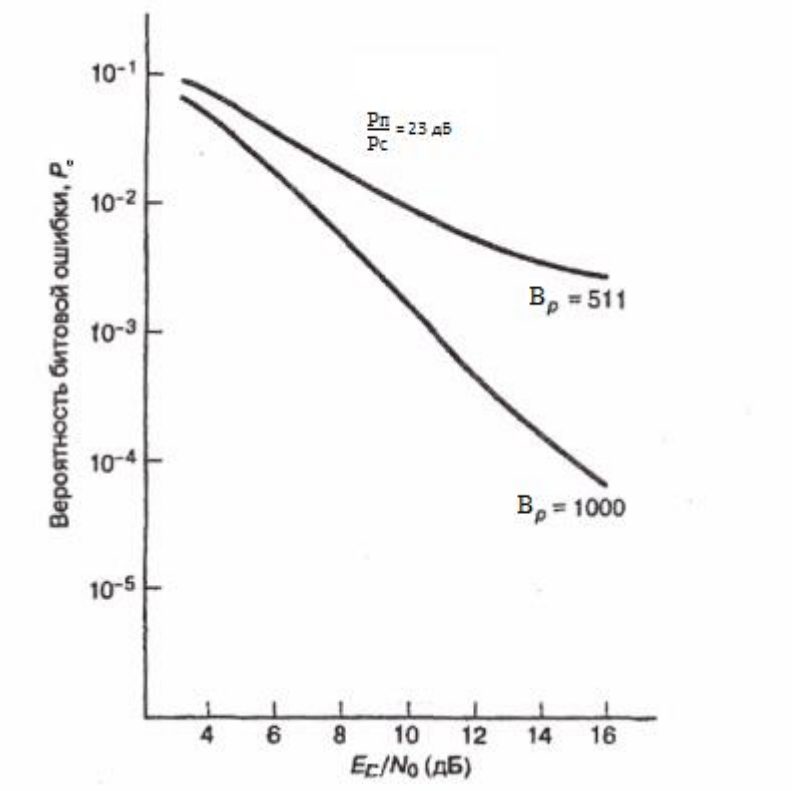


Рис. 1.1 Графики зависимости вероятности ошибки (P_0) от $\frac{E_c}{N_0}$

Весьма характерной ситуацией для практики мешающего воздействия на функционирование телекоммуникационной системы, является узкополосная помеха. Причем данный тип помех может быть реализован как станцией противодействия в целях нарушения работы системы, так и соседствующими станциями, создающими помехи вследствие своего обычного функционирования. Оптимальной процедурой обработки сигнала в этом случае, можно считать фильтрацию, согласованную с мешающим воздействием (абелевый белый гауссовский шум и узкополосная помеха). Такая обработка эквивалентна вырезанию частотного интервала, в котором сосредоточена помеха. При этом вырезаются и частотные компоненты сигнала в пределах полосы помехи. Согласованный фильтр обеспечивает выходное отношение мощностей сигнала и шума (q_j^2) в виде [31]:

$$q_j^2 = q^2 (1 - \frac{W_j}{W}), \qquad (1.8)$$

где $q^2 = \frac{2E}{N_0}$ - отношение мощностей сигнала и шума на выходе согласованного фильтра в отсутствие помехи.

Как отмечалось раньше, при воздействии на ТКС узкополосной помехи методами защиты является режекторная фильтрация части спектра, на которую воздействует помеха, кроме того, возможно реализовать передачу данных путем переноса его спектра в диапазон частот, свободный от воздействия помех.

Станция противодействия, стремясь нарушить функционирование системы, может применить так называемую заградительную шумовую помеху, спектр которой полностью покрывает спектр сигнала. При этом станция противодействия, в целях обеспечения наилучшего эффекта подавления, будет стремиться обеспечить значительное превышение спектральной плотности мощности помехи над спектральной плотностью мощности шума ($P_п \gg N_0$). В этом случае

$$q^2 = \frac{2P(WT)}{P_п}. \qquad (1.9)$$

Из (1.9) следует, что при ограничениях на максимальную мощность сигнала и мощность помехи, создаваемой станцией противодействия, единственной возможностью противостоять заградительной помехе, является привлечение широкополосной технологии, т.е. сигналов со значительным частотно-временным ресурсом (базой сигналов).

Анализ воздействия различных видов помех на ТКС показывает, что выигрыш в отношении сигнал / помеха (определяющего помехоустойчивость приема сигналов) на входе решающего устройства приемника пропорционален базе используемых для передачи данных сигналов (при наложении ограничения на пиковую мощность сигнала). Другими словами, чем больше база сигнала, тем больше отношение сигнал/ помеха, тем сильнее подавляется помехам.

Приведенные выше результаты справедливы для случая, когда помеха является нормальным случайным процессом и обладает равномерной спектральной плотностью. Станция противодействия для подавления системы может использовать мощные структурные помехи с неравномерным спектром. В таких условиях

функционирования ТКС помехоустойчивость в значительной мере определяется подобием (различием) структур сигнала и помехи, т.е. тем, как подавляются отдельные элементы сигнала помехой.

Известно, что коэффициент передачи согласованного фильтра определяется следующим выражением [51]

$$k(\omega) = \frac{cg(\omega)}{N(\omega)}, \qquad (1.10)$$

где: c – постоянная; $g(\omega)$ – спектр сигнала.

Отношение сигнал / помеха при этом определяется выражением

$$q^2 = \frac{2}{\pi}\int_0^{\infty}\frac{|g(\omega)|^2}{N(\omega)} \qquad (1.11)$$

Приведенные соотношения (1.10) - (1.11) указывают на стратегию действий станции постановщика помех и защищенной системы. Помеха, создаваемая постановщиком помех, должна конструироваться таким образом, чтобы выполнялось равенство $N(\omega) = a|g(\omega)|$, где a – постоянная величина. Последнее равенство означает следующую стратегию: сильнее подавлять те спектральные составляющие, которые переносят большую часть энергии сигнала. Путем снижения усиления согласованного фильтра в области резких пиков в спектре помехи осуществляется исключение этой части спектра. Если имеет место «провал» в спектре помехи, то посредством увеличения усиления согласованного фильтра (согласно (1.10)), возможно повышение отношения сигнал / помеха (1.3). Таким образом, помехоустойчивость системы не снижается вследствие воздействия на систему помехи с неравномерным спектром.

Большинство приложений ТКС относятся к многопользовательским системам. В таких системах, вследствие работы большого числа абонентов в общем частотном диапазоне, возникают помехи множественного доступа или взаимные помехи. Рассмотрим влияние взаимной помехи на помехоустойчивость приема данных в ТКС. Пусть ширина общей полосы частот системы равна F. Предположим, что ширина спектра всех сигналов в ТКС равна ширине общей полосы ча-

стот, и все активные абоненты создают на входе j-го приемника сигналы одинаковой мощности P_c. В этом случае мощность взаимной помехи, создаваемой l мешающими абонентами, будет равна $l\ P_c$. Допустим, что спектральная плотность мощности взаимной помехи постоянна в пределах общей полосы частот

$$N_п = \frac{lP_c}{F}, \qquad (1.12)$$

и взаимная помеха по своим статистическим свойствам приближается к нормальному случайному процессу. Таким образом, сделанные предположения позволяют считать взаимную помеху нормальным случайным процессом с ровномерной спектральной плотностью мощности.

Нетрудно убедиться, что отношение сигнал/шум на входе решающего устройства приемника определяется из выражения

$$q^2 = \frac{B}{l}, \qquad (1.13)$$

где:

$$B = FT = FR \qquad (1.14)$$

B- база сигнала, приходящаяся на одну двоичную единицу;

R - скорость передачи информации.

Из (1.13) следует, что при заданном числе активных абонентов $l_a = l+1$ увеличение помехоустойчивости возможно только за счет увеличения базы (B) сигналов. Это объясняется тем, что с увеличением базы (с увеличением ширины спектра сигналов при постоянной скорости передачи информации R) уменьшается спектральная плотность мощности помехи $N_п$. Принципиально увеличение базы позволяет получить сколь угодно высокую помехоустойчивость приема информации в ТКС.

В практике работы ТКС возможны случаи, когда мощность одного или нескольких мешающих сигналов во много раз больше мощности полезного сигнала. Каким образом в этих условиях обеспечить необходимую помехозащищенность.

Пусть мощность полезного сигнала P_c, а мощность мешающей составляющей $P_п$. Мощность сигнальной составляющей на выходе согласованного фильтра в момент принятия решения (отсчета) пропорциональна P_c, а мощность мешающей составляющей $P_п R_{jk}^2(\tau)$, где R_{jk}^2 – взаимнокорреляционная функция (ВКФ) полезного k- го сигнала и j-го мешающего. Величина τ определяется смещением ВКФ относительно момента отсчета. Отношение сигнал-помеха на выходе устройства оптимального приема будет равно [51]:

$$q^2(\tau) = \frac{P_c}{P_п R_{jk}^2(\tau)}. \qquad (1.15)$$

Наименьшее отношение сигнал-помеха будет равно

$$q^2(\tau) = \frac{P_c}{P_п R_{max}^2(\tau)}, \qquad (1.16)$$

где $R_{макс}$ - есть максимальное значение $R_{jk}(\tau)$.

Очевидно, что для повышения помехозащищенности ТКС необходимо выбирать сигналы, у которых максимальные пики ВКФ минимальны.

Если максимальные пики ВКФ уменьшены до среднеквадратического уровня $\sigma_{j,k} = \sigma^2$, то отношение сигнал/помеха будет равно

$$q^2(\tau) = \frac{P_c}{P_п}\ \sigma^2. \qquad (1.17)$$

Например, если: $\sigma^2 = \frac{1}{2FT}$, то

$$q^2 = \frac{P_c}{P_п} 2FT, \qquad (1.18)$$

где FT = B – база сигнала.

Для дискретных фазоманипулированных сигналов $\sigma^2 = \frac{1}{2N}$ (N – число элементов сигнала). Для таких сигналов

$$q^2 = \frac{P_c}{P_п} 2N. \qquad (1.19)$$

Из формул (1.18) - (1.19) следует, что увеличение базы сигнала увеличивает q^2 (а значит, - помехоустойчивость системы) и может компенсировать уменьшение отношения $\frac{P_c}{P_п}$ в случае увеличения станцией противодействия мощности помехи ($P_п$).

При радиоэлектронном противодействии эффективная помеха может быть организована только после обнаружения присутствия противостоящей системы в эфире и оценки таких ее параметров как частотный диапазон, занимаемая полоса, формы используемых сигналов.

Однако станции противодействия могут быть неизвестны заранее сведения о частотном диапазоне и интервале времени, занимаемом сигналом. Учитывая эти обстоятельства, его стратегия будет заключаться в решении задачи обнаружения сигнала либо путем сканирования частотно-временной области, либо в использовании набора параллельных каналов, каждый из которых ответственен за анализ ограниченного участка частотно-временной области. В любом случае качество работы приемника системы-перехватчика будет полностью определяться характеристикой энергетического детектора [15], настроенного на истинную для перехватываемого сигнала частотно-временную зону. Единственной причиной, вынуждающей перехватчик прибегнуть к такому неэффективному инструменту как энергетический приемник, является отсутствие информации о структуре обнаруживаемого сигнала, т.е. используемой формы сигнала (закона модуляции). По этой причине перехватчик не может обрабатывать сигнал аналогично приемнику скрытной системы (т.е. осуществлять согласованную фильтрацию). Очевидно, что в случае недостаточной структурной сложности (скрытности) сигнала и осведомленности перехватчика о его возможных альтернативных вариантах, перехватчик может попытаться их все реализовать. Изложенное выше позволяет утверждать, что для предотвращения возможности обнаружения своего сигнала станцией противодействия телекоммуникационная система должна использовать сигналы с распределенным или широким спектром, которые обладают максимально возможным зна-

чением выигрыша от обработки (произведение полосы частот, занимаемой сигналом на его длительность), и практически не раскрываемой структурой.

1.2 Выбор критериев оценки и показателей эффективности современных телекоммуникационных систем

К ТКС предъявляются все более жесткие требования по обеспечению эффективности их функционирования в условиях сложных внешних и внутренних воздействий: естественные и преднамеренные помехи; помехи от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот; попытки проведения криптографического анализа и нарушения целостности (аутентичности) данных пользователей и др.

Под эффективностью телекоммуникационных систем понимают способность выполнять задачи, стоящие перед системой в заданных условиях. К основным показателям эффективности функционирования ТКС относят: пропускную способность, помехозащищенность, производительность, информационную безопасность, живучесть, своевременность доставки сообщений и др.

Под помехозащищенностью ТКС следует понимать ее способность выполнять задачи в условиях радиоэлектронного подавления (РЭП) со стороны станции противодействия [142]. В целом ряде случаев, РЭП включает радиотехническую разведку и радиопротиводействие. Радиотехническая разведка предполагает установление факта работы ТКС и определение ее параметров (частотный диапазон, занимаемая полоса, закон модуляции, интервал времени, занимаемый сигналом и др.), необходимых для радиопротиводействия. Целью радиопротиводействия является создание условий (например, путем постановки помех), затрудняющих работу ТКС. Очевидно, что постановка помех будет тем эффективнее, чем больше информации выявит станция противодействия о параметрах системы.

Поскольку в качестве критерия эффективности понимается вероятность выполнения задач, стоящих перед системой [114], то в качестве критерия помехозащищенности целесообразно использовать вероятность выполнения функций (за-

дач) системой (например, заданной скрытности функционирования), в условиях РЭП.

Если станция противодействия может осуществить обнаружение факта работы ТКС и параметров сигнала с вероятностью $P_р$, и реализовать нарушение работы ТКС в результате радиопротиводействия с вероятностью $P_н$, для оценки помехозащищенности можно использовать показатель $P_{пз}$ [142]:

$$P_{пз} = 1\text{-}P_р P_н . \qquad (1.20)$$

Вероятность $P_н$ зависит от возможности работы ТКС в условиях действия помех. Поэтому величина $P_{пу} = 1 - P_н$ может быть принята в качестве показателя помехоустойчивости приема сигналов-переносчиков данных.

Таким образом, помехозащищенность ТКС определяется помехоустойчивостью и скрытностью ее функционирования. Под помехоустойчивостью понимают способность системы противостоять воздействию мощных помех.

В качестве показателя помехозащищенности ТКС можно также использовать вероятность подавления радиоканала $(P_{под.})$, которая определяется из соотношения [142]:

$$P_{под.} = P_р P_{оп} + \left(1 - P_р\right) P_{уп} , \qquad (1.21)$$

где: $P_р$ – вероятность разведки параметров сложного сигнала;

$P_{оп}$ – вероятность применения «оптимальной» помехи, т.е. помехи со структурой и энергией близкими к структуре и энергии излучаемого сигнала;

$P_{уп}$ – вероятность применения станцией противодействия помехи (в дальнейшем – универсальной), мощность которой существенно превышает мощность излучаемого сигнала, а полоса частов, в которой сосредоточена помеха, полностью перекрывает спектр, отведенный для передачи данных пользователей системы.

Анализ показывает, что возможности подавления радиоканала универсальной или заградительной помехой ограничены. В таком случае, как следует из выражения (1.21), вероятность подавления системы в значительной степени определяется защищенностью системы от воздействия оптимальных помех, создаваемых

станцией противодействия. В свою очередь постановка такого рода помех зависит от энергетической, структурной и временной скрытности функционирования системы.

Помехозащищенность ТКС будет обеспечена при условии [141-142]:

$$\left(P_{пер}G_{пер}\right)\left(\frac{G_{пр}}{G_{пр_i}}\right)\left(\frac{L_i}{L_l}\right)\left(\frac{1}{K_з}\right)\left[\frac{\sigma R}{F}\frac{2E}{N_п}\right]^{-1} = P_{пер_i}G_{пер_i}, \qquad (1.22)$$

где: $P_{пер}$, $P_{пер_i}$ - мощность передатчика системы и передатчика помех; $G_{пер}$, $G_{пр}$ - коэффициент усиления передающей и принимающей антенн; $G_{пер_i}$, $G_{пр_i}$ - коэффициент усиления передающей и принимающей станции противодействия; L_i, L_l - затухание в среде до станции противодействия; $K_з$ - коэффициент запаса по мощности; $R = 1/T$ - скорость передачи информации (бит/с); F - полоса частот сигнала; E - энергия сигнала; $N_п$ - спектральная плотность мощности помехи ($N_п = P_{пер_i}G_{пер_i}G_{пр_i}\frac{\sigma}{FL_i}$) , где $\sigma = R\,B$ (R - коэффициент взаимной корреляции сигнала и помехи).

Из (1.22) следует, что улучшение помехозащищенности достигается увеличением базы сигнала, а также улучшением направленности антенн передатчика и приемника.

Помехозащищенность ТКС в условиях воздействия помех, преднамеренно создаваемых станцией противодействия, зависит от скрытности выбора и использования параметров системы. При этом под скрытностью системы в целом и скрытностью используемых системой параметров, будем понимать способность ТКС противостоять мерам радиотехнической разведки, направленным на обнаружение факта работы системы (энергетическая скрытность) и определения необходимых для радиопротиводействия параметров сигнала (структурная и информационная скрытность).

Скрытность функционирования системы предполагает способность системы функционировать в режиме, затрудняющим обнаружение факта передачи сообще-

ний и оценку их параметров станцией противодействия. Другими словами скрытность может быть обеспечена за счет:

- энергетической скрытности, характеризующей способность противостоять мерам, направленным на обнаружение сигналов станцией противодействия;

- структурной скрытности используемых сигналов, при которой достоверное предсказание сигналов или их символов по известным предыдущим символам невозможно;

- трудности отождествления принятых сигналов с сообщением, которое передается (информационная скрытность).

Энергетическую скрытность радиоканала определим как способность функционировать с таким энергетическим потенциалом, которого недостаточно для того, чтобы станция противодействия осуществляла перехват и прием информации с требуемой достоверностью:

$$S_э = P\left(E / N_0 < G_{треб.}\right), \tag{1.23}$$

где: E / N_0 – отношение энергии сигнала к спектральной плотности мощности шума на входе решающего устройства станции противодействия;

$G_{треб}$ – требуемое значение отношения E / N_0 для приема данных с требуемыой достоверностью.

Другими словами, энергетическая скрытность радиоканала может быть определена как вероятность того, что отношение сигнал-шум на входе решающего устройства приемника станции противодействия не превысит требуемого значения, необходимого для обнаружения сигнала.

Условие перехвата сигнала станцией противодействия определим в виде [142]:

$$\underbrace{\left(\frac{G_{пр}}{T^0}\right)}_{1}\underbrace{\left(\frac{G_{пер}}{G_{пер_i}}\right)}_{2}\underbrace{\left(\frac{L_i}{L_l}\right)}_{3}\underbrace{\left(\frac{1}{R_з}\right)}_{4}\underbrace{\left[\frac{1}{\left(\frac{2E}{No}\right)\frac{1}{T}\left(\frac{T_и}{F}\right)}\right]}_{5} \leq \underbrace{\left(\frac{G_{пр_i}}{T_i^o Z_o}\right)}_{6} \tag{1.24}$$

где: 1 – характеристика приемника; 2 – характеристики передающей антенны; 3 – потери в линии; 4 – запас по энергетике; 5 – характеристики модуляции; 6 - риск перехвата.

Выражение (1.24) позволяет оценить условие энергетической скрытности ТКС в зависимости от ее параметров и характеристик станции противодействия. Из (1.24) следует, что при увеличении базы сигнала, энергетическая скрытность системы возрастает.

Структурная скрытность характеризует способность ТКС противостоять мерам станции противодействия, направленным на отождествление обнаруженного сигнала с одним из множества априорно известных сигналов (распознаванием формы сигнала, определяемой способами его кодирования и модуляции). Для определения структурной скрытности радиоканала рассмотрим пространство состояний сигналов $\{S_w\}$ – переносчиков информации. Будем полагать при этом, что пространство состояний радиоканала есть $A = \{A_1, A_2, \ldots A_i, \ldots A_n\}$, где A_i – размерность A_i –го параметра сигнала. Скрытность функционирования такого канала можно оценить энтопией

$$S_A = -\sum_{i=1}^{A} P(A_i) \log P(A_i), \qquad (1.25)$$

где $P(A_i)$ – вероятность нахождения радиоканала в A_i - м состоянии.

Степень неопределенности, задаваемая соотношением (1.25), т.е. скрытность функционирования радиоканала, уменьшается после перехвата сигналов, передаваемых через канал. В качестве меры количества информации, получаемой после перехвата, можно принять величину $I(A, W)$, характеризующую степень уменьшения неопределенности состояния радиоканала после перехвата X сигналов:

$$\begin{aligned} I(A, W) &= S_A + \sum_{j=1}^{X} \sum_{i=1}^{A} P(W_j) P(A_i / W_j) \log P(A_i / W_j) = \\ &= -\sum_{i=1}^{A} P(A_i) \log P(A_i) + \sum_{j=1}^{X} \sum_{i=1}^{A} P(W_j) P(A_i / W_j) \log P(A_i / W_j), \end{aligned} \qquad (1.26)$$

где слагаемое $\sum_{j=1}^{X} \sum_{i=1}^{A} P(W_j) P(A_i / W_j) \log P(A_i / W_j) = S(A)$ определяет условную апостериорную энтропию радиоканала: источника сигналов; источника, определяющего закон выбора сигналов для излучения; источника сообщений, после пере-

хвата X W_j сигналов. Из (1.26) следует, что если $S(A)=0$, т.е. $I(A,W)= S_A$, то станция противодействия получает всю необходимую ему информацию об источнике сигналов (система не обладает скрытностью). Если же $S(A)=S_A$, т.е. $I(A,W)=0$, то радиоперехват сигналов оказывается безрезультатным, в том смысле, что станция противодействия не получает никакой дополнительной информации, кроме известной ей а приори о ТКС.

Выполнение равенства $S(A) = S_A$ и условия (1.26), на наш взгляд, является принципиально важными для решения проблемы обеспечения информационной безопасности ТКС на уровне источника сложных сигналов, не прибегая к созданию традиционных систем и средств криптографической защиты информации.

В случае, если в радиоканале осуществляется смена (по определенному закону) форм сигалов и частот, на которых излучают данные сигналы, то выражение (1.26) примет вид

$$S_A = -\sum_{j=1}^{H}\sum_{i=1}^{U} P_{ji}\log P_{ji}, \qquad (1.27)$$

где P_{ji} – совместная вероятность использования i – й формы сигнала из множества U на j несущей частоте из множества частот H.

Выражения (1.25) – (1.27) характеризуют степень неопределенность состояния радиоканала. При этом данные выражения не могут быть использованы для получения показателей структурной скрытности используемых форм сигналов.

Введем понятие структурной скрытности сложного сигнала в виде соотношения:

$$S_{cc} = \frac{\prod_{i=i}^{K} M_i^*}{\prod_{i=i}^{K} M_i}, \qquad (1.28)$$

где M_i^* – число координат сложного сигнала, которые необходимо знать для того, чтобы определить оставшиеся $M_i - M_i^*$ координаты.

Для случая использования в системе фазоманипулированных сигналов, выражение (1.28) примет вид

$$S_{cc} = \frac{l}{L}, \qquad (1.29)$$

где l – число символов, которое необходимо знать, для определения правила (закона) формирования оставшихся L – l символов.

Информационная безопасность ТКС – это способность системы обеспечивать защиту от уничтожения, модификации, блокирования информации, ее несанкционированной утечки или нарушения установленного порядка ее маршрутизации. Под информационной безопасностью следует понимать состояние защищенности систем обработки и хранения данных, при котором обеспечено сохранение конфиденциальности, целостности и доступности информации; кроме того, могут учитываться другие свойства, такие, как аутентичность, отслеживаемость, неопровержимость и надежность [56].

Одной из составляющих информационной безопасности является информационная скрытность (ИС) телекоммуникационной системы. Под ИС системы будем понимать ее способность скрывать смысловое содержание сообщений, способы формирования сообщений (сигналов), сам факт передачи сигналов. В качестве критериев оценки информационной безопасности используют, так называемое, безопасное время ($T_{без.}$) и расстояние единственности (РЕ) [54,56,112].

Безопасное время – это математическое ожидание времени раскрытия системы защиты посредством перебора всех возможных вариантов построения системы. При анализе защищенности системы (ее стойкости к раскрытию) рассматриваются наиболее благоприятные условия, состоящие в том, что станции противодействия (криптоаналитику) известны все параметры преобразования данных, за исключением используемых в данный момент времени ключевых данных. При таких условиях, единственно возможной стратегией станции противодействия является статистическое опробывание (перебор) всех возможных вариантов построения системы защиты (ключевых данных), а $T_{без.}$ – среднее время, затрачиваемое на перебор.

Критерий оценки информационной скрытности может быть записан в виде:

$$T_{без.} = N / K\gamma \qquad (1.30)$$

где: γ – производительность системы, осуществляющей попытки получения доступа к содержанию сообщения, измеряемое числом переборов в секунду; N – число возможных вариантов установления соответствия: бит сообщения - сложный сигнал; $K = 3{,}1 \cdot 10^7$.

Расстояние единственности указывает на объем данных (сигналов), которые необходимо знать (перехватить) станции противодействия, чтобы посредством анализа этих данных получить единственно верное решение о содержании сообщения.

Еще одной составляющей (наряду с информационной скрытностью) информационной безопасности является система имитозащиты (обеспечение целостности) информации. Под имитозахищенностью понимают комплекс организационно - технических мероприятий и средств, а также законодательных норм, которые направлены на обеспечение определенного уровня имитостойкости.

Математический аппарат системы имитозащиты включает криптографический алгоритм имитозащищенного кодирования информации (это может быть алгоритм шифрования, код аутентификации, либо другое преобразование) и алгоритм принятия решения об истинности полученной информации, а также ключевую систему.

По сути имитостостойкость является сложной услугой, которая обеспечивается предоставлением таких услуг как целостность, подлинность, (аутентичность), а также применением различных криптографических протоколов с определенными свойствами [89] .

В дальнейшем под имитостойкостью будем понимать способность криптографической системы, применяемой в ТКС, противостоять навязыванию нарушителем ложных сообщений и данных, их модификации с применением каких-либо способов и средств, в том числе, средств установления подлинности (аутентичности), целостности информации и данных [90]. По сути имитостойкость определяет способность получателя проверить, что полученные сообщения или данные не изменены третьей стороной, не являются повтором ранее переданного сообщения или фальшивым сообщением, созданным третьей стороной. Основным методом обеспечения имитостойкости является внесение в сообщение избыточности, которая

может формироваться в виде контрольных сумм, избыточных символов кодов, которые определяют ошибки, криптографических контрольных сумм (кодов аутентификации сообщений - имитовставок) и др. В качестве показателей имитостойкости могут быть использованы сложность процедур и вероятность навязывания неправдивой (ложной, модифицированной и т.д.) информации, с учетом методов и вычислительных мощностей средств, используемых злоумышленником.

К настоящему времени разработан ряд критериев оценки имитостойкости и методов ее обеспечения. В основном они ориентированы на обеспечении имитостойкости на уровне использования средств криптографической защиты информации и избыточного кодирования. В тоже время, как показали исследования [111-112], обеспечить требуемую в ТКС имитостойкость возможно на уровне источника сложных сигналов за счет увеличения размерности пространства сигналов, степени коррелированности между ними, сложности законов их построения, а также размерности пространства параметров сигналов, относительно которых создается неопределенность. Имитостойкость системы на сигнальном уровне обеспечивается за счет: использования сигналов со сложной структурой, по своим свойствам близким к свойствам случайных последовательностей; изменением (через определенные промежутки времени) параметров сигналов; использованием сигналов с нелинейными законами формирования.

В соответствии с приведенными определениями имитостойкости и имитозахищенности, для их количественной оценки и анализа может быть применена теория аутентификации Дж. Симонса [56]. Симонс показал, что вероятность обмана может быть вычислена по формуле:

$$\log_2 P_{обм} \geq -\Delta I(C,K). \qquad (1.31)$$

Найдем из (1.31) $P_{обм}$:

$$P_{обм} \geq 2^{-\Delta I(C,K)}. \qquad (1.32)$$

Выражение (1.32) означает границу вероятностей обмана в системе. Проведем анализ выражения (1.32).

1. Криптосистемы, в которых достигается равенство (1.32), относят к

системам, обладающим абсолютной имитостойкостью.

2. Для уменьшения вероятности обмана необходимо увеличивать $\Delta I(C,K)$, то есть количество информации, вводимой в криптограмму о ключе аутентификации.

3. Вероятность обмана

$$P_{обм} \geq 2^{-l_i}, \qquad (1.33)$$

где l_i - длина имитовставки (кода аутентификации, размерность сигнального пространства).

На уровне источника сигналов (на физическом уровне) имитостойкость (I_c) зависит от размерности пространства сигналов M, числа разрешенных к использованию в интервале времени t сигналов Z, числа попыток навязывания (имитации) C и политики навязывания X:

$$I_c = F\left(M, Z, C, X\right); \qquad (1.34)$$

$$I_c = C/Z, \text{ если } 1 < C < Z \text{ и } I_c = 1, \text{ если } C > Z. \qquad (1.35)$$

$$I_c = 1 - P_{нав}. \qquad (1.36)$$

$$P_{нав}. = C/M. \qquad (1.37)$$

Помехоустойчивость - характеризует способность ТКС функционировать в условиях воздействия на систему различных помех и определяется отношением, связывающим отношение сигнал-помеха на выходе приемника (на входе согласованного фильтра или коррелятора q^2) с отношением сигнал-помеха на входе приемника ρ^2 [140]:

$$q^2 = 2B\rho^2, \qquad (1.38)$$

где: $\rho^2 = \frac{P_c}{P_п}$ (P_c, $P_п$ – мощности сигнала и помехи соответственно); $q^2 = \frac{2E}{N_п}$ (E – энергия сигнала, $N_п = P_п / F$ – спектральная плотность мощности помехи в полосе F сигнала); B – база сигнала.

Помехоустойчивость ТКС характеризуется вероятностью ошибки ($P_{ош}$), которая, в свою очередь, определяется методами приема (когерентный, некогерентный прием) и используемыми для передачи данных сигналами. В частности при

когерентном приеме вероятность оибки при решении задачи различения сигналов определяется из соотношения [51]:

$$P_{ош} = 1 - F(H), \tag{1.39}$$

где: интеграл вероятности

$$F(x) = \frac{1}{\sqrt{2\pi}} \int_{x}^{\infty} \exp(\frac{-t^2}{2}) dt, \tag{1.40}$$

а аргумент

$$H = \sqrt{[(E_0 + E_1) / 2N_0](1 - R)}; \tag{1.41}$$

E_0, E_1 – энергии соответствннно сигналов $U_0(t)$, $U_1(t)$;

$$R = \frac{2}{E_0 + E_1} \int_{0}^{T} S_j(t) S_j(t) dt. \tag{1.42}$$

Коэффициент R с точностью до постоянной совпадает с коэффициентом корреляции сигналов $U_0(t)$, $U_1(t)$.

Анализ соотношений (1.39) - (1.42) показывает, что помехоустойсчивость приема сигналов определяется $\rho^2 = \frac{P_c}{P_п}$ и базой сигнала B. Причем величина q^2 может быть получена исходя из требований к системе с точки зрения помехоустойчивости приема, даже если $\rho^2 < 1$.

Соотношение (1.38) получено для помехи в виде гауссовского случайного процесса, обладающего равномерной спектральной плотностью мощности в пределах полосы частот, ширина которой равна ширине спектра сигнала. Вместе с тем, необходимо отметить, что во многих случаях эти условия не выполняются, например, при действии мощной структурной помехи. В этих случаях помехоустойчивость в значительной степени определяется степенью коррелированности (подобием и различием структур) сигнала и помехи, т.е. тем, как подавляются отдельные элементы сигнала помехой.

1.3 Концепция синтеза систем сигналов для приложений телекоммуникационных систем

Типичным для теории связи является подход, заключающийся в разработке оптимального приемного устройства, которое с наилучшим качеством восстановит информацию, содержащегося в наблюдаемом колебании. Определение оптимального алгоритма обработки, базирующегося на учёте специфических свойств переданного сигнала, позволяет синтезировать оптимальным образом и сам сигнал, т.е. выбрать наилучшим образом метод его кодирования и модуляции.

В теории связи наиболее распространённой моделью служит канал с аддитивным белым гауссовским шумом, в котором вероятность трансформации каналом заданного входного сигнала в то или иное выходное наблюдение $y(t)$ (переходная вероятность - $P\left[y(t)|S(t)\right]$) экспоненциально уменьшается с ростом квадрата Евклидова расстояния между переданным сигналом и выходным наблюдением [15]:

$$P\left[y(t)|S(t)\right] = k\exp\left(-\frac{1}{N_0}d(s,y)\right), \tag{1.43}$$

где k – константа, не зависящая от S(t) и y(t), N_0 - спектральная плотность мощности одностороннего белого шума; а Евклидово расстояние между S(t) и y(t) определяется как

$$d(S,y) = \sqrt{\int_0^T [y(t) - S(t)]^2 dt}. \tag{1.44}$$

Согласно соотношениям (1.43) и (1.44) похожесть сигнала (вероятность того, что он преобразован каналом в наблюдение y(t)) уменьшается с увеличением Евклидова расстояния между S(t) и y(t). В случае равной вероятности всех сообщений источника (что достигается при правильном проектировании системы) оптимальной стратегией наблюдателя, обеспечивающей минимальную ошибку перепутывания действительно переданного с некоторым другим сигналом, является правило (критерий) максимального правдоподобия (МП). Согласно данному ал-

горитму, после того, как колебание y(t) принято, решение принимается в пользу того сигнала, для которого вероятность трансформации его каналом в принятое наблюдение y(t) является наибольшим (по сравнению с вероятностями для других сигналов). С учётом изложенного, МП решение для гауссова канала может быть преобразовано в правило минимума расстояния

$$d\left(S_j, y\right) = \min d\left(S_i, y\right) \Rightarrow H_j, \tag{1.45}$$

т.е. решение принимается в пользу сигнала $S_j(t)$, поскольку он наиболее близок (в смысле Евклидова расстояния) к наблюдению y(t) среди всех конкурирующих сигналов.

Раскрыв скобки в (1.44), приходим к соотношению

$$d^2(S_i, y) = \int_0^T y^2(t)dt - 2\int_0^T y(t)\cdot S(t) + \int_0^T S^2(t)dt = \|y\|^2 - 2Z_i + \|S_i\|^2, \tag{1.46}$$

где Z_i - соответствует корреляции между наблюдением y(t) и i -м сигналом $S_j(t)$

$$Z_i = \left(y_i, S_i\right) = \int_0^T y(t)S(t)dt. \tag{1.47}$$

Первое слагаемое в правой части соотношения (1.46) фиксировано для данного наблюдения и не влияет на анализируемые расстояния и решение, какой из сигналов был принят. Последний член суммы есть ни что иное, как энергия i -го сигнала E_i. Учитывая это, правило минимума расстояния (1.45) может быть сформулировано как правило максимума корреляции:

$$Zj - \frac{Ej}{2} = \max(Zi - \frac{Ej}{2}) \Rightarrow Hj, \tag{1.48}$$

означающее, в частности, что из M возможных сигналов с одинаковой энергией фактически принятым считается тот, который имеет максимум корреляции с наблюдением y(t).

Одним из ограничений при синтезе сигналов является размерность сигнального пространства, внутри которого осуществляется их упаковка. Физическая сущность этого ограничения обусловлена практическим ресурсом, например, ши-

риной частотной полосы. Если частотно-временной ресурс, в котором могут располагаться M сигналов, ограничен параметрами ΔF и T соответственно, то одно из ограничений учитывает экономию полосы, тогда как второе отражает желание передать данные с приемлемой скоростью $R=\log M/T$. Тогда, согласно теореме отсчётов, имеется около ΔFT независимых отсчётов, которые могут быть использованы при синтезе M сигналов, причём каждый из сигналов трактуется как вектор в пространстве размерности $n_S=\Delta FT$.

Задача выбора множества сигналов может быть сформулирована следующим образом: найти в пространстве заданной размерности n_S созвездие из M векторов, удовлетворяющее энергетическим ограничениям и обладающее максимально возможным минимумом расстояния между векторами $d_{min}=max$. В свете выражений (1.46) – (1.48) предпочтительными являются сигналы с наименьшим значением максимального бокового лепестка. Это требование всегда сопровождается ограничением на метод модуляции или на алфавит, которому принадлежат символы кодовой последовательности. Таким образом, требования, предъявляемые к наилучшему сигналу, могут быть сформулированы в виде следующей оптимизационной задачи: на множестве всех возможных последовательностей длины N с символами из заранее выбранного алфавита найти последовательность или последовательности с минимальной величиной максимального бокового лепестка корреляционной функции.

В настоящее время отсутствуют регулярные методы синтеза дискретных последовательностей (ДП) оптимальных по минимаксному критерию. Более того, не представляется возможным ответить на вопрос: насколько известные сигналы с большим числом позиций N близки к оптимальным. Поэтому актуальным остается поиск эффективных методов расчета ДП с хорошими минимаксными свойствами.

Один из таких методов основан на использовании итерационных алгоритмов [53]. При соответствующем выборе начального приближения и использовании целочисленной оптимизации по минимаксному или среднестепенному критериям

можно получить сравнительно хорошие в указанном смысле сигналы. Однако недостатком итерационных методов является зависимость от начального приближения, резкое увеличение времени расчета сигнала по мере увеличения N и то, что они приводят только к локальному экстремуму.

Другие методы предполагают поиск необходимых условий существования ДП с заданными параметрами. Примером такого подхода является следующий. Известно [8,15], что последовательности с хорошей апериодической автокорреляционной функцией (АКФ) могут быть найдены только среди последовательностей с хорошей периодической АКФ. На первом этапе формируется множество последовательностей кандидатов с хорошей периодической АКФ. На втором этапе осуществляют исчерпывающий поиск по критерию наименьшего уровня максимума бокового лепестка апериодической АКФ среди всех циклических сдвигов одноперiодных сегментов последовательностей кандидатов. Результатом поиска служит последовательность с минимальным значением боковых лепестков апериодической АКФ.

Заслуживает внимания метод синтеза ДП путем гомоморфного отображения мультипликативных групп простого и расширенного поля Галуа с помощью к – значного характера. Исследования показали, что с ростом характеристики поля и числа классов, объем вычислений при направленном переборе резко возрастает.

Известные методы синтеза ДП с заданными корреляционными функциями практически всегда основаны на проведении операций перебора множества вариантов для выбора лучшего результата и при значительном периоде ДП применение таких методов становится проблематичным.

В данной диссертационной работе предлагаются методы синтеза систем сигналов, которые позволяют существенно (по сравнению с известными методами перебора) сократить объем вычислений по нахождению ДП с заданными свойствами (ансамблевыми, корреляционными и др.).

В многопользовательских системах с кодовым разделением необходимы семейства дискретных сигналов с особенными взаимными корреляционными свойствами. Синтез семейств сигналов с необходимыми взаимно корреляционными

свойствами заключается в отыскании семейства последовательностей, обладающего соответствующими взаимно корреляционными функциями. В данной работе представлены методы, позволяющие осуществлять синтез систем нелинейных дискретных сложных сигналов с заданными, для тех или иных приложений ТКС, корреляционными свойствами.

1.4 Формулировка проблемы синтеза и практического использования систем сигналов с заданными свойствами в телекоммуникационных системах. Выбор направлений исследований

Среди основных направлений улучшения показателей эффективности функционирования ТКС, в частности, помехозащищенности, скрытности, информационной безопасности, можно выделить направления, связанные с применением каналов с большой избыточностью, высокой пространственной, структурной, энергетической и временной скрытностью[69-70]. Одним из путей решения данной проблемы является применение радиоканалов с частотной избыточностью (широкополосных каналов). Для ее обеспечения в настоящее время на физическом уровне используются фазоманипулированные широкополосные сигналы (ФМ ШПС) и частотно-фазоманипулированные (ЧФМ) сигналы. Однако построенные с их использованием каналы, не обеспечивают требуемые показатели по помехозащищенности и скрытности функционирования. Это в значительной степени связано с тем, что в качестве манипулирующих (расширяющих спектр) используются сигналы с линейным законом формирования. Как показали исследования [55,58,69,74,79] разрешение указанных противоречий и обеспечение требуемых показателей помехозащищенности, скрытности функционирования ТКС в условиях внутренних и внешних воздействий возможно на основе разработки методов синтеза нелинейных дискретных сложных сигналов с необходимыми корреляционными, ансамблевыми и структурными свойствами. В частности, при использовании таких сигналов в качестве физического переносчика информации временные затраты на раскрытие структуры используемых сигналов возрастают и поста-

новка «оптимальных» помех становится проблематичной [82,93,102]. В работах [57,61,63,111] сформулирована и решена задача синтеза нелинейных дискретных последовательностей, обеспечивающих требуемые значения помехозащищенности, информационной и структурной скрытности функционирования телекоммуникационной системы. Сложные сигналы, полученные на основе таких последовательностей (например, с применением системы расширения спектра методом прямой последовательности), обладают, с одной стороны, структурными свойствами, аналогичными свойствам случайных (псевдослучайных) последовательностей, а с другой, - требуемыми ансамблевыми и корреляционными свойствами. Кроме того, такие системы сигналов существуют и обладают указанными выше свойствами, для широкого спектра значений длин последовательностей. Результаты синтеза и анализа такой системы сигналов приведены в разделах 2 - 4 данной диссертационной работы.

Анализ методов информационного обмена в ТКС показывает, что для передачи данных в таких системах используют дискретные сигналы с линейными законами их формирования. При этом сигналы указанного класса обладают по критерию (1.29) неудовлетворительной скрытностью. Так для раскрытия закона формирования такого класса линейных сигналов, как М-последовательности, достаточно знать (перехватить) 2^m из $2^m - 1$ символов сигнала, где m – число каскадов регистра с обратными связями. В ТКС в процессе синхронизации и передачи данных в течение продолжительного времени используется фиксированное соответствие: бит сообщения – сложный сигнал, что позволяет нарушителю на основе определения параметров используемых в системе сигналов, осуществить постановку преднамеренных помех с минимальными энергетическими затратами.

Использование фиксированного соответствия: бит (m бит) сообщения – сигнал (2^m сигналов) линейной формы основывается на предположении, что радиоканалы, в частности, с фазоманипулированными широкополосными сигналами, являются энергетически скрытными. Однако, как показали исследования [78,80,93,105], такое предположение, особенно в отношении спутниковых радиоканалов, оказалось неверным. Параметры используемых сигналов и алгоритмы их

излучения могут быть определены станцией нарушителя (в зависимости от условий функционирования радиоканалов, метода информационного обмена и применяемых средств разведки, анализа и противодействия нарушителя), либо на основе поэлементной обработки сложного сигнала, либо обработки сигналов в целом средствами вычислительной техники с использованием быстрых преобразований.

Математическая постановка проблемы исследований представляется следующим образом.

Функция цели (Z) состоит в обеспечении гарантированной информационной безопасности (вероятности навязывания ложного сообщения - $P_н$), заданной (необходимой) помехозащищенности (структурной скрытности - S) сигнала-переносчика сообщений, максимизации энергетических ($J_п$) и временных (T) затрат средств радиоэлектронного противодействия, в условиях ограниченной пиковой мощности ($P_с$) сигнала телекоммуникационной системы, минимизации временных ($T_з$) и вычислительных затрат $К_з$ синтеза и анализа сигналов-переносчиков информации, минимизации значения максимальных боковых выбросов функции неопределенности сигналов $R_{б\ макс}$.

$$Z = \min\left\{P_{н,} R_{б\ макс.,} T_з,\ К_з\right\},\ \left\{S < S_{доп,}\right\},\ \left\{J_{п,}, T\right\} = \max.$$

Данная проблема относится к классу оптимизационных задач большой размерности и требует для своего решения значительных трудозатрат. В ней фигурирует большое число факторов, которые трудно формализовать. В этом случае целесообразно провести декомпозицию общей проблемы на совокупность частных задач исследования. Такой подход позволяет представить процесс решения сформулированной проблемы как решение частных задач, с учетом естественных связей между ними.

1. Исследование проблемы защищенности информационного обмена ТКС. Выявление причин, порождающих указанную научную проблему, выбор критериев оценки и показателей эффективности исследуемых процессов и обоснование направлений исследований.

2. Математическое обоснование, разработка и исследование методов синтеза нелинейных сложных сигналов в конечных полях с улучшенными ансамблевыми, корреляционными, структурными свойствами в целях повышения помехозащищенности и информационной безопасности ТКС.

3. Разработка модели структуры сложных нелинейных дискретных сигналов в конечных полях с целью определенияструктурной скрытности данного класса сигналов для оценки показателей помехозащищенности и информационной безопасности ТКС.

4. Разработка и исследование метода синтеза нелинейных криптографических дискретных сложных сигналов с улучшенными ансамблевыми, корреляционными, структурными свойствами в целях повышения помехозащищенности и информационной безопасности ТКС.

5. Исследование свойств новых синтезированных классов нелинейных дискретных сложных сигналов для использования в ТКС в качестве физического переносчика информации.

6. Разработка методов оценки свойств сложных сигналов, позволяющих снизить вычислительные затраты на реализацию процесса синтеза сложных сигналов с улучшенными ансамблевыми, корреляционными, структурными свойствами.

7. Разработка программных моделей, реализующих предложенные методы синтеза нелинейных сложных сигналов для практического использования в ТКС.

8. Разработка и усовершенствование методов быстрой реализации модульных операций

9. Усовершенствование методов информационного обмена в ТКС с целью улучшения показателей помехозащищенности и информационной безопасности.

Сформулируем задачу синтеза одного класса сигналов с заданными корреляционными ансамблевыми и структурными свойствами, обеспечивающих требуемые значения помехозащищенности, имитостойкости и скрытности функционирования системы передачи информации. Потребуем, что бы такие системы сигналов обладали свойством «размытости» по корреляционным свойствам. Указанное свойство означает, что увеличение или уменьшение длины дискретной последова-

тельности не изменяет корреляционные свойства, присущие исходной дискретной последовательности.

Под задачей синтеза сигналов будем понимать задачу построения словарей (подмножеств, векторов) $(W_m^q), q=\overline{1,N}$, $m=\overline{1,M}$, вся $M_k << p^L$, совокупность которых образует систему сигналов размерности $M_k = N \times M_x$ таких, что в каждом из словарей выполняются следующие условия [62].

1. Автосвертка или периодическая функция автокорреляции (ПФАК) каждого из W_m^q ДС удовлетворяет системе нелинейных параметрических неравенств (СНПН)

$$R_{a_1}^q(l) \le \sum_{i=1}^{L-1} W_i^q (W_{i+c}^q)^* \le R_{a_2}^q(l), \quad l=\overline{1,L-1}, \quad q=\overline{1,N}, \qquad (1.49)$$

где $R_{a_1}^q(l)$ и $R_{a_2}^q(l)$ заданные (требуемые) реализации ПФАК.

2. Взаимная свертка (СФВК) ($W^q W^p$) ДС со стыковыми словами W^{qp} и W^{pq} удовлетворяет совокупности систем нелинейных параметрических неравенств:

$$R_{b_{1,1}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,1}}^{qp}(l);$$

$$R_{b_{1,2}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,2}}^{qp}(l);$$

$$R_{b_{1,3}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R_{b_{2,3}}^{qp}(l);$$

$$R_{b_{1,4}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R_{b_{2,4}}^{qp}(l);$$

$$R_{b_{1,5}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R_{b_{2,5}}^{qp}(l); \qquad (1.50)$$

причем $l=\overline{1,L-1}$, для всевозможных сочетаний q и p, $q=\overline{1,N}$, $p=\overline{1,N}$, $q \ne p$, где $R_{b_{1,j}}^{qp}(l)$ и $R_{b_{2,j}}^{qp}(l)$ - заданные (требуемые) реализации ПФВК и СФВК.

3. Исследования показывают, что существенные затруднения в преодолении скрытности функционирования радиоканалов могут быть созданы за счет придания сигналам свойства «размытости». Введем понятие размытости. Причем вначале сформулируем задачу синтеза одиночного сигнала W^q, обладающего размы-

тостью по циклической свертке. Определим интервал размытости Δx по длительности

$$L - x_2 \le \Delta x \le L + x_1, \tag{1.51}$$

Полагая, что в общем случае $|x_1| \ne |x_2|, |x_1|, |x_2| < L$, интервал размытости Δy относительно истинных значений цикловой частоты в виде

$$L - y_2 \le \Delta y \le L + y_1, \tag{1.52}$$

причем $|y_1| \ne |y_2|, |y_1|, |y_2| < L$.

Положим, что на основе обработки потока сигналов $W^{v}W^{v}...W^{v}$ принимается как истинный сигнал

$$W^{\vartheta}_{x_L} = W^{\vartheta}_{L-\delta} W^{\vartheta}_{L} W^{\vartheta}_{x_1 - L - \delta}, \tag{1.53}$$

либо

$$W^{\vartheta}_{x_1} = W^{\vartheta}_{L-\delta} W^{\vartheta}_{X_1 + \delta}, \tag{1.54}$$

при $\Delta x \ge L$, либо сигнал

$$W^{\vartheta}_{x_2} = W^{\vartheta}_{L - X_2}, \tag{1.55}$$

либо

$$W^{\vartheta}_{x_{21}} = W^{\vartheta}_{\delta} W^{\vartheta}_{L - x_2 - \delta}, \tag{1.56}$$

при $\Delta x < L$, где индексы x_1 и x_2, δ, L, $x_1 + \delta - L$, L-δ, $x_1 + \delta$, $L - x_2 - \delta$ указывают число символов усеченного сигнала W^{ϑ} (первых или последних соответственно расположению его символов $W^{\vartheta}_{X_1}$ или $W^{\vartheta}_{X_2}$. Тогда размытость сигналов, заданных (1.53 – 1.56) будем представлять совокупностью систем нелинейных параметрических неравенств:

$$R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W^{\vartheta}_i \left(W^{\vartheta}_{i+k}\right)^* + \sum_{i=L-k+1}^{L} W^{\vartheta}_i \left(W^{\vartheta}_{i-L+K}\right)^* + \sum_{i=1}^{L-K} W^{\vartheta}_i \left(W^{\vartheta}_{i+k}\right) + \sum_{i=L-k+1}^{L} W^{\vartheta}_i \left(W^{\vartheta}_{i-L+K}\right)^* + \text{а)}$$

$$+ \sum_{i=1}^{x_1 - L + \vartheta} W^{\vartheta}_i \left(W^{\vartheta}_{i+k}\right)^* \le R'_{a_2}(k);\ k = \overline{0, L + x_2},$$

$$R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W^{\vartheta}_i \left(W^{\vartheta}_{i+k}\right)^* + \sum_{i=L-k+1}^{L} W^{\vartheta}_i \left(W^{\vartheta}_{i-L+K}\right)^* + \sum_{i=1}^{L-K} W^{\vartheta}_i \left(W^{\vartheta}_{i+k}\right) + \sum_{i=L-k+1}^{L} W^{\vartheta}_i \left(W^{\vartheta}_{i-L+K}\right)^* \le R'_{a_2}(k); \quad \text{б)}$$

$$k = \overline{0, L + x_1},$$

$$R_{a_2}(k) \le \sum_{i=1}^{L-x_1} W_i^{\vartheta} \left(W_{i-k}^{\vartheta}\right)^* \le R'_{a_2}(k), k = \overline{0, L-x_2}, \qquad \text{в)}$$

$$R_{a_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* + \qquad \text{г)}$$

$$+ \sum_{i=1}^{L-x_2+\vartheta} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* \le R'_{a_2}(k); \; k = \overline{0, L-x_2}, \qquad (1.57)$$

где $R'_{a_1}(k)$ и $R'_{a_2}(k)$ - различные реализации ПФАК, задаваемые при синтезе сигналов.

В случае размытости по ПФВК и СФВК в интервале Δx, определяемого как:

$$L - x_2 \le \Delta x \le L + x_1,$$

размытость может быть задана совокупностью систем нелинейных неравенств

$$R'_{b_1}(k) \le \sum_{i=\delta}^{L-K} W_i^q \left(W_{i+k}^{\vartheta_1}\right)^* + \sum_{i=L-k+1}^{L} W_i^q \left(W_{i-L+K}^{\vartheta_2}\right)^* + \sum_{L=1}^{L-K} W_i^p \times \left(W_{L+k}^{\vartheta_2}\right)^* + \sum_{i=L-K+1}^{L} W_i^p \left(W_{i-L+K}^{\vartheta_3}\right)^* + \qquad \text{а)}$$

$$+ \sum_{i=1}^{L-K} W_i^r \times \left(W_{i+K}^{\vartheta_3}\right)^* \le R'_{b_2}(k); \; k = \overline{0, L+x},$$

$$R'_{b_1}(k) \le \sum_{i=\delta}^{L-K} W_i^q \left(W_{i+k}^{\vartheta_1}\right)^* + \sum_{i=L-k+1}^{L} W_i^q \left(W_{i-L+K}^{\vartheta_2}\right)^* + \sum_{L=1}^{L-K} W_i^p \times \left(W_{L+k}^{\vartheta_2}\right)^* + \sum_{i=L-K+1}^{L} W_i^p \left(W_{i-L+K}^{\vartheta_3}\right)^* \le R'_{b_2}(k); \quad \text{б)}$$

$$k = \overline{0, L+x},$$

$$R'_{b_2}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q * (W_i^{\vartheta_1} + k)^* \le R_{b_2}(k), k = \overline{0, L-x_{2,}} \qquad \text{в)}$$

$$R'_{b_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q \left(W_{i+k}^{\vartheta_2}\right)^* + \sum_{i=L-k+1}^{L} W_i^q \left(W_{i-L+K}^{\delta_2}\right)^* + \sum_{i=1}^{L-x_2+\delta} W_i^p \left(W_{i+k}^{\vartheta_2}\right)^* \le R'_{b_2}(k); \qquad \text{г)}$$

$$k = \overline{0, L-x_2}, \qquad (1.58)$$

Таким образом, условие которое должно выполняться для синтезируемой системы сигналов W_m^q, может быть сформулировано следующим образом: словарь $\{W_m^q\}$ удовлетворяет совокупности систем нелинейных параметрических неравенств (1.57) – (1.58), т.е. словарь $\{W_m^q\}$ обладает в интервалах Δx и Δy разностью по длительности и цикловой частоте.

4. В каждом из M словарей существуют сигналы $W_{m_1}^{q_1}$ и $W_{m2}^{q_2}$, авто - и взаимная свертка которых, удовлетворят совокупности неравенств вида (1.49) и (1.50);

5. Закон формирования каждого из сигналов W_m^q может быть определен при перехвате не менее L сигналов, то есть по критерию (1.29) W_m^q обладает структурной скрытностью.

6. Апериодическая нормированная автосвертка W_m^q удовлетворяет системе нелинейных неравенств

$$r_{a_1}^q(l) \le \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \le r_{a_2}^q(l);\ l=\overline{1,L},\ m=\overline{1,L}, \tag{1.60}$$

где $r_{a_1}^q(l)$ и $r_{a_2}^q(l)$ - заданные реализации АФАК.

7. Апериодическая взаимная свертка удовлетворяет двум системам нелинейных параметрических неравенств

$$r_{b_{1,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \le r_{b_{1,2}}^{qp}(l);$$

$$l=\overline{1,L},\ m=\overline{1,L},$$

$$r_{b_{2,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \le r_{b_{2,2}}^{pq}(l);$$

$$l=\overline{1,L},\ m=\overline{1,L}. \tag{1.61}$$

8. Целевая функция

$$\mathrm{Int}(E) = \sum_{j=1}^{n} C_j S_j \tag{1.62}$$

принадлежит интервалу (A,B), где S_j - значения реализаций функций системы передачи информации, описывающих законы распределения величин апериодических и периодических функций корреляции, определяющих структурную скрытность сигналов, алгоритмы построения ДС и др., а C_j - соответствующие им штрафы.

Выводы к разделу 1

В первом разделе диссертации решена **первая** задача исследования.

1. Информационный обмен в телекоммуникационных системах осуществляется, как правило, в условиях внутренних и внешних негативных воздействий

(факторов). К внутренним факторам можно отнести помехи, которые создают другие станции многопользовательской системы. Кроме того, в ряде приложений ТКС имеют место внешние воздействия (угрозы, факторы), к которым относят, в частности, помехи, создаваемые станцией противодействия. При этом противоборствующая сторона осуществляет активную разведку и радиоэлектронне противодействие. Эффективное радиоэлектронное противодействие может быть осуществлено только после обнаружения факта функционирования ТКС и оценки ее параметров: частотного диапазона; занимаемой полосы; закона модуляции (формы дискретных последовательностей (чипов), используемых для модуляции информационных битов данных пользователей системы) и др. При этом, станция противодействия, как правило, ставит перед собой цель нанести максимальный ущерб ТКС и /или ее пользователям и собственникам, при минимизации собственных затрат. В указанных условиях особенно важной проблемой для защищенной ТКС является обеспечение минимизации потерь при максимальных затратах станции противодействия.

В случае, когда ТКС использует в качестве физического переносчика информации систему сигналов с нетривиальным законом модуляции, параметры которой неизвестны станции противодействия, последняя лишена возможности реализовывать согласованную фильтрацию, и вынуждена рассматривать перехватываемый сигнал в виде случайного и осуществлять процедуру обнаружения, используя набор параллельных каналов для анализа участка частотно-временной области, либо комбинировать (выполнять перебор) возможных состояний неизвестных параметров системы.

2. Анализ показал, что станция противодействия может иметь полную информацию о ТКС, режимах ее функционирования, а также таких параметрах радиоканалов, как частотный диапазон работы, вид или класс сигналов – переносчиков, время сеансов связи, объем передаваемой информации. Кроме того, станция противодействия может владеть аналогичными образцами объектов ТКС и т.п. В указанных условиях создание радиоканалов телекоммуникационной системы должно осуществляться таким образом, чтобы наиболее эффективной страте-

гией станции противодействия была стратегия нарушение функционирования системы путем постановки, так называемой, заградительной помехи.

3. В процессе радиоэлектронного противодействии, если станции противодействия неизвестны заранее сведения о используемых частотном диапазоне и интервале времени, отводимом для передачи данных, то стратегия противодействия должна сводиться к решению задачи обнаружения сигналов. Для этого станция противодействия должна использовать энергетический приемник (детектор), настроенный на истинную для перехватываемого сигнала частотно-временную зону. Причиной этому является отсутствие у станции противодействия информации о структуре обнаруживаемого сигнала, например законов модуляции, расширения спектра и т.п. Поэтому для предотвращения возможности обнаружения станцией противодействия сигнала телекоммуникационная система должна использовать сигналы с распределенным или широким спектром, которые обладают максимально возможным значением выигрыша от обработки, и практически не раскрываемой структурой.

4. В условиях противодействия помехозащищенность радиоканалов ТКС зависит от скрытности выбора и использования параметров системы. Под скрытностью радиоканалов в целом и скрытностью используемых в них параметров, будем понимать их способность противостоять мерам радиотехнической разведки, направленным на обнаружение факта работы системы (энергетическая скрытность) и определения необходимых для радиопротиводействия параметров сигнала (структурная и информационная скрытность). Энергетическая скрытность, характеризует способность системы противостоять мерам, направленным на обнаружение станцией противодействия факта функционирования системы. Структурная скрытность используемых сигналов характеризует сложность достоверного предсказания сигналов или их символов (по известным предыдущим). Информационная скрытность системы характеризует сложность отождествления принятых сигналов с передаваемым сообщением.

5. Качество услуг, которые предоставляет ТКС, предлагается оценивать уровнем обеспечения информационной безопасности. При этом под информационной

безопасностью будем понимать способность ТКС обеспечивать защиту от уничтожения, модификации, блокирования информации, ее несанкционированной утечки или от нарушения установленного порядка ее маршрутизации. Также под информационной безопасностью следует понимать состояние защищенности систем обработки и хранения данных, при котором обеспечено сохранение конфиденциальности, целостности и доступности информации, а также других свойств информации и услуг: аутентичности, отслеживаемости, неопровержимости и надежности.

6. Основным ограничением при синтезе дискретных сигналов является размерность сигнального пространства, внутри которого осуществляется их упаковка. Как правило, сущность этого ограничения обусловлена наличием практического ресурса, например, шириной полосы частот. В общем случае, задача выбора множества сигналов может быть сформулирована следующим образом: необходимо найти в пространстве заданной размерности n_S множество M векторов, которое удовлетворяет энергетическим ограничениям и обладает максимально возможным минимумом расстояния между векторами (сигналами). При этом наиболее предпочтительными являются сигналы с наименьшим значением максимального бокового лепестка функции неопределенности. Поэтому, одно из требований к наилучшему (наиболее рациональному) сигналу, может быть сформулировано в виде следующей оптимизационной задачи: на множестве всех возможных последовательностей длины N с символами из заранее выбранного алфавита найти последовательность или последовательности с минимальной величиной максимального бокового лепестка функции неопределенности.

7. Проведенный анализ подтвердил, что в настоящее время отсутствуют регулярные методы синтеза дискретных последовательностей (ДП) оптимальных по минимаксному критерию. Задача синтеза ДП оказывается еще более сложной, если выдвигаются требования к размерности (объему) системы сигналов, структурным свойствам и числу элементов ДП. Поскольку для технологии распределенного спектра свойства сигналов – переносчиков данных полностью определяются свойствами ДП, манипулирующих информационные биты данных пользователей системы [27], весьма актуальной проблемой остается поиск эффективных методов

синтеза дискретных сигналов (последовательностей), отвечающих потенциально достижимым граничным характеристикам (минимаксным свойствам).

Основными путями решения приведенного противоречия является повышение помехозащищенности, в том числе энергетической, структурной и информационной скрытности, а также информационной безопасности, в том числе, имитостойкости на уровне источника сложных сигналов. Указанное может быть достигнуто на основе усовершенствования методологических основ построения ТКС путем разработки методов информационного обмена, а также методов синтеза новых классов нелинейных дискретных сложных сигналов с необходимыми ансамблевыми, корреляционными и структурными свойствами.

8. В наиболее обобщенном виде математическая постановка проблемы диссертационных исследований формулируется следующим образом.

Функция цели (Z) состоит в обеспечении: гарантированной информационной безопасности, оцениваемой вероятностью навязывания ложного сообщения - $P_н$; требуемой для конкретных приложений системы помехозащищенности, оцениваемой структурной скрытностью - S сигнала-переносчика сообщений и помехоустойчивостью приема сигналов - $P_{ош}$; максимизации энергетических ($J_п$) и временных (Т) затрат средств радиоэлектронного противодействия, при условии ограниченной пиковой мощности ($P_с$) сигнала телекоммуникационной системы; минимизации временных ($Т_з$) и вычислительных затрат $К_з$ синтеза и анализа сигналов-переносчиков информации; минимизации значения максимальных боковых выбросов функции неопределенности используемых сигналов. В такой постановке решение проблемы повышения помехозащищенности и информационной безопасности ТКС можно свести к решению оптимизационных задач большой размерности. Для решения таких задач необходимо учитывать большое число факторов, которые трудно формализовать. Поэтому целесообразно провести декомпозицию общей проблемы на совокупность частных задач исследования. Такой подход позволяет представить процесс решения сформулированной проблемы как решение частных задач, с учетом естественных связей между ними.

В разделе 1 сформулирована в общем виде (в виде систем уравнений и условий) проблема синтеза систем нелинейных дискретных сложных сигналов с заданными корреляционными, ансамблевыми, структурными свойствами.

9. Обоснован выбор критериев синтеза систем сигналов и показателей для оценки значений помехозащищенности, информационной безопасности, скрытности, имитостойкости системы.

РАЗДЕЛ 2
МЕТОДЫ СИНТЕЗА НЕЛИНЕЙНЫХ СЛОЖНЫХ ДИСКРЕТНИХ СИГНАЛОВ С НЕОБХОДИМЫМИ СВОЙСТВАМИ

В широкополосных системах применение получили дискретно – кодированные сигналы (ДКС), в которых манипулируемые параметры (амплитуда, фаза, частота) изменяются через строго фиксированные интервалы времени. Закон применения манипулируемого параметра в ДСК задается дискретными последовательностями (ДП), которые полностью определяют свойства ДКС и часто отождествляются с ними. Поэтому внимание исследователей широкополосных систем оказалось сфокусированным на анализе, синтезе и обработке ДП.

Проектирование широкополосных систем во многом основывается на нахождении ДКС с соответствующими ансамблевыми, корреляционными, структурными, технологическими и другими свойствами. Под технологическими свойствами ДКС понимают существование регулярных правил и алгоритмов формирования ДП, допускающих возможность аппаратной, программно-аппаратной и программной их реализации. В качестве манипулирующих (расширяющих спектр) в широкополосных системах используются сигналы с линейным законом формирования. Такие сигналы обладают весьма ограниченными ансамблевыми характеристиками и низкой кодовой устойчивостью против раскрытия законов их формирования (низкой структурной скрытностью). Как было отмечено в разделе 1, повышение помехозащищенности, скрытности функционирования телекоммуникационных систем может быть достигнуто за счет использования ДКС, которые могут быть синтезированы длоя широкого спектра значенний периода сигнала. Однако при использовании линейных классов сигналов корреляционные, спектральные, ансамблевые и структурные свойства сигналов существенно ухудшаются, что, в свою очередь, приводит к ухудшению указанных выше показателей функционирования ТКС [55,140].

Как показали исследования [58,85,96,98], разрешение указанных противоречий и обеспечение требуемых показателей помехозащищенности, скрытности

функционирования ТКС в условиях внутренних и внешних воздействий возможно на основе разработки методов анализа и синтеза нелинейных сложных сигналов с необходимыми корреляционными, ансамблевыми и структурными свойствами. В частности, при использовании таких сигналов в качестве физического переносчика информации временные затраты на раскрытие структуры используемых сигналов возрастают и постановка «оптимальных» помех становится проблематичной [111].

В данном разделе приводится описание методов синтеза одного класса нелинейных дискретных сигналов: характеристических дискретных сигналов. В последующих разделах будут приведены оценки показателей функционирования телекоммуникационной системы, достигаемые при применении данного класса сигналов в качестве физического переносчика данных абонентов системы.

2.1 Теоретические основы синтеза нелинейных дискретных сигналов в конечных полях Галуа

Одним из путей повышения эффективности радиоканалов является создание частотной избыточности с применением фазоманипулированных широкополосных сигналов (ФМШПС). При этом к манипулирующим (расширяющим спектр) последовательностям предъявляется ряд требований: хорошие автокорреляционные свойства, относительно равномерный спектр, допустимый уровень максимальных пиков взаимно-корреляционных функций, большой объем, существование для большого числа значений длительностей. Подходя с этих позиций к различным системам сигналов, можно выделить, как наиболее отвечающие перечисленным требованиям, М-последовательности, последовательности с трехуровневой функцией взаимной корреляции, характеристические дискретные сигналы и др. [27,55,100,140].

М-последовательности обладают малым объемом, определяемым из соотношения [51]:

$$M = \phi(N) / m, \qquad (2.1)$$

где $\varphi(N)$ — функция Эйлера; N — число элементов последовательности; *m* — степень примитивного полинома, в соответствии с которым построен линейный рекуррентный регистр сдвига — формирователь М-последовательности.

М-последовательности существуют для весьма разреженного числа значений N, определяемых из выражения:

$$N = 2^m - 1. \qquad (2.2)$$

При этом естественное стремление расширить спектр возможных значений N с целью увеличения ансамбля системы сигналов приводит к ухудшению корреляционных свойств данной системы сигналов.

В разделе рассмотрены N-позиционные коды (характеристические дискретные сигналы) с двухуровневой периодической функцией автокорреляции (ПФАК), построение которых базируется на использовании характера мультипликативной группы [144] поля $GF(p^n)$ для $N = 4x + 2 = p^n - 1$ и $N = 4x = p^n - 1$.

Воспользуемся понятием двузначного характера ψ мультипликативной группы $GF(p^n)$ и сформулируем правила кодирования для данной системы сигналов:

$$\mu = \{\mu_i : i = 0, 1, \ldots, p^n - 2\},$$

$$\left.\begin{array}{l} \mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \equiv 0 (\mathrm{mod}\ p); \\ \mu_i = 1, \qquad\quad \text{если } \Theta^i + 1 \equiv 0 (\mathrm{mod}\ p); \end{array}\right\}, \qquad (2.3)$$

$$\left.\begin{array}{l} \mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \equiv 0 (\mathrm{mod}\ p); \\ \mu_i = -1, \qquad\quad \text{если } \Theta^i + 1 \equiv 0 (\mathrm{mod}\ p); \end{array}\right\}, \qquad (2.4)$$

где θ - первообразный элемент поля $GF(p^n)$.

Воспользовавшись выражением для периодической функции автокорреляции (ПФА) бинарного фазоманипулированного сигнала, построенного на базе кода

$$R_\mu(m) = \sum_{i=0}^{N-1} \mu_i \mu_{i+m},$$

с учетом правила кодирования (3) и, учитывая, что $\psi(0) = 0$, найдем

$$R_\mu(m)=\begin{cases} N, \text{ если } m\equiv 0(\text{mod } N);\\ \sum\limits_{i=1}^{p^n-2}\psi(\Theta^i+1)\psi(\Theta^{i+m}+1)+\\ +\psi(-\Theta^m+1)+\psi(-\Theta^{-m}+1)=\\ =A+\psi(-\Theta^m+1)+\\ +\psi(-\Theta^{-}+1)\text{если } m\equiv 0(\text{mod } N). \end{cases} \qquad (2.5)$$

С учетом свойств характера ψ выражение для A из (2.5) можно записать в виде

$$A=\psi(\Theta^m)\sum_{i=0}^{p^n-2}\psi(\Theta^i+1)\psi(\Theta^i+\Theta^{-m})=\psi(\Theta^m)E. \qquad (2.6)$$

Когда i в (2.5) пробегает все значения от нуля до p^n-2, степени первообразного элемента Θ побегают все ненулевые элементы расширенного поля $GF(p^n)$. Поэтому, обозначая нулевые элементы поля - $a_i, i=0,1,\dots,p^n-2$, можно перейти от суммы по индексу i к сумме по всем нулевым элементам поля $GF(p^n)$:

$$E=\sum_{\substack{a_i\in GF(p^n),\\ a_i\neq 1(\text{mod } p)}}\psi(a_i+1)\psi(a_i+\Theta^{-m}).$$

Обозначим $b_i=a_i+1$ и с учетом того, что a_i пробегают все ненулевые элементы поля $GF(p^n)$, то b_i пробегают все элементы поля $GF(p^n)$, за исключением 1, поэтому

$$E=\sum_{\substack{b_i\in GF(p^n),\\ b_i\neq 1(\text{mod } p)}}\psi(b_i)\psi(b_i+\Theta^{-m}-1). \qquad (2.7)$$

Далее, если $b_i=1$, то $E=\psi(\Theta^{-m})$. Поэтому, добавляя и вычитая $\psi(\Theta^{-m})$ и, учитывая, что $\psi(0)=0$, можно преобразовать (2.7) к виду

$$E=\sum_{b_i\in GF(p^n),}\psi(b_i)\psi(b_i+\Theta^{-m}-1)=\sum_{\substack{b_i\in GF(p^n),\\ b_{i\neq 0(\text{mod } p)}}}\psi(b_i)\psi(b_i+\Theta^{-m}-1)-\psi(\Theta^{-m})=$$

$$=\sum_{\substack{b_i\in GF(p^n),\\ b_{i\neq 0(\text{mod } p)}}}\psi(b_i^2)\psi[1+(\Theta^{-m}-1)b_i^{-1}]-\psi(\Theta^{-m})=\sum_{\substack{b_i\in GF(p^n),\\ b_{i\neq 0(\text{mod } p)}}}\psi[1+(\Theta^{-m}-1)b_i^{-1}]-\psi(\Theta^{-m}).$$

Но, так как $b_i \in GF(p^n), b_{i\neq 0(\mathrm{mod}\, p)}$, то b_i^{-1} также побегает все ненулевые элементы поля $GF(p^n)$, т.е. обозначая $c_i = b_i^{-1}$, имеем

$$E = \sum_{\substack{c_i \in GF(p^n),\\ c_{i\neq 0(\mathrm{mod}\, p)}}} \psi[1 + dc_i] - \psi(\Theta^{-m}), \tag{2.8}$$

где $d = (\Theta^{-m} - 1) \neq 0(\mathrm{mod}\, p)$, так как для $m \neq 0(\mathrm{mod}\, N)$.

Известно, что для любого нетривиального характера справедливо:

$$\sum_{x\in GF(p)} \psi(ax + b) = 0, \quad a \neq 0(\mathrm{mod}\, P), \; a, b \in GF(p^n). \tag{2.9}$$

Из соотношения (2.9) следует:

$$\sum_{x\in GF(p^n)} \psi(ax + b) = \sum_{\substack{x\in GF(p^n)\\ x\neq 0(\mathrm{mod}\, P)}} \psi(ax + b) + \psi(b) = 0, \tag{2.10}$$

откуда

$$\sum_{x\in GF(p^n)} \psi(ax + b) = -\psi(b). \tag{2.11}$$

С учетом (2.8) - (2.11) получим

$$E = -1 - \psi(\Theta^{-m}). \tag{2.12}$$

Подставляя выражение (2.12) в (2.6) и (2.5), находим

$$R_\mu(m) = \psi(\Theta^m)[-1 - \psi(\Theta^{-m})] + \psi(-\Theta^m + 1) + \psi(-\Theta^{-m} + 1). \tag{2.13}$$

Заметим, что выражение (2.13) справедливо для любого $N = p^n - 1$.

Далее ограничимся случаем $N = 4x + 2 \equiv 2(\mathrm{mod}\, 4)$.

Одним из свойств двухзначного характера является [144]

$$\psi(-1) = \begin{cases} -1, p^n - 1 \equiv 2(\mathrm{mod}\, 4) \\ 1, p^n - 1 \equiv 0(\mathrm{mod}\, 4) \end{cases}. \tag{2.14}$$

Тогда, согласно (2.14)

$$\psi(-1) = -1. \tag{2.15}$$

Учитывая (2.15) и то, что

$$\psi(a) = \psi(a^{-1}), \quad a \neq 0(\mathrm{mod}\, P), \tag{2.16}$$

преобразуем (2.13) к виду

$$R_\mu(m) = -1 - \psi(\Theta^m) + \psi(\Theta^m - 1)\cdot[-1 + \psi(\Theta^m)]. \qquad (2.17)$$

Из выражения (2.17) следует, что:

если $\psi(\Theta^m) = 1$ и $\psi(\Theta^m - 1) = 1$, то $R_\mu(m) = -2$,

если $\psi(\Theta^m) = 1$ и $\psi(\Theta^m - 1) = -1$, то $R_\mu(m) = -2$,

если $\psi(\Theta^m) = -1$ и $\psi(\Theta^m - 1) = 1$, то $R_\mu(m) = 2$,

если $\psi(\Theta^m) = -1$ и $\psi(\Theta^m - 1) = -1$, то $R_\mu(m) = -2$. $m \neq 0(\text{mod } N)$.

Так как Θ - первообразный элемент поля $GF(p^n)$, то степени $\Theta^i, i = 0,1,\ldots, p^n - 2$, пробегают все $p^n - 1$ ненулевые элементы поля $GF(p^n)$, а элементы $\Theta^i + 1, i = 0,1,\ldots, p^n - 2$, нулевой и все нулевые элементы поля $GF(p^n)$, кроме 1, поскольку для некоторого $i, \Theta^i + 1 \equiv 0(\text{mod } p)$ и ни для какого $i, \Theta^i + 1 \neq 1(\text{mod } p)$, так как $\Theta^i \neq 0(\text{mod } p)$.

Учитывая изложенное и то, что $\psi(1) = 1$, легко заключить, что среди $p^n - 2$ ненулевых элементов $\Theta^i + 1$ поля $GF(p^n)$ имеется $[1/2(p^n - 1) - 1]$ элементов, для которых ψ равно -1 (т.е. квадратичных невычетов поля $GF(p^n)$). Поэтому для правила кодирования (3) число символов кода μ, принимающих значение +1, равно

$$K^+ = \frac{1}{2}(p^n - 1) - 1 + 1 = \frac{1}{2}(p^n - 1) = \frac{N}{2} = 2x + 1.$$

Таким образом, правило кодирования (2.3) приводит к коду с двухуровневой ПФА $R_\mu(m) = -2, 2$.

Для кодов, полученных согласно правилу кодирования (2.4), ПФА $R_\mu(m)$ равна N, если $m \equiv 0(\text{mod } N)$;

$$N = 4x + 2,\ K^+ = 2x + 1,\ \lambda_1 = x. \qquad (2.18)$$

$$\sum_{i=0}^{p^n-2} \psi(\Theta^i + 1)\psi(\Theta^{i+m} + 1) - \psi(-\Theta^m + 1) - \psi(\Theta^i + 1) - \psi(-\Theta^{-m} + 1) = \\ = A - \psi(-\Theta^{-m} + 1) - \psi(-\Theta^{-m} + 1), \qquad (2.19)$$

если $m \neq 0(\text{mod } N)$.

После преобразований, аналогичных (2.6) - (2.7), получим

$$R_{\mu}(m) = \psi(\Theta^{m})[-1-\psi(\Theta^{m})] - \psi(-\Theta^{m}+1) - \psi(-\Theta^{-m}+1). \qquad (2.20)$$

Выражение (2.20) справедливо для любого $N = p^{n} - 1$. Для $N = 4x + 2 = 2(\mathrm{mod}\ 4)$, учитывая (2.15) и (2.16), преобразуем (2.20) к виду

$$R_{\mu}(m) = -1 - \psi(\Theta^{m}) - \psi(-\Theta^{m}-1)[-1+\psi(\Theta^{m})]. \qquad (2.21)$$

Из выражения (2.21) следует, что:

если $\psi(\Theta^{m}) = 1$ и $\psi(\Theta^{m}-1) = 1$, то $R_{\mu}(m) = -2$,

если $\psi(\Theta^{m}) = 1$ и $\psi(\Theta^{m}-1) = -1$, то $R_{\mu}(m) = -2$,

если $\psi(\Theta^{m}) = -1$ и $\psi(\Theta^{m}-1) = 1$, то $R_{\mu}(m) = 2$,

если $\psi(\Theta^{m}) = -1$ и $\psi(\Theta^{m}-1) = -1$, то $R_{\mu}(m) = -2$, $m \neq 0(\mathrm{mod}\ N)$.

Для правила кодирования (2.4) рассуждения, аналогичные приведенным ранее, показывают, что число символов кода, принимающие значение 1, равно $2x$. Таким образом, правило кодирования (2.4) приводит к коду с двухуровневой ПФА $R_{\mu}(m) = -2,2$, с параметрами

$$N = 4x + 2,\ K^{+} = 2x,\ \lambda_{1} = x - 1,\ \lambda_{2} = x. \qquad (2.22)$$

В разделах 4.3 – 4.5 будут рассмотрены ансамблевые, корреляционные и структурные свойства данного класса нелинейных дискретных сигналов, сформулированы предложения о возможности использования таких сигналов в различных приложениях ТКС.

2.2 Разработка усовершенствованного метода синтеза нелинейных дискретных сигналов в конечных полях

В разделе приводятся результаты исследований, связанные с разработкой метода синтеза одного класса сложных сигналов, основанного на использовании свойств полей Галуа. Кроме того, приводятся полученные в ходе исследований аналитические выражения, устанавливающие связи характеров элементов мультипликативной группы поля Галуа и зависимости символов дискретных кодов,

построенных с использованием свойств характеров мультипликативной группы поля.

В [144] рассмотрены характеристические дискретные сигналы (ХДС) с числом позиций (символов) $L = 4x + 2$ и $L = 4x$, синтез которых базируется на использовании характера ψ мультипликативной группы поля $GF(P)$.

Правило кодирования таких кодов для $L = 4x + 2$ имеет вид:

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

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

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0(\text{mod } P), \quad (2.23)$$

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

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0(\text{mod } P), \quad (2.24)$$

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

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

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

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

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0(\text{mod } P), \quad (2.25)$$

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

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0(\text{mod } P). \quad (2.26)$$

В [144] показано, что мощность метода данного класса сигналов (M) равна числу классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы на смежные классы по классу автоморфных коэффициентов, и определяется как $M = \phi(L)/2\cdot$, где (φ(L)) – функция Эйлера.

Известно так же [144], что правила кодирования (2.23) и (2.24) приводят к коду с двухуровневой периодической функцией автокорреляции $R_\mu = \{-2, 2\}$, а правила кодирования (2.25) и (2.26) — к $R_\mu = \{0, -4\}$ и $R_\mu = \{0, 4\}$ соответственно.

Максимальные по модулю значения боковых лепестков функции автокорреляции импульсного бинарного фазоманипулированного сигнала, построенного на базе кода μ:

$$r_{\mu}(m) = \sum_{i=0}^{N-m-1} \mu_i \, \mu_{i+m}, \qquad (2.27)$$

для правил (2.23) и (2.24) находятся в пределах $(0,47 \div 0,82)/\sqrt{N}$, для правила (2.25) - $(0,57 \div 0,82)/\sqrt{N}$, а для правила (2.26) в пределах $-(0,50 \div 0,82)/\sqrt{N}$.

Метод формирования ХДС [144] длительностью N, базирующийся на комплексном использовании аппарата теории полей Галуа $GF(p^n)$, теории чисел и комбинаторики ввиду ориентации на составленные в теории чисел таблицы элементов и индексов элементов поля Галуа уже при $n \geq 1$ и $N \geq 100$ становится трудно реализуемым, что приводит к сложности аппаратной, программно-аппаратной и программной реализации данного метода. Указанное объясняется прежде всего тем, что при гомоморфном отображении элементов поля a_i в множество символов дискретной последовательности при использовании комплекснозначной функции $\psi(ai) = W_i = -e^{j\pi U_i}$, необходимо решать в среднем N/2 сравнений вида

$$a_i \equiv \Theta_j^{U_i} (\mathrm{mod}\ P),\ i = \overline{0, P-1}. \qquad (2.28)$$

где: $U_i = \overline{0, P-2}$ – индекс элемента поля GF(P); Θ_j – j-й первообразный элемент поля; P – характеристика поля Галуа.

Для решения сравнений вида (2.28) используются предварительно рассчитанные таблицы элементов и индексов элементов полей Галуа. Вычислительная сложность такого метода формирования ХДС определяется из соотношения:

$$t_{\sum} = N(t_y + t_{сл} + 3t_з + (N-2)t_{сч} + (N+1)t_{ср}), \qquad (2.29)$$

где: t_y, $t_{сл}$, $t_з$, $t_{сч}$, $t_{ср}$ — время выполнения операций умножения, сложения, записи, считывания и сравнения соответственно. Анализ выражения (2.7) показывает, что основные временные затраты при построении ХДС связаны с квадратичными членами $N(N+2)t_{сч}$, $N(N+1)t_{ср}$.

В ходе исследований получен усовершенствованный метод синтез ХДС, обладающий значительно меньшей вычислительной сложностью по сравнению с методами, рассмотренными в [144]. Синтез ХДС базируется на использовании наименьшего по значению первообразного элемента θ_j поля GF(P)) и задается Утверждением 2.1.

Утверждение 2.1. Пусть характер мультипликативной группы поля фиксируется функцией

$$\psi(a_i)=e^{j\pi U_i}, \tag{2.30}$$

тогда метод построения характеристического сигнала описывается следующими этапами.

1. Формируется массив элементов-чисел $A_i, i=\overline{0, P-2}$ поля GF(P):

$$A(i)=\Theta_j^i (\mathrm{mod}\, P). \tag{2.31}$$

2. Формируется группа чисел поля GF(P), сдвинутая по значениям на единицу, в соответствии с правилом:

$$H(i)=A(i)+1, \text{ если } \Theta_j^i+1 = 0(\mathrm{mod}\, P);$$

$$H(i)=1, \text{ если } \Theta_j^i+1\equiv 0(\mathrm{mod}\, P). \tag{2.32}$$

3. Формируется массив индексов $X(i), i=\overline{0, P-2}$, значениями которого являются соответствующие элементу поля индексы i+1, упорядоченные по содержимому с адресом:

$$A(i): X(i)=X\left[A(i)\right]. \tag{2.33}$$

4. Строится массив индексов J(i), значениями которого являются индексы массива X(i), выбранные по адресу $H(i): J(i)=X[H(i)], i=\overline{0, P-2}$.

5. Вычисляется характер элементов поля по правилу [144]:

$$\psi(a_i)=\psi[J(i)]=\begin{cases}1, \text{ если } J(i)\equiv 0(\mathrm{mod}\, 2);\\ -1, \text{ если } J(i)\equiv 0(\mathrm{mod}\, 2).\end{cases} \tag{2.34}$$

Приведем пример синтеза ХДС в соответствии с описанными выше этапами.

Пусть $P=13, L=12, \Theta_j=2$, Тогда

$$A(i) = \Theta_j^i (\text{mod } P) = \{1,2,4,8,3,6,12,11,9,5,10,7\};$$

$$i = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 5, 10, 11\}.$$

Упорядочим ряд $i+1 = \{1,2,3,4,5,6,7,8,9,5,10,11,12\}$ по закону (адресу) $\Theta_j^i = A(i)$. В соответствии с (2.31) - (2.33) получим массив индексов $X(i)=\{1,2,5,3,10,6,12,4,9,11,8,7\}$. Произведем выборку элементов-чисел из поля X(i) по адресу $H(i) = \Theta_j^i + 1(\text{mod } P) = \{2,3,5,9,4,7,1,12,10,6,11,8\}$.

В результате получим поле чисел $J(i)=\{2,5,10,9,3,12,1,7,11,6,8,4\}$. Вычисляя характер по правилу (2.12), получаем инверсию характеристического сигнала $W_{12} = \{1,-1,1,-1,-1,1,-1,-1,-1,1,1,1\}$. Инвертируя W_{12}, получаем базовый изоморфизм.

Доказательство утверждения 2.1. С выполнением шагов 1, 2 утверждения 2.1 обеспечивается формирование мультипликативной группы поля GF(P) $A(i) = \Theta_j^i + 1(\text{mod } P), i = \overline{0, P-2}$ и группы чисел H(i), сдвинутой по отношению к A(i) на единицу, т.е. $H(i) = \Theta_j^i + 1$. Рассмотрим шаги 3, 4 утверждения 2.1. В результате записи последовательность чисел i+1, сдвинутых на единицу индексов поля $A(i), i = \overline{0, P-2}$, по адресу Θ_j^i в массиве X(i) оказываются записанными по сравнению с соответствующими элементами поля GF(P) сдвинутые по значению на единицу числа-индексы. При считывании с массива X(i) в качестве индексов элементов-чисел с адресом $\Theta_j^i + 1$, индексы U_i, соответствующие элементам $A(i) = \Theta_j^i + 1$, также оказываются сдвинутыми на единицу [43], т.е. считываются индексы со значением U_i+1. Для получения же индексов U_i их нужно сдвинуть по значению на единицу, выполняя, как и ранее, все операции по модулю простого числа P. Однако сдвиг не выполняют, т.к. характер поля $\psi(a_k) = e^{j\pi(U_i+1)} = e^{j\pi} \cdot e^{j\pi U_i} = (\cos\pi + j\sin\pi)e^{j\pi U_i} = -e^{j\pi U_i}$, т.е. сдвиг на единицу индексов приводит к инверсной форме изоморфизма ХДС. Изложенное подтверждает справедливость шага 5. Таким образом, утверждение доказано.

В ходе исследований был разработан метод синтеза ХДС в расширенных полях Галуа.

Пусть $\varphi(a_i)$, $i = \overline{1, P^n - 1}$, есть поле Галуа $GF(P^n)$ степенью n расширения и элементами-полиномами, степень которых не превышает n, вычисляются над полем $GF(P)$, $\Phi_k(x)$ и θ_j – соответственно k-й первообразный примитивный полином и j-й первообразный элемент поля, функция характеров гомоморфного отображения элементов поля $GF(P^n)$ на поле $GF(2)$ зафиксирована функцией $\psi(a_i) = e^{j\pi u_i}$, причем элемент-полином поля a_i определяется из решения сравнения $a_i \equiv \theta_j^{u_i} (\mathrm{mod}\ \Phi_k(x),\ P)$, а u_i есть множество чисел-индексов, $u_i = \overline{0, P^n - 2}$, упорядоченных по возрастанию. Тогда основными этапами метода синтеза ХДС в поле $GF(P^n)$ являются следующие.

1) Формируется массив сдвинутых по значению индексов $u_i^{'} = u_i + 1, i = \overline{0, P^n - 2}$, упорядоченных по возрастанию, и массив элементов-полиномов a_i поля $GF(P^n)$:

$$A(i) = \theta_j^i (\mathrm{mod}\ \Phi_k(x),\ P). \qquad (2.35)$$

2) Формируется массив $H(i)$ элементов-полиномов поля $GF(P^n)$, сдвинутый по значениям на единицу относительно значений массива $A(i)$:

$$\begin{gathered} H(i) = A(i) + 1, \text{ если } \theta_j^i + 1 \neq 0 (\mathrm{mod}\ \Phi_k(x),\ P), \\ H(i) = 1, \text{ если } \theta_j^i + 1 \equiv 0 (\mathrm{mod}\ \Phi_k(x),\ P). \end{gathered} \qquad (2.36)$$

3) Массив индексов u_i записывается в массив $X(i)$ по адресам, определяемым значениями коэффициентов при полиномах $A(i)$ в P-ичной системе счисления.

4) Формируется массив индексов $J(i), i = \overline{0, P^n - 2}$, значениями которого являются индексы u_i, считанные из массива $X(i)$ с адресами, заданными значениями коэффициентов при элементах-полиномах $H(i)$ в P-ичной системе счисления.

5) Вычисляется для всех значений массива индексов J(i) двузначный характер

$$\psi(a_i) = \psi(\theta_j^i + 1) = -\psi(J(i)) = \begin{cases} 1, \text{ если } J(i) \equiv 0 (\mathrm{mod}\, 2), \\ -1, \text{ если } J(i) \neq 0 (\mathrm{mod}\, 2). \end{cases} \qquad (2.37)$$

Рассмотрим пример. Построим ХДС с параметрами:

$$L = 3^2 - 1, \text{ т.е. } P = 3 \text{ и } n = 2.$$

Используя [2], выберем $\Phi_k(\theta) = \theta^2 - \theta - 1$ и выполним расчеты в соответствии с шагами 1-5. Для этого запишем ряд сдвинутых индексов $u_i^{'}$ в массив $X(i)$.

$$u_i^{'} = u_i + 1 = \{1,2,3,4,5,6,7,8\}$$

по адресам, заданным коэффициентами при элементах-полиномах

$$A(i) = \theta_v^i (\mathrm{mod}\ \theta^2 - \theta - 1, 3) = \{1,\ \theta,\ \theta + 1, 2\theta + 1, 2, 2\theta, 2\theta + 2,\ \theta + 2\},$$

учитывая, что P = 3, т.е. подставляя вместо θ число P. Указанные коэффициенты принимают значения:

$$K_1^{'} = \{1,3,4,7,2,6,8,5\}.$$

Далее сформируем массив $H(i)$:

$$H(i) = A(i) + 1 = \{2,\ \theta + 1,\ \theta + 2, 2\theta + 2, 1, 2\theta + 1, 2\theta,\ \theta\}$$

и соответствующий массив коэффициентов $K_2^{'} = \{2,4,5,8,1,7,6,3\}$.

При этом массив коэффициентов формируется, например, для $2\theta + 2$, по правилу:

$$K_{2,4}^{'} = (2P + 2) \mathrm{mod} P^2 = 2 \cdot 3 + 2 = 8.$$

Сформируем массив $X(i)$:

$$X(i) = \{1,5,2,3,8,6,4,,7\}.$$

Считывая из массива $X(i)$ индексы по адресу $K_2^{'}$, получаем

$$J(i) = \{5,3,8,7,1,4,6,2\}.$$

Воспользовавшись правилом (2.15), синтезируем ХДС для длины

$$L = 3^2 - 1 = 8 : \psi(J(i)) = \{1,1,-1,1,1,-1,-1,-1\}.$$

Реализация всех этапов синтеза ХДС в расширенных полях Галуа сведены в таблице 2.1.

Таблица 2.1 − Синтез ХДС для $L = 3^2 - 1$

i	1	2	3	4	5	6	7	8
$A(i) = \theta_v^i$	1	θ	$\theta+1$	$2\theta+1$	2	2θ	$2\theta+2$	$\theta+2$
$K_1^{'}$	1	3	4	7	2	6	8	5
H(i)	2	$\theta+1$	$\theta+2$	$2\theta+2$	1	$2\theta+1$	2θ	θ
$K_2^{'}$	2	4	5	8	1	7	6	3
X(i)	1	5	2	3	8	6	4	7
J(i)	5	3	8	7	1	4	6	2
$\psi(J(i))$	1	1	-1	1	1	-1	-1	-1

Вычислительная сложность метода синтеза сигналов (время t_c построения) ХДС, как следует из утверждения 2.1, может быть определена из выражения:

$$t_c = L(t_y + t_{сл} + t_{ср} + 4t_{сч} + t_з) = L\left(t_y + t_{сл} + t_{ср} + 5t_з\right). \qquad (2.38)$$

В выражении (2.38) учтено, что время, необходимое для выполнения операций записи ($t_з$) и считывания ($t_{сч}$) равны. Анализ (2.38) показывает, что время построения ХДС предложенным методом линейно зависит от периода формируемой последовательности, тогда как для известного метода (выражение (2.29)), зависимость - квадратичная.

Выигрыш во времени синтеза нелинейных сигналов в конечных полях с применением разработанных методов по сравнению с известным методом составляет: для периода L = 256, - 25,5 раз; для периода L = 1018 -106,5 раза; для периода L = 4000 - 417 раза; для периода L = 9972 – 1039,6 раза.

В ходе исследований была разработана программная модель синтеза характеристических дискретных сигналов в простых и расширенных полях Галуа. Выполнено компьютерное моделирование параметров, используемых при синтезе

системы: первообразные элементы поля, примитивные полиномы степени n, простые числа. Указанные программные средства приведены в Приложениях А и Б.

В ходе исследований разработаны технические решения, реализующие предложенные методы синтеза ХДС в простых и расширенных полях Галуа, на которые получены 4 авторских свидетельства на изобретение [39-42], что подтверждает мировую новизну и практическую значимость полученных в диссертации научных результатов.

2.3 Разработка усовершенствованного метода синтеза всей системы нелинейных дискретных сигналов в конечных полях Галуа

В разделе предлагается метод построения характеристического кода, обладающий меньшей вычислительной сложностью по сравнению с методом, основанном на использовании разностного множества [144] с инверсно-изоморфными коэффициентами, который базируется на формировании изоморфизма характеристического кода с применением предварительно построенных таблиц, устанавливающих связи индексов и характеров элементов поля.

Предлагаемый метод построения системы изоморфизмов для числа элементов кода N задаётся следующим утверждением.

Утверждение 2.2. Если характеристический код $\{W_i\}, i=\overline{1,N}$ с числом элементов (периодом) N подвергнуть операции децимации с коэффициентом децимации C, где C - взаимно простое с N ($C \in \phi(N)$), то результирующая последовательность (код) $\{v_i\}$ является изоморфизмом кода $\{w_i\}$.

Процедура децимации означает выбор каждого C- го символа кода $\{w_i\}$ и запись полученных таким образом символов, так что

$$v_i = (w_i + C) \bmod N. \qquad (2.39)$$

Рассмотрим пример получения последовательности v_i с числом элементов $N=10$. Пусть один из изоморфизмов характеристического кода имеет вид

$$w_i = \{-1,1,1,1,-1,1,-1,-1,1,-1\}. \qquad (2.40)$$

Для $N=10$ коэффициенты децимации C, в соответствии с ограничениями утверждения, - это числа взаимно простые с N. Для нашего примера $\{C\}=1,3,7,9$. Выполняя операцию децимации над строкой w_i в соответствии с (2.39) по коэффициенту децимации, например, $C=7$, т. е. считывая каждый седьмой символ кода (2.40), получим код

$$v_i = \{-1,-1,1,1,1,1,-1,-1,1,-1\}. \qquad (2.41)$$

Приведём доказательство утверждения 2.2.

Правило кодирования для характеристического кода можно представить в виде [144]

$$\psi\left(a_\nu^w\right) = \psi\left(\Theta_i^\nu + 1\right) = e^{j\cdot\pi\cdot u_\nu}, \qquad (2.42)$$

где: Θ - есть i-й первообразный элемент поля;

u_ν - ν-й индекс элемента поля, $\nu = \overline{1, N-1}$;

$\psi(x)$ - характер мультипликативной группы поля $GF\left(p^n\right)$.

Правило кодирования для метода децимации имеет вид

$$\psi\left(a_{\nu\cdot c}^\nu\right) = \psi\left(\Theta_i^{\nu\cdot c} + 1\right) = e^{j\cdot\pi\cdot u_{\nu\cdot c}}. \qquad (2.43)$$

Вычислим характер элементов поля для правил (2.42) - (2.43) и запишем результаты в виде таблицы (Табл. 2.1 – 2.2). После замены переменных $\Theta_i^{C\nu} = \Theta_C^\nu$ содержимое таблицы 2.2 примет вид (см. табл.2.3). Вычисление характеров элемента поля в соответствии с (2.42) приводит к изоморфизму характеристического кода. Но, если для табл. 2.3 Θ - первообразный элемент поля $GF\left(p^n\right)$, то вычисление характеров в соответствии с (2.43) также приводит к изоморфизму.

Таблица 2.1 - Значение характеров элементов поля для правила (2.42)

ν	$\psi(a_i)$
$\nu=0$	$\psi(a_0)=\psi(2),$
$\nu=1$	$\psi(a_1)=\psi(\Theta_i+1),$
$\nu=2$	$\psi(a_2)=\psi(\Theta_i^2+1),$
$\nu=l$	$\psi(a_l)=\psi(\Theta_i^l+1),$
$\vdots$	
$\nu=N-1$	$\psi(a_{N-1})=\psi(\Theta_i^{N-1}+1)$

Таблица 2.2 - Значение характеров элементов поля для правила (2.43)

ν	$\psi(a_i)$
$\nu=0$	$\psi(a_0)=\psi(2),$
$\nu=1$	$\psi(a_1)=\psi(\Theta_i^C+1),$
$\nu=2$	$\psi(a_2)=\psi(\Theta_i^{2C}+1),$
$\nu=l$	$\psi(a_l)=\psi(\Theta_i^{lC}+1),$
$\vdots$	
$\nu=N-1$	$\psi(a_{N-1})=\psi(\Theta_i^{(N-1)C}+1)$

Таблица 2.3 - Значение характеров элементов поля при $\Theta_i^{C\nu}=\Theta_C^{\nu}$

ν	$\psi(a_i)$
$\nu=0$	$\psi(a_0)=\psi(2),$
$\nu=1$	$\psi(a_1)=\psi(\Theta_C+1),$
$\nu=2$	$\psi(a_2)=\psi(\Theta_C^2+1),$
$\nu=l$	$\psi(a_l)=\psi(\Theta_C^l+1),$
$\vdots$	
$\nu=N-1$	$\psi(a_{N-1})=\psi(\Theta_C^{N-1}+1)$

Известно, что период E первообразного элемента поля является максимальным, т. е. $E = p^n - 1 = N$. Очевидно, что период элемента Θ_C есть

$$\Theta_C = E/(E,C), \tag{2.44}$$

где (E,C) - наибольший общий делитель (НОД) чисел E и C.

При $(E,C)=1$, как следует из (2.44), Θ_C имеет максимальный период E, а значит, реализация операций, приведенных в табл. 3, приводит к изоморфизму.

Утверждение доказано.

Есть ещё одна возможность доказать приведенное утверждение. Для этого достаточно доказать, что характеристический код $\{w_i\}$, построенный на основе разностного множества, с точностью до циклического сдвига (автоморфизма) совпадает с кодом $\{v_i\}$, построенным по правилу (2.23).

Для кодов с двухуровневой периодической функцией автокорреляции (ПФА) каждому коду можно поставить в соответствие разностное множество, сбалансированное на два уровня B. Разностным множеством, сбалансированным на два уровня

$$B = \{b_1, b_2, ..., b_{k^+}\}, \tag{2.45}$$

называется подмножество $K+$ целых чисел по модулю N, такое, что разность $d_i - d_u (\mathrm{mod}\, N), i \neq U, i, U = 1,2,...,k^+$, принимает каждое из n_1 различных значений из множества чисел $1,2,...,N-1$ точно λ_1, раз и $n_2 = N - n - 1$ других различных значений из этого же множества чисел точно λ_2 раз.

Если ввести понятие коэффициента $t : (t, N) = 1$ и определить множества .. и B_s следующим образом

$$\begin{aligned} B_t &\equiv tB(\mathrm{mod}\, N) = \{tb_1, tb_2, ..., tb_{k^+}\} \mathrm{mod}\, N \\ B_s &\equiv \{b_1 + S, b_2 + S, ... + b_k + S\} \mathrm{mod}\, N \end{aligned}, \tag{2.46}$$

то можно доказать, что множества B_t и B_s также являются разностными множествами, сбалансированными на два уровня, с теми же параметрами

$N, k, ^{+}, \lambda_1, \lambda_2$, что и множество B. И в этом случае в зависимости от выбора коэффициента t в преобразовании (2.46) множества B_t и B_s могут быть автоморфными или изоморфными. Таким образам, число изоморфизмов разностного множества, сбалансированного на два уровня, равно числу непересекающихся классов коэффициентов t.

С учётом (2.45) и (2.46) идентичность методов построения характеристического кода можно представить в виде

$$B_t = \left\{tb_1, tb_2, \ldots, tb_{k^+}\right\} \bmod N \Leftrightarrow SOD\left[v_i\left(\zeta + C_l\right) \bmod N\right], \qquad (2.47)$$

где: символ $\Leftrightarrow$ - означает, что члены строки (2.47) совпадут с точностью до циклического сдвига;

оператор SOD означает размещение символа сигнала $[v_i]$, образуемого путем децимации, на позиции $\left(\zeta + C_l\right) \bmod N$;

ζ - есть величина ($\zeta = \overline{1, N}$), определяющая автоморфизм кода.

Покажем справедливость (2.47). Для этого представим данное выражение в виде двух числовых рядов:

$$tb_1, tb_2, tb_3, \ldots, tb_{k^+}, \qquad (2.48)$$

и

$$\zeta + C_l, \zeta + 2C_l, \zeta + 3C_l, \ldots, \zeta + NC_l. \qquad (2.49)$$

Ряд (2.27) содержит N членов, т. е. в два раза больше, чем в (2.48), так как ввиду сбалансированности характеристических сигналов по числу символов 1 и -1 $N = 2k^+$. При этом k^+ чисел будут определять позиции символов -1.

Далее доказательство проведём, задаваясь конкретными параметрами N, $T = \{t\}$, $C = \{c\}$ и Θ.

Пример 1. Пусть $N = 10$, $\Theta = 2$. Изоморфизм для данных параметров имеет вид: $w_i = \{-1,1,1,1,-1,1,-1,-1,1,-1\}$, а множество коэффициентов: $T = \{1,3,7,9\}$. Построенные с использованием метода разностных множеств по множеству коэффициентов T характеристические коды, имеют вид

$$w^1_{t=1} = \{-1,1,1,1,-1,1,-1,-1,1,-1\},$$
$$w^2_{t=3} = \{-1,-1,-1,1,1,1,1,-1,-1,1\},$$
$$w^3_{t=7} = \{-1,1,-1,-1,1,1,1,1,-1,-1\},$$
$$w^4_{t=9} = \{-1,-1,1,-1,-1,1,-1,1,1,1\}.$$

Не инверсные и инверсные изоморфизмы характеристического кода, построенные на основе использования метода децимации, имеют вид

$$v^1_{c=1} = \{1,1,1,-1,1,-1,-1,1,-1,-1\},$$
$$v^2_{c=3} = \{1,-1,-1,1,1,1,1,-1,-1,-1\},$$
$$v^3_{c=7} = \{-1,-1,1,1,1,1,-1,-1,1,-1\},$$
$$v^4_{c=9} = \{-1,1,-1,-1,1,-1,1,1,1,-1\}.$$

На рис. 2.1 представлен граф соответствий множеств w_i и v_i. Анализ рис. 3.1 указывает на соответствие изоморфизмов, построенных по рассматриваемым методам. На рис. 3.1 введены обозначения: оператор $\overline{T}$ означает зеркальное отображение изоморфизмов, полученных по различным методам; $\overline{T}^{-r}$ - зеркальное отображение со сдвигом влево на r символов кода; T^{-r} - на r единиц влево; T^r - на r единиц вправо. На рис. 2.2 приведен граф соответствий между изоморфизмами для исследуемых методов построения характеристических кодов для $N = 48$ без детализации зеркального отображения и сдвигов изоморфизмов.

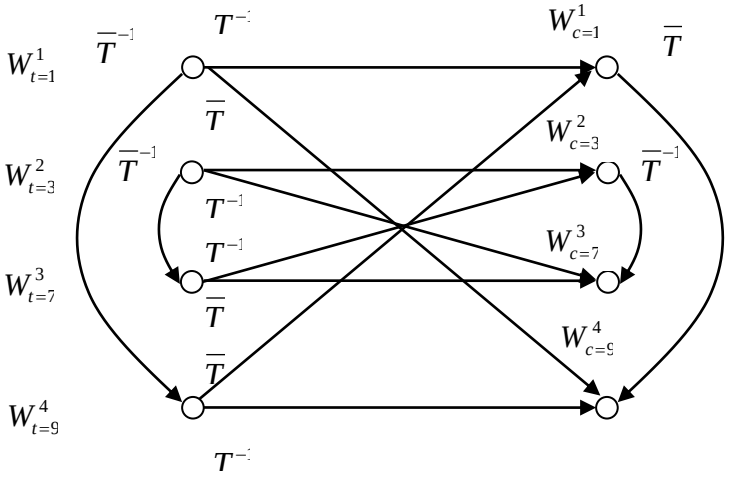


Рисунок 2.1 - Граф соответствий изоморфизмов, построенных методами децимации и разностного множества при $N = 10$

Выполним оценку вычислительной сложности ($T_{дец}$) метода децимации. Для формирования изоморфизма характеристического кода необходимо реализовать

(в соответствии с (2.17)) операции выборки элементов по коэффициенту децимации. Время выполнения данных операций обозначим соответственно $t_{выб}$ и $t_{слож}$. Тогда вычислительная сложность ($T_{дец}$) метода децимации, может быть оценена с помощью выражения:

$$T_{дец} = N\left(t_{слож} + t_{выб}\right). \qquad (2.50)$$

Анализ операций, выполняемых при реализации метода разностных множеств показывает, что вычислительная сложность последнего ($T_{разн.мн.}$) определяется из соотношения:

$$T_{разн.мн.} = N\left(2t_{сч} + t_{ср} + 0,5t_{умн}\right), \qquad (2.51)$$

где $t_{сч}$, $t_{ср}$, $t_{умн}$ - время выполнения операций считывания, сравнения, умножения соответственно.

В таблице 2.4 приведены значения выигрыша достигаемого при использовании разработанного метода синтеза всей системы нелинейных сигналов по сравнению с известным методом, основанном на теории разностных множеств.

Таблица 2.4 Оценки быстродействия метода синтеза сигналов на основе операции децимации

Период последовательности, параметры синтеза	Метод децимации	Метод разностных множеств
L=1020, P=1021, $\Theta = 2, \phi(N)$ = 256	0.134 сек	2.199 сек
L=2052, P=2053, $\Theta = 2$, $\phi(N)$ = 648	0.585 сек	13.072 сек
L = 2380, P = 2381, $\Theta = 2$, $\phi(N)$ = 768	0.875 сек	22.762 сек.

Анализ данных таблицы 2.4 показывает, что разработанный метод синтеза всей системы нелинейных дискретных сигналов на основе операции децимации и считывания элементов последовательности существенно превосходит по быстродействию известный метод разностных множеств. Так для периода сигнала 2380 элементов выигрыш во времени составляет более 28 раз.

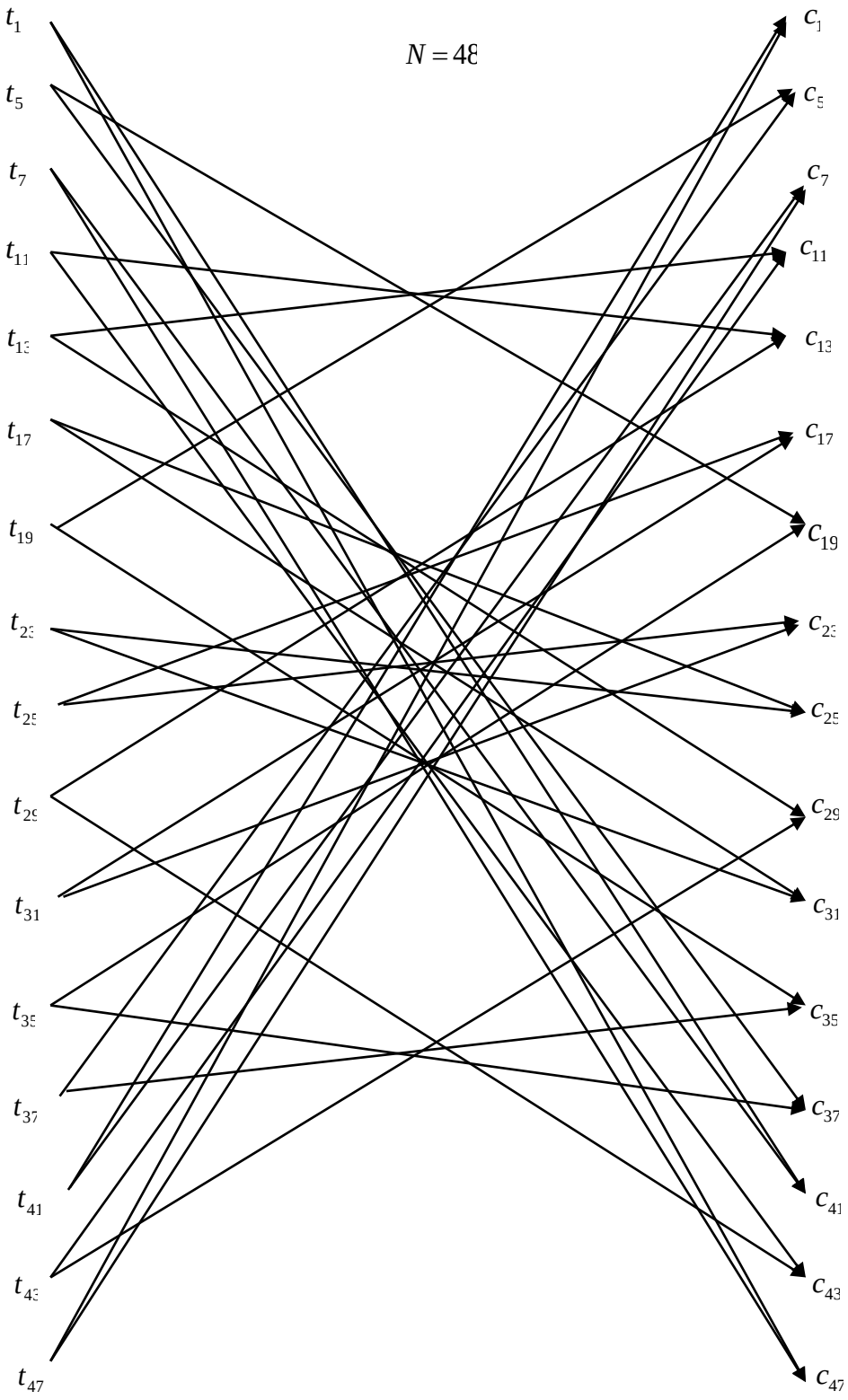


Рисунок 2.2 - Граф соответствий изоморфизмов, построенных методами децимации и разностного множества при $N = 48$

В ходе исследований была разработана программная модель полученного метода синтеза всей системы нелинейных сигналов в конечных полях (Приложение А). Выполнено компьютерное моделирование параметров, используемых при синтезе системы: первообразные элементы поля, примитивные полиномы степени n, коэффициенты децимации и др. (Приложение Б).

В ходе исследований разработаны технические решения, реализующие предложенные методы синтеза всей системы нелинейных сигналов в простых и расширенных полях Галуа на основе операции децимации и считывания элементов последовательности, на которые получено авторское свидетельство на изобретение [38], что подтверждает мировую новизну и практическую значимость полученных в диссертации научных результатов.

2.4 Синтез нелинейных производных дискретных сигналов в конечных полях Галуа

Системы нелинейных дискретных сигналов являются плотноупакованными по периодической функции корреляции (ПФАК), существуют для большого спектра длительностей N, однако размерность ансамбля ХДС ограничена. Например, для нелинейных сигналов характеристического типа, функцией Эйлера. Проведенные исследования показали [60], что дальнейшее увеличение размерности ансамбля и улучшение структурных свойств сигналов, составляющих ансамбль, может быть достигнуто на основе использования L-позиционных (производных) нелинейных сигналов, построение которых осуществляется посредством образования последовательного произведения $Z_i, i = \overline{1,k}$, символов W_j^i нелинейных сигналов с одно- или двухуровневой ПФАК.

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

$$W_i^p = \prod_{j=1}^{k} W_{i(\mathrm{mod}\, L_i),j}\,. \qquad (2.52)$$

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

$$R_w^p(l)=\sum_{i=0}^{L-1}\prod_{j=r}^{K_1} W_{i(\mathrm{mod}L_i),j}\prod_{j=1}^{K_2} W_{i+l(\mathrm{mod}L_i),j}, \qquad (2.53)$$

где в общем случае $K_1\neq K_2$.

Анализ корреляционных свойств с использованием (2.53) в общем виде затруднен, поэтому рассмотрим ряд частных случаев, важных как с теоретической, так и с практической точки зрения.

1. Пусть $K_1=K_2$, а $L_1\neq L_2$, тогда (2.53) имеет вид

$$R_w(l)=\sum_{i=0}^{L-1} W_{i(\mathrm{mod}L_1),i}\cdot W_{i+l(\mathrm{mod}L_1),1}\cdot W_{i(\mathrm{mod}L_1),2}\cdot W_{i+l(\mathrm{mod}L_2),2}. \qquad (2.54)$$

Для преобразования (2.54) представим индекс суммирование i в L_2-р ичной системе счисления

$$i=\upsilon L_2+\varepsilon,\quad 0\le\varepsilon\le L_2,\ 0\le\upsilon\le L_1 \qquad (2.55)$$

$$R_w(l)=\sum_{\upsilon=0}^{L_1-1}\sum_{\varepsilon=0}^{L_2-1} W_{\upsilon L_2+\varepsilon(\mathrm{mod}L_1),1}\cdot W_{\upsilon L_2+\varepsilon(\mathrm{mod}L_2),2}\cdot W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}L_1),2}\cdot W_{\upsilon L_2+\varepsilon l(\mathrm{mod}L_2),2}=\sum_{\varepsilon=0}^{L_1-1} W_{\varepsilon(\mathrm{mod}L_1),1}\cdot \qquad (2.56)$$

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

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

$$\sum_{\varepsilon=0}^{L_2-1} W_{\varepsilon(\mathrm{mod}L_2),2}\cdot W_{\varepsilon+l(\mathrm{mod}L_2),2}=R_{W_2}(l) \qquad (2.57)$$

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

$$\sum_{\varepsilon=0}^{L_1-1} W_{\upsilon L_2+\varepsilon(\mathrm{mod}L_1),1}\cdot W_{\upsilon L_2+\varepsilon+l(\mathrm{mod}L_1),1}=\sum_{q=0}^{L_1-1} W_{q(\mathrm{mod}L_1),1}\cdot W_{q+\varepsilon(\mathrm{mod}L_1),1}=R_{W_1}(l) \qquad (2.58)$$

и ПФАК ПНС может быть рассчитана с использованием выражения

$$R_{W^n}(l)=R_{W_1}(l)\cdot R_{W_2}(l). \qquad (2.59)$$

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

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\bmod L); \\ L_2 R_{W_1}(l), \quad \text{при } l\equiv 0(\bmod L_2),\ L\neq 0\ (\bmod L_1); \\ L_1 R_{W_2}(l), \quad \text{при } l\equiv 0(\bmod L_1),\ l\neq 0(\bmod L_2); \\ R_{W_1}(l)\cdot R_{W_2}(l), \quad \text{при } l\neq 0(\bmod L_1, \bmod L_2). \end{cases} \tag{2.60}$$

Анализ (2.60) показывает, что минимальные боковые лепестки ПНС достигаются в случае, если L_2, $R_{w_1}(l)$, L_1, $R_{w_2}(l)$ принимают минимальные значения.

2. Пусть $K=3$, а $L_1\neq L_2\neq L_3$. В этом случае по аналогии с (2.60) выражение (2.53) можно представить в виде

$$R_{W^n}(l)=R_{W_1}(l)\cdot R_{W_2}(l)\cdot R_{W_3}(l), \tag{2.61}$$

или

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\bmod L); \\ R_{W_1}(l)\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\neq 0(\bmod L_1, L_2, L_3); \\ L_1\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\bmod L_1),\ l\neq 0(\bmod L_2, L_3); \\ L_2\cdot R_{W_1}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\bmod L_2),\ l\neq 0(\bmod L_1, L_3); \\ L_3\cdot R_{W_1}(l)\cdot R_{W_2}(l), \quad \text{при } l\equiv 0(\bmod L_3),\ l\neq 0(\bmod L_1, L_2); \\ L_1\cdot R_{W_2}(l)\cdot L_3, \quad \text{при } l\equiv 0(\bmod L_1, L_3),\ l\neq 0(\bmod L_2); \\ L_1\cdot L_2\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\bmod L_1, L_2),\ l\neq 0(\bmod L_3); \\ R_{W_1}(l)\cdot L_2\cdot L_3, \quad \text{при } l\equiv 0(\bmod L_2, L_3),\ l\neq 0(\bmod L_1). \end{cases} \tag{2.62}$$

Рассмотрение (2.62) показывает, что для минимизации $R_{W^n}(l)$ необходимо и достаточно, чтобы $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W3}(l)$ были минимальными, а L_1, L_2 и L_3 – минимальными и взаимно простыми. Минимальное значение R_{W_i}, $i=\overline{1,3}$, равное 0 и достигается только при использовании в качестве W_1 последовательности [58] вида {1 1 1 -1}. В этом случае выражение (2.62) принимает вид

$$R_{W^n}(l)=\begin{cases} L, \quad \text{при } l\equiv 0(\bmod L); & \text{а)} \\ L_1\cdot R_{W_2}(l)\cdot R_{W_3}(l), \quad \text{при } l\equiv 0(\bmod L_1),\ l\neq 0(\bmod L_2, L_3); & \text{б)} \\ L_1\cdot R_{W_3}(l)\cdot L_2, \quad \text{при } l\equiv 0(\bmod L_1, L_2),\ l\neq 0(\bmod L_3); & \text{в)} \\ L_1\cdot R_{W_2}(l)\cdot L_3, \quad \text{при } l\equiv 0(\bmod L_1, L_3),\ l\neq 0(\bmod L_2). & \text{г)} \end{cases} \tag{2.63}$$

Исследование выражений (2.63 а, б и г) показывает, что для их минимизации необходимо, чтобы как принимаемые значения ПФАК $R_{W_1}(l)$, $R_{W_2}(l)$ и $R_{W_3}(l)$, так и значения их длительностей были бы минимальными. С учетом того, что $L_1 = 4$, максимальные значения ПФАК $R_W(l)$ дают слагаемые в) и г). Если L_2 и L_3 – взаимно простые, то минимальные значения $R_{W_2}(l)$ и $R_{W_3}(l)$ могут быть соответственно равны $\{\pm 1\}$ и $\{-4, 0\}$ или $\{0, 4\}$, или $\{2, -2\}$, поэтому

$$R_{W^n}(l) = \begin{cases} L, \quad \text{при } l \equiv 0(\bmod L); & \text{а)} \\ \pm 4, \quad \text{при } l \equiv 0(\bmod L_1), l \neq 0(\bmod L_2, L_3); & \text{б)} \\ \pm 4L_1L_2, \quad \text{при } l \equiv 0(\bmod L_1, L_2), l \neq 0(\bmod L_3); & \text{в)} \\ \pm L_1L_3, \quad \text{при } l \equiv 0(\bmod L_1, L_3), l \neq 0(\bmod L_2). & \text{г)} \end{cases} \qquad (2.64)$$

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

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

$$R_{W^n}(l) = \begin{cases} L, \quad \text{при } l \equiv 0(\bmod L); \\ R_{W_1}(l) \cdot R_{W_2}(l) \cdot R_{W_3}(l), \quad \text{при } l \neq 0(\bmod L_1, L_2, L_3); \\ L_1 \cdot R_{W_2}(l) \cdot R_{W_3}(l), \quad \text{при } l \equiv 0(\bmod L_1), l \neq 0(\bmod L_2, L_3); \\ L_2 \cdot R_{W_1}(l) \cdot R_{W_3}(l), \quad \text{при } l \equiv 0(\bmod L_2), l \neq 0(\bmod L_1, L_3); \\ L_3 \cdot R_{W_1}(l) \cdot R_{W_2}(l), \quad \text{при } l \equiv 0(\bmod L_3), l \neq 0(\bmod L_1, L_3). \end{cases} \qquad (2.65)$$

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

$$R_{W_n}(l) = \sum_{i=0}^{L-1} \prod_{j=1}^{K} W_{i,j}^{q} \prod_{j=1}^{K} W_{i+l,j}, \qquad (2.66)$$

причем (2.66) позволяет вычислить ПФАК, если положить, что $q = r$.

Проведенные исследования показали, что для (2.66) можно получить оценки, если воспользоваться теорией двухзначных характеров, в частности, тем, что для любого нетривиального характера справедливо [6,148]

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

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

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

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

либо (2.67)

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

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

Приведем вывод аналитического выражения для ПФАК ПНС.

Используя (15) и полагая, что $q \neq r$, имеем

$$R_{W_n}(l) = \sum_{i=0}^{L-1} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1). \qquad (2.68)$$

С учетом того, что $\Psi(0) = 0$, [148], при $1 \neq 0 (\mathrm{mod}\, L)$

$$R_{W_n}(l) = \sum_{i=0}^{P^n - 2} \Psi(\Theta_q^i + 1) \cdot \Psi(\Theta_q^{i+l} + 1) \cdot \Psi(\Theta_r^{i+l} + 1) \pm Z \qquad (2.69)$$

где Z – учитывает сумму слагаемых, входящих в (17), для которых

$$\left(\Theta_q^i + 1\right) \equiv 0 \vee \left(\Theta_q^{i+l} + 1\right) \equiv \left(\Theta_r^i + 1\right) \equiv \left(\Theta_r^{i+1} + 1\right) \equiv 0 [\mathrm{mod}\, f_m(x), P] \qquad (2.70)$$

Более точно структуру (2.70) определяют сформулированные ниже утверждения.

Утверждение 2.3. Пусть $\Theta_{\upsilon}^{i}+1$ и $\Theta_{\upsilon}^{i+1}+1$ есть элементы поля $GF(P^n)$ а $\Theta_{\upsilon}^{\upsilon}$ – υ-ый первообразный элемент, тогда при $l' \neq 0(\mathrm{mod}\, L)$ $\Theta_{\upsilon}^{i}+1$ и $\Theta_{\upsilon}^{i+l}+1$ никогда не сравнимы с $0[\mathrm{mod}\, f_m(x), P]$. Доказательство утверждения следует из цикличности поля $GF(P^n)$ [4].

Утверждение 2.4 Пусть $\Theta_{\upsilon}^{r}+1$ и $\Theta_{k}^{m}+1$ – элементы поля $GF(P^n)$, а Θ_{υ} и Θ_{k} – первообразные. Существуют T^{s1} и T^{s2} автоморфные преобразования, при которых

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

Доказательство утверждения следует из авто- и изоморфных свойств поля $GF(P^n)$ [148].

С учетом утверждения (17) и (18) выражение (19) распадается на следующие логические высказывания.

$$\begin{aligned}
&\Theta_{q}^{i}+1 \equiv 0 \wedge \Theta_{q}^{i+l}+1 \equiv 0 \wedge \Theta_{r}^{i+l} \neq 0(\mathrm{mod}\, L); && \text{а)}\\
&\Theta_{q}^{i}+1 \equiv 0 \wedge \Theta_{q}^{i+l}+1 \neq 0 \wedge \Theta_{r}^{i}+1 \equiv 0 \wedge \Theta_{r}^{i+l}+1 \neq 0(\mathrm{mod}\, L); && \text{б)}\\
&\Theta_{q}^{i}+1 \equiv 0 \wedge \Theta_{q}^{i+l}+1 \neq 0 \wedge \Theta_{r}^{i}+1 \neq 0 \wedge \Theta_{r}^{i+l}+1 \equiv 0(\mathrm{mod}\, L); && \text{в)}\\
&\Theta_{q}^{i}+1 \neq 0 \wedge \Theta_{q}^{i+l}+1 \equiv 0 \wedge \Theta_{r}^{i}+1 \neq 0 \wedge \Theta_{r}^{i+l}+1 \neq 0(\mathrm{mod}\, L); && \text{г)}\\
&\Theta_{q}^{i}+1 \neq 0 \wedge \Theta_{q}^{i+l}+1 \equiv 0 \wedge \Theta_{r}^{i}+1 \equiv 0 \wedge \Theta_{r}^{i+l}+1 \neq 0(\mathrm{mod}\, L); && \text{д)}\\
&\Theta_{q}^{i}+1 \neq 0 \wedge \Theta_{q}^{i+l}+1 \equiv 0 \wedge \Theta_{r}^{i}+1 \neq 0 \wedge \Theta_{r}^{i+l}+1 \equiv 0(\mathrm{mod}\, L); && \text{е)}\\
&\Theta_{q}^{i}+1 \neq 0 \wedge \Theta_{q}^{i+l}+1 \neq 0 \wedge \Theta_{r}^{i}+1 \equiv 0 \wedge \Theta_{r}^{i+l}+1 \neq 0(\mathrm{mod}\, L); && \text{ж}\\
&\Theta_{q}^{i}+1 \neq 0 \wedge \Theta_{q}^{i+l}+1 \neq 0 \wedge \Theta_{r}^{i}+1 \neq 0 \wedge \Theta_{r}^{i+l}+1 \equiv 0(\mathrm{mod}\, L). && \text{з)}
\end{aligned} \qquad (2.71)$$

Анализ (2.71) показывает, что исключающими являются высказывания а), г), ж), з), поэтому

$$\begin{aligned}
&Z = \Psi\left(-\Theta_{q}^{i+l}+1\right)\cdot\Psi\left(-\Theta_{r}^{i}+1\right)\cdot\Psi\left(-\Theta_{r}^{i+l}+1\right)+\Psi\left(-\Theta_{q}^{-l}+1\right)\cdot\Psi\left(\Theta_{r}^{i}+1\right),\\
&\Psi = \left(\Theta_{r}^{i+l}+1\right)+\Psi\left(-\Theta_{r}^{l}+1\right)\cdot\Psi\left(\Theta_{q}^{i}+1\right)\Psi\left(\Theta_{q}^{i+l}+1\right)+\\
&+\Psi\left(-\Theta_{r}^{-l}+1\right)\Psi\left(\Theta_{q}^{i}+1\right)\Psi\left(\Theta_{q}^{i+l}+1\right)
\end{aligned}. \qquad (2.72)$$

Действительно, если истинно выражение (2.71), а), то $\Psi\left(\Theta_q^i+1\right)=0$, так как $\Theta_q^i+1\equiv 0(\mathrm{mod}\,L)$ [144], поэтому

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

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

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

Преобразуем выражение (2.69), используя свойство характера Ψ [Альберт], обозначив его переменной X:

$$\begin{aligned}X&=\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^i+1\right)\cdot\Psi\left(\Theta_q^{i+1}+1\right)\cdot\Psi\left(\Theta_r^i+1\right)\cdot\Psi\left(\Theta_r^{i+1}+1\right)=\\&=\Psi\left(\Theta_q^i\right)\cdot\Psi\left(\Theta_r^i\right)\sum_{i=0}^{P^n-2}\Psi\left(\Theta_q^i+1\right)\cdot\Psi\left(\Theta_q^i+\Theta_q^{-1}\right)\cdot\Psi\left(\Theta_r^i+1\right)\cdot\Psi\left(\Theta_r^i+\Theta_r^{-1}\right)=\Psi\left(\Theta_q^l\right)\cdot\Psi\left(\Theta_r^l\right)\cdot Q\end{aligned}\qquad(2.73)$$

Проанализируем выражение

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

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

$$Q=\sum_{a_i,b_i\in GF(P^n)}\Psi\left(a_i+1\right)\cdot\Psi\left(a_i+\Theta_q^{-1}\right)\cdot\Psi\left(b_i+1\right)\cdot\Psi\left(b_i+\Theta_r^{-1}\right).\qquad(2.74)$$

Полагая в (2.74) $c_i=a_i+1$ и $d_i=b_i+1$, проанализируем все c_i и d_i, если a_i и b_i пробегают при изменении все ненулевые элементы поля $GF(P^n)$, то c_i и d_i так же пробегают все ненулевые элементы поля $GF(P^n)$ исключая 1, поэтому

$$Q=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 1(\mathrm{mod}\,P)}}\Psi\left(c_i\right)\cdot\Psi\left(c_i+\Theta_q^{-1}+1\right)\cdot\Psi\left(d_i\right)\cdot\Psi\left(d_i+\Theta_r^{-1}-1\right).\qquad(2.75)$$

Если же $c_i=1$, то $Q_1=\Psi\left(\Theta_1^{-1}\right)\Psi\left(d_i\right)\Psi\left(d_i+\Theta_r^{-1}-1\right)$; а) (2.76)

$$d_i = 1, \quad \text{то } Q_2 = \Psi(c_i)\Psi\left(c_i + \Theta_q^{-1} - 1\right)\Psi\left(\Theta_r^{-1}\right); \qquad \text{б)}$$

$$c_i = 1, d_i = 1, \quad \text{то } Q_3 = \Psi\left(\Theta_q^{-1}\right)\Psi\left(\Theta_q^{-1}\right)\Psi\left(\Theta_r^{-1}\right); \qquad \text{в)}$$

Исключим в (2.76) условие $c_i, d_i \neq 1(\mathrm{mod}\, P)$, для этого добавим в него и вычтем Q_1, Q_2 и Q_3. В результате получим

$$\begin{aligned} Q = &\sum \Psi(c_i)\Psi\left(c_i + \Theta_q^{-1} - 1\right)\Psi(d_i)\Psi\left(d_i + \Theta_r^{-1}\right) - \Psi\left(\Theta_q^{-1}\right)\Psi(d_i)\Psi\left(d_i + \Theta_r^{-1} - 1\right) - \\ &-\Psi(c_i)\Psi\left(c_i + \Theta_q^{-1} - 1\right)\Psi\left(\Theta_r^{-1}\right) - \Psi\left(\Theta_q^{-1}\right)\Psi\left(\Theta_r^{-1}\right) = \\ &= \sum_{\substack{c_i, d_i \in GF(P^n) \\ c_i, d_i \neq 0(\mathrm{mod}\, P)}} \Psi\left(c_i^{\,2}\right)\Psi\left(1 + \left(\Theta_q^{-1} - 1\right)c_i^{-1}\right)\Psi\left(d_i^{\,2}\right)\Psi\left[1 + \left(\Theta_r^{-1} - 1\right)d_i^{-1}\right] - Q_1 - Q_2 - Q_3. \end{aligned} \qquad (2.77)$$

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

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

С учетом (2.72), (2.74), (2.76), выражение (2.69) есть:

$$\begin{aligned} R_{W^n}(l) = &\Psi\left(\Theta_q^l\right)\Psi\left(\Theta_r^l\right)\{\sum_{\substack{x_i, y_i \in GF(P^n) \\ x_i, y_i \neq 0(\mathrm{mod}\, P)}} \Psi(1 + q_i x_i)\Psi(1 + q_2 y_1) - [\Psi\left(\Theta_q^{-l}\right)\cdot\Psi(d_i)\Psi\left(d_i - \Theta_r^{-l} - 1\right) + \\ &+\Psi(c_i)\Psi\left(c_i + \Theta_q^{-1} - 1\right)\Psi\left(\Theta_r^{-1}\right) + \Psi\left(\Theta_q^{-1}\right)\Psi\left(\Theta_r^{-1}\right)]\} + \{\Psi\left(-\Theta_q^l + 1\right)\Psi\left(\Theta_q^i + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_q^{-1} + 1\right)\Psi\left(\Theta_r^i + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \Psi\left(-\Theta_r^l + 1\right)\Psi\left(\Theta_q^i + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_r^{-1} + 1\right)\Psi\left(\Theta_r^{-1} + 1\right)\Psi\left(\Theta_r^{i+l} + 1\right) + \Psi\left(-\Theta_r^l + 1\right)\Psi\left(\Theta_q^i + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right) + \\ &+\Psi\left(-\Theta_r^{-1} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right)\Psi\left(\Theta_q^{i+l} + 1\right)\}, \end{aligned} \qquad (2.78)$$

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

Упростим (2.78) учитывая, что все слагаемые

$$\begin{aligned} &\Psi\left(\Theta_q^l\right), \Psi\left(\Theta_r^l\right)\Psi\left(\Theta_q^{-1}\right), \Psi(d_i), \Psi\left(d_i - \Theta_r^{-1} - 1\right), \ldots, \\ &\Psi\left(-\Theta_r^{-1} + 1\right)\Psi\left(\Theta_q^i + 1\right)\Psi\left(\Theta_q^{i+1} + 1\right) \in \{1; -1\}. \end{aligned} \qquad (2.79)$$

Из (2.79) непосредственно следует, что

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

принимает значение на множестве чисел $Z'=\{-4,-3,-2,-1,0,1,2,3,4\}$. Поэтому, используя (2.79), выражение (2.78) можно представить

$$R_{W^n}(l)=\{\pm\sum_{\substack{x_i,y_i\in GF(P^n)\\ x_i,y_i\neq 0(\mathrm{mod}P)}}\Psi\left(1+q_1x_i\right)\Psi\left(1+q_2y_i\right)\pm[3]\}\pm[4], \tag{2.80}$$

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

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

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

получим $(j=m)$

$$R_{W^n}^B(l)=\sum_{i=0}^{L-1}\Psi\left(\Theta_{r_1}^i+1\right)\Psi\left(\Theta_{r_2}^i+1\right)\Psi\left(\Theta_{r_3}^{i+l}\right)\Psi\left(\Theta_{r_4}^{i+l}+1\right). \tag{2.81}$$

Приведем вывод выражения для оценки выбросов ПФВК

$$R_{W^n}^B(l)=\sum_{i=0}^{L-1}\Psi\left(\Theta_{r_1}^i+1\right)\Psi\left(\Theta_{r_2}^i+1\right)\Psi\left(\Theta_{r_3}^{i+l}+1\right)\Psi\left(\Theta_{r_4}^{i-l}+1\right). \tag{2.82}$$

Далее, аналогично выражению (2.70)

$$R_{W_n}(l)=\sum_{i=0}^{P^n-1}\Psi(\Theta_{r_1}^i+1)\cdot\Psi(\Theta_{r_2}^i+1)\cdot\Psi(\Theta_{r_3}^{i+l}-1)\cdot\Psi\left(\Theta_{r_4}^{i+l}-1\right)\pm Z, \tag{2.83}$$

где Z представляет собой сумму слагаемых, входящих в (2.82), для которых $\Theta_{r_1}^i+1\equiv 0\vee\left(\Theta_{r_2}^i+1\right)\equiv 0\vee\left(\Theta_{r_3}^{i+l}+1\right)\equiv 0\vee\left(\Theta_{r_4}^{i+l}+1\right)\equiv 0$, что эквивалентно:

$$\Theta_{r_1}^i+1\equiv 0\vee\Theta_q^{i+l}+1\neq 0\wedge\Theta_{r_3}^{i+l}+1\neq 0\wedge\Theta_{r_4}^{i+l}+1\neq 0(\mathrm{mod}L);\qquad \text{а)}$$
$$\Theta_{r_1}^i+1\neq 0\vee\Theta_q^{i+l}+1\equiv 0\wedge\Theta_{r_3}^{i+l}+1\neq 0\wedge\Theta_{r_4}^{i+l}+1\neq 0(\mathrm{mod}L);\qquad \text{б)}$$
$$\Theta_{r_1}^i+1\neq 0\vee\Theta_q^{i+l}+1\neq 0\wedge\Theta_{r_3}^{i+l}+1\equiv 0\wedge\Theta_{r_4}^{i+l}+1\neq 0(\mathrm{mod}L);\qquad \text{в)}$$
$$\Theta_{r_1}^i+1\neq 0\vee\Theta_q^{i+l}+1\neq 0\wedge\Theta_{r_3}^{i+l}+1\neq 0\wedge\Theta_{r_4}^{i+l}+1\equiv 0(\mathrm{mod}L);\qquad \text{г)}$$

поэтому:

$$Z=\pm\{\Psi\left(\Theta_{r_2}^{i}+1\right)\Psi\left(\Theta_{r_3}^{i+l}+1\right)\Psi\left(\Theta_{r_4}^{i+l}+1\right)+\Psi\left(\Theta_{r_1}^{i}+1\right)\Psi\left(\Theta_{r_3}^{i+l}+1\right)\Psi\left(\Theta_{r4}^{i+l}+1\right)+$$
$$+\Psi\left(\Theta_{r_1}^{i}+1\right)\Psi\left(\Theta_{r_2}^{i}+1\right)\Psi\left(\Theta_{r_3 i+l}+1\right)+\Psi\left(\Theta_{r_1}^{i}+1\right)\Psi\left(\Theta_{r_2}^{i}+1\right)\Psi\left(\Theta_{r_4}^{i+l}+1\right)\},\qquad(2.84)$$

может принимать значения на множестве $Z'=\{-4,-3,-2,-1,0,1,2,3,4\}$, следовательно (2.83) есть

$$R_{W_n}(l)=\sum_{i=0}^{P^n-1}\Psi(\Theta_{r_1}^{i}+1)\cdot\Psi(\Theta_{r_2}^{i}+1)\cdot\Psi(\Theta_{r_3}^{i+l}+1)\cdot\Psi\left(\Theta_{r_4}^{i+l}+1\right)\pm[4]=x\pm[4].\qquad(2.85)$$

Преобразуем выражение для x следующим образом:

$$x=\Psi\left(\Theta_{r_3}^{l}\right)\Psi\left(\Theta_{r_4}^{l}\right)\sum_{i=0}^{P^n-1}\Psi(\Theta_{r_1}^{i}+1)\Psi(\Theta_{r_2}^{i}+1)\Psi(\Theta_{r_3}^{i}+\Theta_{r_3}^{-l})\Psi(\Theta_{r_4}^{i}+\Theta_{r_4}^{-l})=$$
$$=\Psi(\Theta_{r_3}^{l})\Psi(\Theta_{r_4}^{l})\cdot Q.\qquad(2.86)$$

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

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

С учетом (2.75) – (2.77), а также того, что $\Theta_{r_3}^{-l}$ и $\Theta_{r_4}^{-l}$ могут принимать все значения из $GF(P^n)$, обозначив $c_i=\Theta_{r_s}^{i}+\Theta_{r_s}^{-l}$ и $d_i=\Theta_{r_4}^{4}+\Theta_{r_4}^{-l}$, причем, так как, во-первых, $\Theta_{r_3}^{i}\neq 0(\mathrm{mod}\,P)$ и $\Theta_{r_3}^{-l}\neq 1(\mathrm{mod}\,P), \Theta_{r_3}^{i}+\Theta_{r_3}^{-l}\neq 1(\mathrm{mod}\,P)$, а во-вторых, при $\Theta_{r_4}^{i}\neq 0(\mathrm{mod}\,P)$ и $\Theta_{r_4}^{-l}\neq 1(\mathrm{mod}\,P)$, $\Theta_{r_4}^{i}+\Theta_{r_4}^{-l}\neq 1(\mathrm{mod}\,P)$, (2.86) можно представить в виде:

$$R_{W^n}^{B}(l)=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi\left(a_i\right)\Psi\left(b_i\right)\Psi\left(c_i\right)\Psi\left(d_i\right)=$$
$$=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi\left(a_i\right)\Psi\left(b_i\right)\Psi\left(c_i\right)\Psi\left(d_i\right)\pm[4]\pm[15]=\qquad(2.87)$$
$$=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi\left(a_i\right)\Psi\left(b_i\right)\Psi\left(c_i\right)\Psi\left(d_i\right)\pm[19].$$

Анализ (2.87) показывает, что элементы полей c_i, d_i представляют собой автоморфизмы полей $\Theta_{r_3}^{i}$ и $\Theta_{r_4}^{i}$ при $i=\overline{0,P^{n-2}}$. Сумма в нем берется по всевозможным произведениям характеров над $a_i,b_i,c_i,d_i\in GF(P^n)$ и дает оценку для максимально

достигаемого выброса $R^{B}_{W^n}(l)_{max}$. С учетом того, что элементы a_i, b_i, c_i и d_i строятся по различным первообразным и пары условий

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

не истинны, (2.86) имеет вид

$$R_{W^n}(l)=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[8]\pm[4]= \sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[4]\pm[12]. \tag{2.88}$$

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

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

При $k=2$ аналогично (2.83)

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

где Z представляет собой сумму слагаемых, для которых

$$\Theta_{r_1}^i+1=0\vee\Theta_{r_2}^i+1\equiv 0(\mathrm{mod}\,P), \tag{2.89}$$

то есть

$$Z=\pm\Psi\left(\Theta_{r_1}^i+1\right)+\Psi\left(\Theta_{r_2}^i+1\right)\to\pm 2 \tag{2.90}$$

Далее обозначив $a_i=\Theta_{r_1}^i$ и $b_i=\Theta_{r_2}^i$, а затем $c_i=a_i+1$ и $d_i=b_i+1$ аналогично (2.72) – (2.76) имеем

$$x=\sum_{\substack{a_i,b_i\in GF(P^n)\\ a_i,b_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i+1)\Psi(b_i+1)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 1(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)= \sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)-\Psi(c_i)-\Psi(d_i)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)\pm[2] \tag{2.91}$$

С учетом (2.91)

$$R^{B}_{W^n}(0)=\sum_{\substack{c_i,d_i\in GF(P^n)\\ c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(c_i)\Psi(d_i)\pm[4]. \tag{2.92}$$

Заметим, что для случая $k=4$, $R_{W^n}(0)$ можно оценить, используя соотношения (2.88), то есть

$$R^{B}_{W^n}(0)=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i)\Psi(b_i)\Psi(c_i)\Psi(d_i)\pm[12]. \tag{2.93}$$

Анализ (2.93) показывает, что несбалансированность, а, следовательно, и шумы неортогональности с увеличением k увеличиваются и уже при $k=4$ достигают значительной величины, даже без учета результатов сумм в (2.92) и (2.93).

Особенности вычисления выражений (2.80), (2.88), и оценки их значений рассмотрим с использованием выражения (2.93). Воспользовавшись свойством функции характеров, имеем

$$R^{B}_{W^n}(0)=\sum_{\substack{a_i,b_i,c_i,d_i\in GF(P^n)\\ a_i,b_i,c_i,d_i\neq 0(\mathrm{mod}\,P)}}\Psi(a_i,b_i,c_i,d_i)\pm 12. \tag{2.94}$$

Для случая двухзначного характера, используя (2.66) имеем

$$R^{B}_{W^n}(0)=\sum_{u_i^*\in GF(P^n)}\exp\left(-j\pi u_i^*\right)\pm 12. \tag{2.95}$$

Непосредственный анализ (2.95) показывает, что оценка максимальных боковых лепестков ПФАК, ПФВК и несбалансированности в числе символов (1) и (–1) может быть сведена к изучению несбалансированности по четности и нечетности индексов производного поля, элементами которого являются числа (полиномы) вида: $x_i=a_i\cdot b_i\cdot c_i\cdot d_i\left[\mathrm{mod}\,f(x),P\right]$. Анализ выражения (2.94) показывает, что для анализа нелинейных сигналов (ПНС) по критерию минимума максимальных выбросов $R^{B}_{W}(l)\left(R^{B}_{W^n}(l)\right)$ с точки зрения вычислительной сложности, предпочтительнее использовать алгоритм (2.94), а при вычислении основных статистических характеристик алгоритм (2.95).

Выводы к разделу 2

Во втором разделе диссертации решена **вторая** задача исследования.

1. Применяемые в различных приложениях защищенных ТКС сложные сигналы, как правило, формируются с использованием линейных правил (законов),

что позволяет нарушителю определять последующие символы таких сигналов на основе небольшого числа предшествующих символов. В целом, структурная скрытность, ансамблевые, а в ряде случаев и корреляционные свойства таких сигналов, с точки зрения возможностей обеспечения требуемых значений помехоустойчивости, структурной и информационной скрытности, имитостойкости и некоторых других показателей функционирования телекоммуникационной системы, оказываются неудовлетворительными.

Указанные недостатки линейных сигналов либо ограничивают возможность их применения, либо приводят к необходимости применения на уровне источника сообщений систем и средств криптографической защиты и имитозащиты. Одним из путей решения данной проблемы является применение радиоканалов с частотной избыточностью (широкополосных каналов), в которых модуляция параметров сигнала осуществляется с использованием сигналов, использующих нелинейные правила построения.

2. Проведенные исследования показали, что разрешение указанных противоречий в значительной мере может быть разрешено на основе разработки и применения методов анализа и синтеза нелинейных дискретных сигналов с необходимыми, но потенциально возможными, корреляционными, ансамблевыми и структурными свойствами. Основным преимуществами применения таких нелинейных дискретных сигналов является сложность постановки в реальном времени станцией противодействия (нарушителем) «оптимальных» помех».

3. В процессе исследований было установлено, что одним из возможных классов нелинейных сигналов, который может быть альтернативой сигналов с линейными правилами построения, является нелинейные характеристические сигналы. Так показано, что указанная система сигналов обладает потенциально возможными, с точки зрения «плотной упаковки», автокорреляционными и ансамблевыми свойствами. Однако такие сигналы к настоящему времени не были в достаточной мере исследованы с точки зрения их взаимно-корреляционных, структурных и технологических свойств. В частности, проблемными оставались правила построения (технологические свойства) ансамблей таких сигналов. Разрабо-

танные методы синтеза нелинейных характеристических сигналов позволили разрешить это противоречие и позволяют реализовать построение всего ансамбля характеристических сигналов с линейной сложностью. Созданные программные модели позволили подтвердить теоретические результаты относительно корреляционных, структурных и ансамблевых свойств ансамблей характеристических и производных характеристических сигналов. Разработанные теоретические основы синтеза систем нелинейных дискретных сигналов базируются на использовании свойств характеров простых и расширенных конечных полей. Так с использованием этих свойств разработаны методы синтеза отдельных изоморфизмов нелинейных сигналов, которые основываются на установленных зависимостях между элементами и индексами элементов конечного поля. Такие зависимости позволили существенно уменьшить сложность и, следовательно, повысить быстродействие синтеза отдельных изоморфизмов сигналов. Например, выигрыш во времени синтеза сигнала, с применением полученного метода, по сравнению с известным методом, для сигнала с периодом 256 элементов составляет - 25,5 раз, а для периода 9972 элементов – 1039,6 раза.

4. Предложен метод синтеза всей системы нелинейных дискретных сигналов характеристического типа, который базируется на применения преобразований децимации. Применение такого метода позволило получить выигрыш при формировании всей системы нелинейных дискретных сигналов характеристического типа (с использованием программной модели), по сравнению с известным, при периоде формируемого сигнала 1020 элементов, - в 16 раз, а при периоде 2380 - 26 раз. В целом при увеличении длины сигнала выигрыш возрастает.

5. Разработанные в ходе исследований методы синтеза нелинейных характеристических дискретных сигналов, и основанные на свойствах характеров конечных полей, теории чисел, комбинаторики и теории множеств, позволяют существенно (по сравнению с известными методами) повысить быстродействие синтеза данного класса сигналов. Полученные методы позволяют формировать и, следовательно, использовать дискретные сигналы характеристического типа в реальном времени во многих приложениях телекоммуникационных систем при реше-

нии целого ряда задач оптимального приема сигналов (оценка параметров, обнаружение и различение сигналов, фильтрация процессов и др.).

6. В разделе 2.5 приведены аналитические соотношения для авто- и взамнокорреляционных функций производных нелинейных сигналов характеристического типа, которые позволяют оценить значения максимальных боковых пиков указанных корреляционных функций. Более глубокие исследования структурных, корреляционных, статистических, ансамблевых характеристик нелинейных сигналов в конечных полях, в т.ч. производных нелинейных сигналов приведены в четвертом разделе данной диссертации.

7. В целом, разработанные методы, математические и программные модели позволяют решать задачи синтеза и анализа ансамблей характеристических и производных характеристических нелинейных сигналов. На основе этих моделей разработано специализированное программное обеспечение, которое позволяет решать практические задачи синтеза и анализа. На основе разработанных и усовершенствованных в диссертации методов синтеза систем нелинейных сигналов в работе представлены алгоритмы для их реализации, в соответствии с которыми синтезирован класс аппаратных средств формирования и обработки отдельных изоморфизмов и всей системы нелинейных сигналов в простых и расширенных полях Галуа, на которые получено 5 авторских свидетельств на изобретения, что подтверждает практическую значимость полученных в диссертации научных результатов работы.

РАЗДЕЛ 3
МЕТОДЫ СИНТЕЗА СЛОЖНЫХ НЕЛИНЕЙНЫХ ДИСКРЕТНЫХ КРИПТОГРАФИЧЕСКИХ СИГНАЛОВ С НЕОБХОДИМЫМИ АНСАМБЛЕВЫМИ, СТРУКТУРНЫМИ И КОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ

Поскольку кодовое разделение основано на различии сигналов, то построение многопользовательских систем и их характеристики определяются выбором сигналов и их свойствами. Обычно число абонентов достаточно велико, поэтому выбор сигналов для приложений телекоммуникационных систем (системы мобильной связи, космические системы связи и др.) сводится к синтезу систем сигналов с заданными ансамблевыми, корреляционными и другими свойствами. Развитие многопользовательских ТКС, основанных на кодовом разделении сигналов и привело к исследованиям в области теории систем сигналов.

Появление в последние годы новых областей использования псевдослучайных последовательностей потребовало дополнительного и более тщательного изучения их ансамблевых, корреляционных, структурных и других свойств. Например, возросший интерес к широкополосной связи стимулировал исследование апериодических корреляционных функций, а не только периодических. Применение методов кодового уплотнения каналов в системах с многостанционным доступом потребовало более глубокого анализа взаимно-корреляционных свойств. Необходимость противодействовать мешающему влиянию злоумышленников на функционирование ТКС привело к поиску (синтезу) сигналов с заданными корреляционными, структурными, ансамблевыми, технологическими и другими свойствами.

Для большинства приложений, в частности, для широкополосных систем с многостанционным доступом, интерес представляют не пары, а большие множества последовательностей с хорошими взаимно-корреляционными свойствами, улучшенными ансамблевыми и структурными свойствами. В некоторых системах число одновременно используемых последовательностей может превышать не-

сколько сотен. Известны большие множества периодических последовательностей (множества Касами, Голда), обладающие сравнительно небольшими значениями боковых лепестков взаимно-корреляционных функций. Для генерации таких последовательностей применяются сдвиговые регистры с линейной обратной связью. Правила построения указанных классов последовательностей указывают на низкую структурную скрытность формируемых последовательностей, и, следовательно, сигналов, обеспечивающих передачу информации в ТКС.

В разделе 1 было показано, что показатели помехозащищенности и информационной безопасности ТКС в значительной степени определяются корреляционными, структурными и ансамблевыми свойствами переносчиков данных пользователей. В разделе 3.3 представлен впервые полученный метод синтеза нелинейных криптографических дискретных сигналов, который использует случайные или псевдослучайные процессы, и создает последовательности символов (сигналов) определенного алфавита, которые удовлетворяют требованиям необратимости, неразличимости, непредсказуемости, и обладают необходимыми структурными, ансамблевыми и корреляционными свойствами, что позволяет улучшить показатели помехозащищенности, имитостойкости, структурной скрытности ТКС, а так же помехоустойчивости приема сигналов в условиях воздействия структурных, заградительных, ретранслированных и других видов помех.

В разделе 3.4 представлен разработанный усовершенствованный метод синтеза нелинейных дискретных сигналов с заданными ансамблевыми, корреляционными и структурными свойствами, отличающийся от известного метода тем, что использует механизм направленного (ограниченного) перебора, для отбора сигналов с заданными свойствами, что позволяет повысить производительность синтеза системы сигналов.

В разделе 3.1 - 3.2 приведено описание функций криптографических систем, общие требования к проектированию и применению таких систем, представлены принципы синтеза современных криптографических систем.

3.1 Функции криптографической системы. Общие требования к проектированию и применению криптографических систем

Широкое применение облачных вычислений, средств удаленного подключения с мобильных и удаленных стационарных устройств через сети общего назначения приводят к «исчезновению периметра» критических систем и значительному усложнению обеспечения их безопасного функционирования. Поэтому обеспечение безопасности телекоммуникационных систем стало одной из приоритетных задач в современном мире. В условиях внутренних и внешних несанкционированных действий нарушителей на ТКС фактически, для любого сообщения, блока данных или программного кода необходимо реализовать ряд услуг (функций) безопасности.

К основным функциям (услугам) информационной безопасности следует отнести следующие [54,56,66].

Конфиденциальность информации - свойство защищенности информации (с заранее заданным качеством (вероятностью)) от несанкционированного доступа к ней и попыток раскрытия (получение содержания) неавторизованными пользователями и (или) процессами.

Целостность информации - свойство защищенности информации, которое заключается в том, что информация практически не может быть изменена случайно или намеренно неавторизованными субъектами (нарушителями) или объектами (процессами), причем факт возможности нарушения целостности может быть определен с заранее заданной вероятностью.

Подлинность (аутентичность) - свойство объектов/субъектов (в том числе информации, ресурсов, сообщений, данных, пользователей и т.д.) обеспечить установление достоверности утверждения о том, что субъект или объект имеет заявленные (ожидаемые) свойства.

Доступность - свойство ресурса системы (информации, услуги, объекта информационной и (или) телекоммуникационной системы), которое заключается в том, что авторизованный пользователь и (или) процесс, наделен соответствую-

щими полномочиями, может использовать ресурс в соответствии с правилам и с определенным качеством.

Неотказуемость – свойство, связанное с предотвращением возможности возражения реальными субъектами (пользователями) и объектами (процессами) фактов полного или частичного принятия участия в информационном обмене или информационном взаимодействии. Как правило, включает формирование, предоставление и передачу доказательств реального принятия участия в информационном обмене или информационном взаимодействии.

Наблюдаемость - свойство ресурса системы (компьютерной системы, объекта компьютерной системы и т.д.), которое позволяет регистрировать (фиксировать) действия пользователей и процессов, использование ресурса системы, однозначно устанавливать идентификаторы (имена) причастных к определенным событиям пользователей и процессов, а также реагировать на эти события с целью минимизации возможных потерь в системе, осуществляется, в том числе, за счет использования криптографических преобразований.

Указанные услуги в полной мере могут быть предоставлены посредством использования симметричных и асимметричных криптографических преобразований и протоколов.

Существенной проблемой в предоставлении указанных услуг с соответствующей гарантией является обеспечение криптографической живучести ключевых данных и ключевой информации. В дальнейшем под криптографической живучестью будем понимать свойство криптографической системы обеспечивать необходимый уровень криптографической стойкости криптографических преобразований в условиях компрометации заархивированных, очередных, а также частей действующих ключевых данных и ключевой информации [56].

Блочные симметричные шифры (БСШ) являются одним из наиболее распространенных криптографических примитивов. Кроме обеспечения конфиденциальности (шифрования) основных объемов информации, передаваемых по сети или хранимых локально, они применяются как конструктивный элемент других примитивов (функций хеширования, кодов аутентификации сообщений, генера-

торов псевдослучайных последовательностей и пр.). Значение этого криптографического преобразования подчеркивает и ряд международных конкурсов, таких как AES, NESSIE, CRYPTREC [1], которые были ориентированы на разработку блочного шифра (как основной цели или в составе набора перспективных решений).

Симметричные криптографические системы должны удовлетворять ряду требований [16-17, 37].

1. Обеспечение криптографической стойкости алгоритма. При этом должны выполняться следующие требования:

- множество шифрованных / открытых текстов, необходимых для выполнения криптоаналитической атаки, должно превышать множество допустимых шифрованных / открытых текстов;

- сложность любой аналитической атаки должна быть больше или равна сложности силовой атаки;

- объем памяти, необходимый для хранения промежуточных результатов при осуществлении аналитической атаки должен быть не меньше, чем при реализации атаки по словарю на полный шифр.

2. Защищенность алгоритмов от криптоаналитических атак (криптоанализа). При этом основными методами криптоанализа являются: дифференциальный криптоанализ; расширение для дифференциального криптоанализа; поиск лучшей дифференциальной характеристики; линейный криптоанализ; интерполяционное вторжение; вторжение с частичным угадыванием ключа; вторжение с использованием связанного ключа; вторжение на основе обработки сбоев; поиск лазеек и потенциальных атак и др.

3. Статистическая безопасность криптографических алгоритмов. Предусматривается обеспечение «хороших» статистических свойств исходной последовательности шифра (криптограммы или гаммы), при которых криптограммы и гаммы шифрования практически не отличаются от свойств случайной последовательности.

4. Устойчивость при модификации, когда «кандидаты» в криптоалгоритмы проверяются на устойчивость к разного рода модификациям: устойчивость к криптоаналитическим атакам при уменьшении числа циклов шифрования и др.

5. Особенности конструкции и открытость структуры. Криптоалгоритм должен обладать понятной, легко анализируемой структурой и основываться на надежном математическом аппарате.

6. Вычислительная сложность (скорость) зашифрования / расшифрования.

Сложность программной, аппаратной и программно-аппаратной реализации должна оцениваться объемом памяти, как для программной, так и аппаратной реализации. В том числе, при программной реализации - количеством необходимой оперативной памяти, размером исходного кода, скоростью работы программы на разных платформах при реализации на известных языках программирования. При аппаратной реализации криптографического алгоритма вычислительная сложность оценивается количеством вентилей и скоростью в соответствующих единицах (например, Мб/с).

7. Универсальность криптографического алгоритма, которая предусматривает:

• возможность работы с различными длинами начальных ключей и информационных блоков;

• безопасность реализации на различных платформах и приложениях;

• возможность использования криптографического алгоритма в необходимых обоснованных режимах работы БСШ.

8. Обеспечение требуемого класса криптографической стойкости в виде следующих необходимых условий:

• сверхвысокая устойчивость, когда длина блока информации и длина выходного ключа равняются не менее 512 бит;

• высокая устойчивость, когда длина блока информации и длина ключа составляют не менее 256 бит;

• нормальный уровень устойчивости, когда длина блока информации и длина ключа составляют не менее 128 бит;

• удовлетворительный уровень устойчивости, когда длина блока информации составляют не менее 64 бит, а длина ключа - не менее 128 бит.

БСШ отвечать ряду требований с точки зрения конкретных параметров криптоалгоритма, принципов построения и др. [16,56,66].

1. Параметры криптоалгоритма:

• криптоалгоритм должен быть блочным симметричным шифром;

• размер блока данных - 128, 256 и 512 бит;

• размер разового (сеанса) ключа - 128, 256, 512 бит.

2. Принципы построения:

• способность противостоять известным методам криптографической анализа и иметь запас устойчивости с учетом тенденций развития средств электронной вычислительной техники и криптографической науки;

• используемые криптографические преобразования должны базироваться на надежной и прозрачной математической базе и не иметь встроенных лазеек;

• быстродействие криптоалгоритма должна быть не меньше, чем быстродействие существующего государственного стандарта шифрования.

3. Реализация криптоалгоритма:

• криптоалгоритм должен быть ориентированным на возможность реализации на 32-х или 64-х разрядных процессорах;

• указанные в криптоалгоритме операции должны иметь эффективную программную и аппаратную реализацию;

• необходимый для работы объем памяти должен учитывать возможность реализации криптоалгоритма в микроустройствах;

• должна быть предусмотрена возможность параллельного выполнения нескольких операций.

4. Ключевая система:

• криптоалгоритм должен предусматривать наличие долговременного ключа;

• длина синхронизирующей посылки должна быть не менее 64 битов.

Эффективность криптографической защиты напрямую зависит от режимов применения БСШ. В перспективных криптоалгоритмах должны быть предусмотрены следующие режимы шифрования [56]:

- режим простой замены, который является обязательной составляющей для всех других режимов. Заключается в обеспечении конфиденциальности отдельных блоков открытого текста путем их шифрования на основе введенного секретного ключа;

- режим гаммирования, который предназначен для обеспечения конфиденциальности путем быстрого шифрования блоков открытого текста с возможностью применения параллельных вычислений. Заключается в шифровании набора входных блоков, которые являются выходом счетчика и в сложении результирующих блоков (блоков гаммы) с блоками открытого текста;

- режим гаммирования с обратной связью, предназначенный для обеспечения конфиденциальности путем шифрования потока данных с «размножением» ошибок и обеспечения невозможности манипуляций с отдельными блоками открытого текста;

- режим сцепления шифр блоков, предназначенный для обеспечения конфиденциальности, когда процесс шифрования реализуют путем объединения блоков открытого текста с блоками зашифрованного текста, полученными на предыдущих шагах шифрования;

- режим выработки имитовставки, который основан на использовании режима сцепления шифр блоков с дополнительным прибавлением ключа к последнему шифрблоку. Полученная таким образом имитовставка предназначена для обеспечения подлинности и целостности информации;

- режим гаммирования с обратной связью по шифр гамме, предназначенный для обеспечения конфиденциальности. Заключается в шифровании вектора инициализации (синхропосылки) для генерации блоков шифргаммы;

- режим имитовставки с выборочным гаммированием, который предназначен для обеспечения конфиденциальности и целостности информации;

- режим индексированной замены, который предназначен для обеспечения конфиденциальности данных при их хранении на определенных физических носителях (винчестерах, оптических дисках и т.д.).

3.2 Принципы синтеза и особенности построения современных криптографических систем

При построении перспективных БСШ в настоящее время используют три методологических подхода.

В основу реализации первого методологического подхода положена хорошо испытанная Фейстеля-подобная схема. Она реализована в стандартах БСШ DES, DEA, TDEA, ГОСТ 28147 - 89, а также в MISTY1, Camellia. На настоящее время стандарты БСШ, имеющие Фейстель подобную структуру, по-прежнему относятся к перспективным криптографическим структурам.

Второй методологический подход использует расширенную схему Лея-Массея, известную своей устойчивостью к криптографическому анализу. Схема Лея-Массея является собственностью швейцарской компании MediaCrypt, которой принадлежат права на распространение IDEA и, которая, является владельцем патентов на IDEA NXT.

Третий подход связан с использованием SPN структур. Общая структура - SPN, square-type, байт - байт ориентированный шифр. На основе таких структур были разработаны и нашли признание БСШ Rijndael и его версия - AES (FIPS - 197).

Для обоснования устойчивости БСШ по SPN схеме применяется принцип широкого следа (Рис. 3.1), согласно которому шифр проектируется так, чтобы распространить диффузию в соответствии с определенными математическими принципами.

Каждый слой преобразования имеет свою собственную функцию:

• линейный слой (миксирование): гарантирует высокое рассеивание над многочисленными раундами;

• нелинейный слой: параллельное применение S-блоков, которые обеспечивают нелинейную замену байт промежуточного состояния;

• слой добавления ключа: сложение по модулю 2 промежуточного состояния с раундовым ключом.

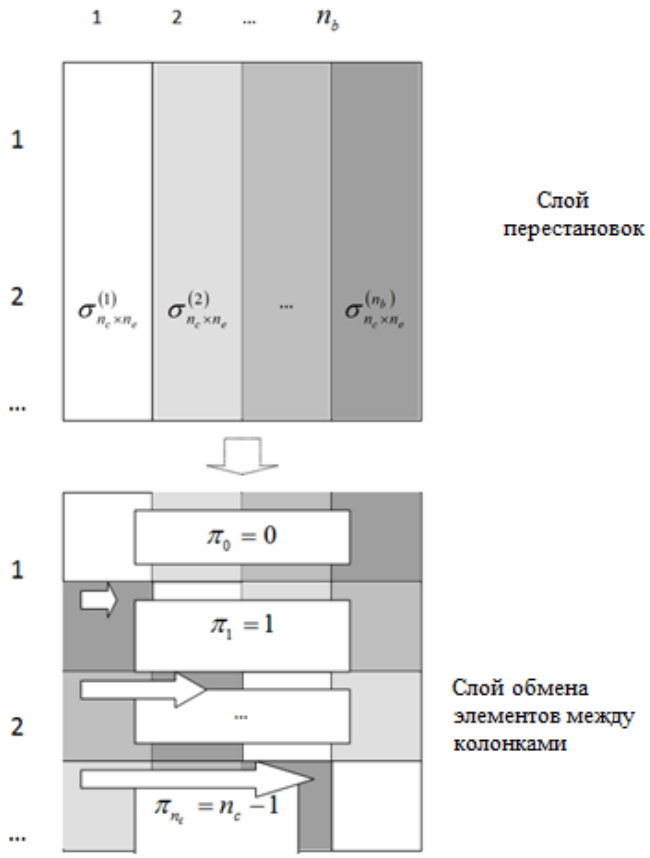


Рис. 3.1 Раунд SPN схемы шифра

Принцип широкого следа заключается в том, что:

- выбирают S-блоки, для которых максимальная вероятность дифференциального следа и максимальная корреляция входных и выходных битов имеют как можно меньшие значения;

- выбирают линейные преобразования таким образом, чтобы не имелось «следов» с несколькими активными S-блоками.

В значительной степени указанным выше требованиям к современным БСШ удовлетворяет Национальный криптографический стандарт блочного симметричного преобразования ДСТУ 7624:2014, определяющий шифр „Калина” и режимы его работы для обеспечения конфиденциальности и целостности информации [68]. Национальный стандарт поддерживает размер блока и длину ключа шифро-

вания 128, 256 и 512 бит (длина ключа равна размеру блока или в два раза превышает его), обеспечивая нормальный, высокий и сверхвысокий уровень стойкости (сейчас это единственный в мире стандарт блочного шифрования, поддерживающий 512-битовые симметричные ключи). Разные варианты стандарта обеспечивают гибкость выбора параметров для разработчиков систем криптографической защиты, что позволяет получить как наивысший уровень быстродействия, так и наибольший запас стойкости преобразования.

Высокоуровневая конструкция использует хорошо исследованную Square-подобную SPN-структуру, применяемую в алгоритмах AES/Rijndael, Whirlpool, «Стрибог», «Кузнечик» и многих других. Цикловое преобразование построено на базе таблиц подстановки (S-блоков) и умножения на МДР-матрицу над конечным полем, обеспечивая необходимые криптографические свойства. Применение именно такой конструкции позволяет обеспечить доказуемую стойкость к дифференциальному, линейному и другим видам криптоанализа, одновременно обеспечивая эффективную реализацию для широкого спектра программных и программно-аппаратных платформ. При выборе размера МДР-матрицы был принят во внимание размер кэша L1 современных и перспективных процессоров, что позволило оптимизировать быстродействие программной реализации шифра.

Стандарт Украины обеспечивает наибольшую нелинейность булевых функций, что дает дополнительный запас стойкости по отношению к линейному криптоанализу. Еще большее значение нелинейности для взаимо-однозначной подстановки можно обеспечить, применяя, например, аффинно-эквивалентные степенные функции в конечном поле, но такие преобразования, использованные в AES, Camellia и др. алгоритмах, ставят шифр под угрозу реализации алгебраической атаки (этот метод криптоанализа был успешно применен против шифра Keeloq, используемого в системах автомобильной безопасности).

В качестве схемы разворачивания ключей используется конструкция со следующими свойствами:

- обеспечение криптографической стойкости к известным методам анализа, отсутствие «слабых» ключей, которые могут ухудшить свойства преобразования;

- удобство программной и программно-аппаратной реализации (для формирования цикловых ключей применяются только операции, используемые при шифровании);

- высокая вычислительная сложность восстановления ключа шифрования по одному или нескольким цикловым ключам.

Последнее свойство обеспечивает дополнительную защиту к атакам на реализацию, когда злоумышленник пытается атаковать инженерные решения (измеряя потребляемый устройством ток, умышленно вызывая сбои в работе через намеренный перегрев шифратора и пр.). Эта особенность является существенным преимуществом для ряда приложений, в частности, при реализации шифрования на смарт-картах, USB-токенах и пр., когда ключ записан в устройстве и должен быть защищен от внешнего доступа (например, в модулях доступа к платным цифровым ТВ каналам и др.).

Количество циклов шифрования зависит от длины ключа: 10 циклов для 128-битового, 14 циклов для 256-битового и 18 циклов для 512-битового ключа шифрования.

По сравнению с другими алгоритмами на основе Square-подобной SPN-структуры, блочный шифр «Калина» имеет следующие существенные конструктивные отличия:

- начальное и конечное «забеливание» с использованием модульного сложения (264) для повышения сложности криптоаналитических атак;

- применение четырех различных S-блоков (вместо одного) со свойствами для защиты от алгебраических атак, и при сравнении характеристик с другими блочными и поточными шифрами обеспечивают наибольшую нелинейность булевых функций, что дает дополнительный запас стойкости преобразования;

- увеличенный размер МДР-преобразования, что улучшает криптографические свойства и позволяет оптимизировать быстродействие на современных 64-битовых платформах.

Оценка криптографической стойкости к дифференциальному, линейному, алгебраическому, интегральному и другим методам анализа (практический крите-

рий) показала, что шифр является стойким при 6 циклах для 128-битового блока, 7 циклах для 256-битового и 9 циклах для 512-битового (каждый дополнительный цикл обеспечивает экспоненциальный рост сложности криптоанализа). Таким образом, шифр, содержащий 10, 14 и 18 циклов для блока 128, 256 и 512 битов соответственно, обеспечивает защиту от рассмотренных видов анализа и имеет существенный запас стойкости.

Национальный стандарт БСШ обладает рядом отличий от известных БСШ, в частности, - криптоалгоритма Rijndael, а именно:

- увеличено количество циклов шифрования, тем самым, обеспечивая некоторый запас устойчивости;

- использование операций сложение по модулю 2^{32} и по модулю 2 для ввода ключевой информации (защита от алгебраических атак, линейного и дифференциального криптоанализа, интерполяционной атаки и т.п.);

- использование 8 блоков нелинейного преобразования (S-блоков) вместо одного (дополнительная защита от алгебраических атак, улучшение свойств рассеяния шифра - улучшенные статистические свойства, соответственно более высокий уровень устойчивости к диференциальному и линейному криптоанализу и т.п.);

- использование случайно формируемых S-блоков, отобранных по критериям устойчивости к диференциальному, линейному криптоанализу и степени нелинейности булевых функций (в отличие от S-блока Rijndael / Camellia и других шифров, используют обращение в поле и, соответственно, квадратичную зависимость между входом и выходом, тем самым обеспечивая защиту от алгебраических атак);

- принципиально новая схема выработки подключей (защита от всех известных атак на схемы выработки подключей; достаточно высокая производительность; достаточно защищенная процедура восстановления мастер-ключа по отдельному подключу, что является дополнительной защитой от атак, которые направлены на востановление подключей).

Указанные выше решения направлены на увеличение устойчивости шифра и перекрытие потенциальных уязвимостей, которые имеют место при применении криптоалгоритма Rijndael.

Таким образом, стандарт «Калина» удовлетворяет требованиям к проектированию современных криптографических систем, реализует высокие показатели криптографической стойкости. Именно поэтому национальный криптографический стандарт блочного симметричного преобразования ДСТУ 7624:2014, определяющий шифр „Калина” и режимы его работы для обеспечения конфиденциальности и целостности, был выбран для решения задач синтеза нелинейных дискретных сигналов.

3.3 Разработка метода синтеза нелинейных криптографических дискретных сигналов на основе использования случайных (псевдослечайных) процессов

Одним из режимов стандарта шифрования „Калина” [68] является режим гаммирования. Зашифрование в режиме гаммирования заключается в суммировании открытого текста с гаммой шифра, которая вырабатывается блоками длины s путем зашифрования последовательности значений счетчика базовым алгоритмом (режим простой замены).

Процедура зашифрования блока открытых данных в указанном режиме может быть представлена в виде:

for j = 1, 2 … n

$O_j = CIPH_K(T_j)$;

for j = 1, 2 … n-1

$C_j = P_j \oplus O_j$;

$C^*_n = P^*_n \oplus MSB_u(O_n)$, (3.1)

где: O_j – j-й выходной блок;

$CIPH_K$ – функция шифрования над j-м блоком счетчика;

C_j – j-й выходной блок криптопреобразования;

P_j – j-й блок исходного (открытого) текста

C^*_n, P^*_n – последующие блоки выходного и исходного текстов;

$MSB_u(O_n)$ – битовая строка, состоящая из наиболее значимых n бит битовой строки O.

Процедура расшифрования блока зашифрованных данных в указанном режиме может быть представлена в виде:

for j = 1, 2 … n;

$O_j = CIPH_K(T_j)$;

for j = 1, 2 … n-1

$P_j = C_j \oplus O_j$;

$P^*_n = C^*_n \oplus MSB_u(O_n)$. (3.2)

Схема зашифрования и расшифрования данных с применением указанного алгоритма представлена на рисунке 3.2.

Метод синтез систем сложных нелинейных криптографических сигналов с заданными свойствами корреляционных функций, ансамблевыми и структурными свойствами включает следующие действия [63].

1. Генерация массива псевдослучайных последовательностей символов заданного периода с использованием криптографического алгоритма (источников случайные или псевдослучайные последовательностей символов) [1-2,16,68].

2. Тестирование полученных последовательностей с применением критериев и показателей качества генераторов, определенных международными и ведомственными стандартами FIPS PUB 140-1 [10], FIPS PUB 140-2 [11], AIS 20 [3] и AIS 31 [4], NIST 800-22 [25], NIST 800-90b [26].

3. Формирование дискретных последовательностей (ДП) символов фиксированного периода (например: 31, 63, 127, 255, 1023, 2047, ...).

4. Отбор ДП, значения боковых лепестков периодической функции автокорреляции (ПФАК) которых, близких к границе «плотной упаковки» [33,145].

5. Получение матрицы состояний взаимно-корреляционных функций всех возможных пар последовательностей, прошедших отбор по результатам предыдущего шага.

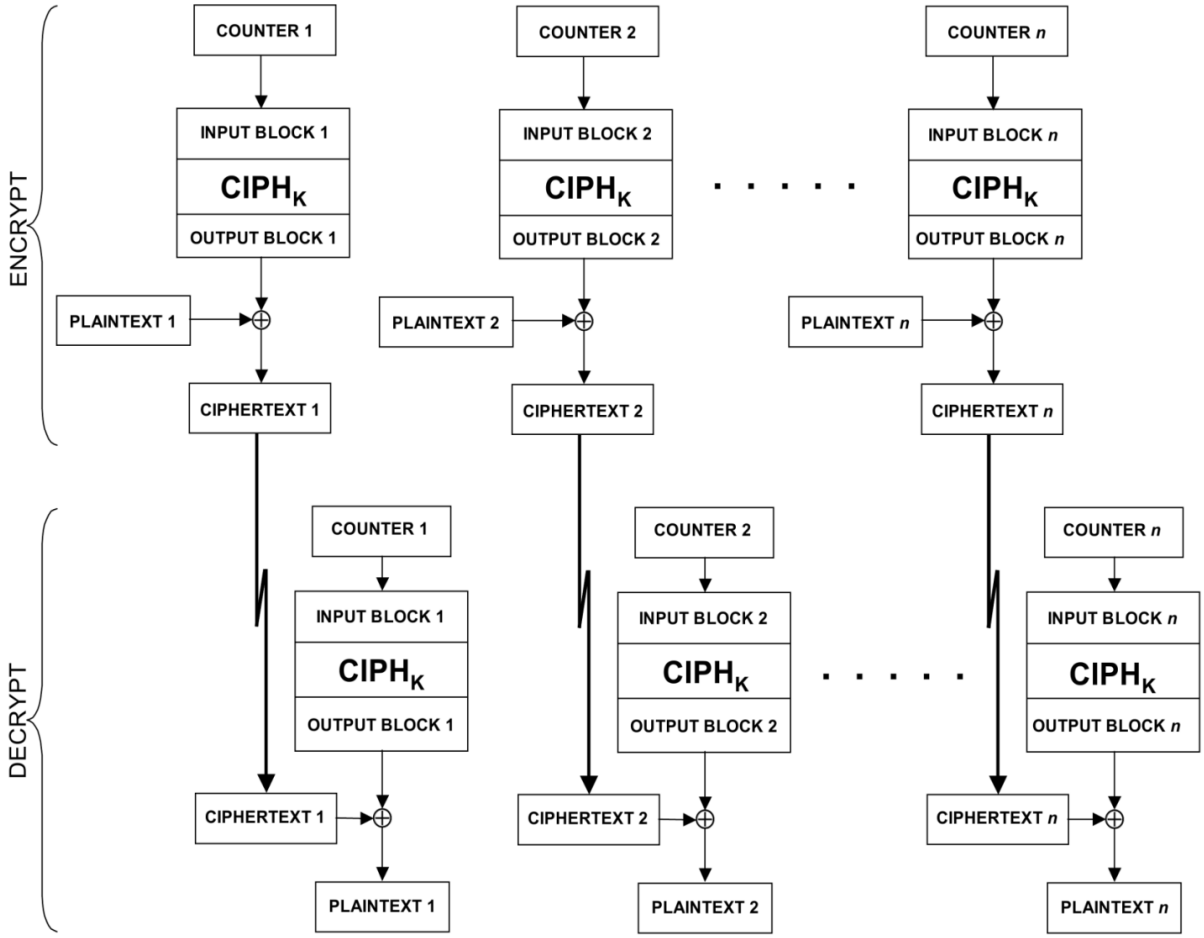


Рис.3.2 Схема зашифрования и расшифрования данных в режиме гаммирования

6. Обработка матрицы, заключающаяся в том, что осуществляется отбор последовательностей, удовлетворяющих границам «плотной упаковки» для соответствующих корреляционных функций.

Обоснуем необходимость шага 4 представленного метода синтеза сигналов. Многочисленные приложения NRC указывают на важность периодических автокорреляционных свойств используемых сигналов: дальномерные системы с непрерывным излучением, пилотный канал и канал синхронизации в цифровых системах передачи данных (пилотные сигналы «вниз» стандартов cdma One и cdma2000, вторичный канал синхронизации стандарта CDMA [15,20,24]), радарные и сонарные системы с непрерывным излучением и др. Кроме того, хорошая

периодическая автокорреляционная функция (АКФ) сигнала указывает на возможность отбора сигналов с хорошими апериодическими АКФ.

Минимизация уровня боковых лепестков АКФ имеет наибольшее значение при конструировании сигнала для таких приложений как измерение времени запаздывания, временное разрешение и др. Следует иметь в виду, что равенство нулю всех боковых лепестков невозможно для финитных или апериодических ФМ сигналов [8,15]. Действительно, если сигнал имеет длину N, то это влечет выполнение равенства $a_o \neq 0$ и $a_{n-1} \neq 0$, поскольку в противном случае длина сигнала была бы меньше N. Тогда крайний правый боковой лепесток нормированной апериодической АКФ сигнала будет:

$$P_a(N-1) = \frac{a_0 a_{N-1}}{\|a\|^2} \neq 0. \qquad (3.3)$$

Последнее соотношение приводит к применению минимаксного критерия при синтезе сигналов, который требует достижения минимально возможной величины максимального бокового лепестка АКФ апериодического кода. Формальная запись данного критерия имеет вид:

$$P_{a,max} = \max_{m \neq 0} \{|P_a(m)|\} = \min. \qquad (3.4)$$

В соответствии с критерием (3.4) предпочтительными являются кодовые последовательности с наименьшим значением максимального бокового лепестка. Таким образом, требования, предъявляемые к наилучшему сигналу, могут быть сформулированы в виде следующей оптимизационной задачи: на множестве всех возможных последовательностей длины N с символами из заранее выбранного алфавита найти последовательность или последовательности с минимальной величиной максимального бокового лепестка апериодической АКФ.

Сформулированная выше оптимизационная задача, как и многие другие задачи дискретной оптимизации, не имеют общего аналитического решения, и типичной процедуры ее выполнения является осуществление исчерпывающего поиска.

Для любого ФМ сигнала $|a_i|=1, i=0,1...N-1$, так что $|a_0 a_{N-1}|=1$, и крайний правый боковой лепесток апериодической АКФ (2) $|p_f(N-1)|=1/N$. Следовательно, максимальный боковой лепесток ФМ сигнала ограничен снизу величиной:

$$p_{a,max} \geq 1/N.$$

Естественно, что ФМ сигналы, удовлетворяющие данной границе, будут оптимальными.

Задача нахождение оптимальных бинарных последовательностей большой длины, может быть сформулирована в виде: найти бинарный код с удовлетворительно малым уровнем периодического бокового лепестка $p_{a,max}$. Общая идея алгоритмов, направленных на решение этой задачи, состоит в предварительном отборе некоторого ограниченного множества последовательностей, которое кажется многообещающим в плане корреляционных свойств, и последующем поиске кода с минимальным значением $p_{a,max}$ только среди последовательностей, вошедших в указанное множество.

Обозначая через $R_{p,max}$, максимальный боковой лепесток периодической АКФ: $R_{p,max} = \max_{m=1,2,...n-1}\{|R_p(m)|\}$, и используя неравенство:

$$\max\{|x+y|\} \leq \max\{|x|+|y|\} \leq \max\{|x|\} + \max\{|y|\},$$

приходим к оценке $R_{p,max} \leq R_{a,max}$ или:

$$R_{a,max} \geq \frac{1}{2} R_{p,max}. \qquad (3.5)$$

Из (3.5) следует, что последовательности с хорошей апериодической АКФ могут быть найдены среди последовательностей с хорошей периодической АКФ.

С учетом указанного вызывает интерес определение потенциала минимизации максимального бокового лепестка ПАКФ бинарных кодов.

В теории сложных сигналов известен ряд интегральных равенств [27]. Пусть C - множество комплексных чисел, а C^N - множество векторов с комплексными компонентами. Элементы множества $w, x, y, z \in C^N$ - произвольные векторы, а

w, x, y, z - соответствующие им дискретные последовательности. Четыре взаимно-корреляционные функции $R_{w,x}$, $R_{y,z}$, $R_{w,y}$, $R_{x,z}$ связаны соотношением

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,z}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_{y,z}(l+n)]^* . \qquad (3.6)$$

Положив в (3.6) $z = y$, получим

$$\sum_{l=0}^{N-1} R_{w,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_{w,x}(l)[R_{y}(l+n)]^* . \qquad (3.7)$$

Положив в (3.7) $w = x$, получим

$$\sum_{l=0}^{N-1} R_{x,y}(l)[R_{x,y}(l+n)]^* = \sum_{l=0}^{N-1} R_{x}(l)[R_{y}(l+n)]^* . \qquad (3.8)$$

Наконец, положив в (3.8) $n = 0$, получим

$$\sum_{l=0}^{N-1} \left|R_{x,y}(l)\right|^2 = \sum_{l=0}^{N-1} R_{x}(l)[R_{y}(l)]^* . \qquad (3.9)$$

С помощью (3.6) - (3.9) получен ряд важных границ оценки корреляционных функций. Кроме того, использование этих соотношений приводит к полезным вычислительным алгоритмам и методам построения последовательностей. Так, тождество (3.6) означает, что взаимно-корреляционная функция последовательностей $R_{w,y}$ и $R_{x,z}$ совпадает с взаимно-корреляционной функцией последовательностей $R_{w,x}$ и $R_{y,z}$. Если предположить, что последовательности w и x не коррелированны, тогда, согласно (3.6), последовательности $R_{w,y}$ и $R_{y,z}$ также не коррелированны. Причем отсутствие корреляции имеет место при произвольном выборе y и z. В частности, как видно из (3.7) последовательности y и z могут совпадать. Таким образом, имея две некоррелированные последовательности, могут быть построены две новые последовательности с такими же свойствами. Равенство (3.8) означает, что автокорреляционная функция последовательности $R_{x,y}$ совпадает взаимно-корреляционной функцией последовательностей R_{x} и R_{y}. Пусть последовательности x и y - последовательности периода L с двухуровневой автокорреляцией. Тогда последовательности $R_{x,y}$ и $R_{y,x}$ также имеют период L и об-

ладают двухуровневыми автокорреляционными функциями. Кроме того, из (3.9) следует, что среднее значение квадрата модуля функции взаимной корреляции сигналов x и y равно среднему значению произведения их автокорреляционных функций. Фактически это означает, что сигналы, обладающие хорошими автокорреляционными свойствами, будут обладать и хорошими свойствами взаимно-корреляционных функций.

В [27] приведены неравенства, устанавливающие границы для среднеквадратичных значений корреляционных функций. Границы для максимальных значений можно определить следующим образом. Множество периодических последовательностей M охарактеризуем параметром R_c - максимальным значением взаимно-корреляционной функции:

$$R_c = \max\{|R_{k,l}(m)|: 0 < m < N-1, k \in M, \\ l \in M, k = 1\} \tag{3.10}$$

и параметром R_a - максимальным значением бокового лепестка автокорреляционной функции:

$$R_a = \max\{|R_k(m)|: 0 < m < N-1, k \in M\}, \tag{3.11}$$

где: N – период дискретной последовательности.

Если M содержит K последовательностей, то

$$(R_c^2 / N) + N - 1 / N(K-1) \cdot (R_a^2 / N) > 1 \tag{3.12}$$

Из (3.12) следует

$$R_{max} = \max\{R_a, R_c\} \geq N\left[\frac{K-1}{KN-1}\right]^{1/2}, \tag{3.13}$$

что совпадает с известными границами Сидельникова [145] и Уэлча [33].

Таким образом, в соответствие с (3.10) - (3.13) для соответствующих значений периода сигналов могут быть установлены границы значений функций корреляции и осуществлен отбор сигналов, значения боковых лепестков функции корреляции которых, не превышает данные границы.

В качестве иллюстрации метода в таблице 3.1 представлены (в соответствии с этапом 1 метода синтеза) отдельные псевдослучайные последовательности с пе-

риодом N=32, полученные на выходе криптографического алгоритма «Калина», прошедших процедуру тестирования на соответствие требованиям стандарта NIST 800-22 [25] (в соответствии с шагом 2 метода). В таблице 3.1 указано также число символов {1,0} в последовательности.

В таблицах 3.2 - 3.3 приведены матрицы состояний взаимно-корреляционных функций (ПФВК) (значения максимальных и минимальных выбросов взаимно-корреляционных функций) некоторых пар псевдослучайных последовательностей и периодических функций автокорреляции последовательностей (ПФАК), полученных при реализации шага 1 предлагаемого метода.

В таблице 3.4 представлены (в соответствии с шагом 5 метода), результаты отбора пар последовательностей. Другими словами, в таблице 3.4 приведены номера пар и собственно пары последовательностей, боковые пики взаимно-корреляционные функции (значения боковых пиков приведены в таблице) которых, удовлетворяют границе «плотной упаковки».

Таблица 3.1

Массив псевдослучайных последовательностей символов

№	Последовательность	1	0
1	01111011000011010001110001111010	17	15
2	00110000000100010111101000010111	13	19
3	00000001010101100100111100100101	13	19
4	00101001000000010010011100100000	9	23
5	00111001010010110010110001110010	15	17
6	00010100010001100011100000011001	11	21
7	00000100011110100011100100111111	16	16
8	01001001001010000010111100001010	12	20
9	01011101001001010001001100110111	16	16
10	00110000000111100011001101010111	15	17
11	00011100000001110010011000110010	12	20
12	00100010000010100101010100011001	11	21
13	00111110001101100011110000101101	17	15
14	01011011010111000011101110010110	18	14
15	00011101010101110011101100100000	15	17
16	01111101001001000111010100000100	14	18

Таблица 3.2

Значения максимальных боковых выбросов ПФВК пар последовательностей

№	Значения максимальных боковых выбросов пар
1	32 -8 -12 -8 16 -12 18 10 -14 12 -18 12 -16 -10 -12 -10 8 -14 -14 12 -14 20 8 14 16 -22 8 10 -10 -14 20 16
2	8 32 -12 16 -12 12 -14 14 10 16 -10 12 -12 -14 -12 -14 16 14 14 16 14 -12 20 14 12 10 12 14 -14 14 12 16
3	12 12 32 12 -12 12 -14 14 18 12 14 12 -12 -10 12 14 8 18 14 -12 10 16 12 10 12 -10 16 14 10 10 -12 16
4	-8 16 12 32 12 12 14 14 -10 12 14 12 -12 -10 12 14 16 10 18 16 -14 12 16 14 16 -14 12 14 14 6 -8 16
5	16 -12 12 12 32 12 18 14 14 12 14 12 12 14 12 10 12 -18 18 -12 -14 12 8 14 8 14 16 14 14 14 12 12
6	-12 12 12 12 12 32 14 10 -14 12 14 16 12 -14 12 -10 12 -14 14 12 -10 16 -12 14 12 -14 12 14 -14 14 12 16
7	18 -14 -14 14 18 14 32 -12 -12 -14 -12 -14 14 -12 14 12 14 -12 -12 -14 8 14 14 16 14 -12 10 -12 16 -12 -14 14
8	-10 14 14 14 -14 10 12 32 12 10 12 14 -14 -16 -10 -12 10 16 16 14 -16 14 -14 12 14 -12 10 16 -12 -12 14 14
9	-14 -10 18 10 14 -14 -12 -12 32 14 12 -14 14 -20 10 12 10 16 12 10 -16 -10 14 16 10 -12 18 -16 12 -12 -14 -10

Таблица 3.3

Значения боковых пиков ПФАК последовательностей из таблицы 1

№	Значения ПФАК сигналов
1	32 4 -4 -8 -12 0 8 0 8 4 -8 -4 -4 4 4 0 -12 0 4 4 -4 -4 -8 4 8 0 8 0 -12 -8 -4 4
2	32 4 4 0 4 0 -12 0 0 0 -8 -4 8 0 0 0 12 0 0 0 8 -4 -8 0 0 0 -12 0 4 0 4 4
3	32 -4 4 4 0 -4 4 -4 4 4 4 -8 4 -4 0 0 -4 0 0 -4 4 -8 4 4 4 -4 4 -4 0 4 4 -4
4	32 4 4 12 4 8 0 0 12 -4 0 12 0 12 8 4 12 4 8 12 0 12 0 -4 12 0 0 8 4 12 4 4
5	32 -4 -8 -4 -8 8 4 -4 -4 8 -4 4 0 -4 4 -4 4 -4 4 -4 0 4 -4 8 -4 -4 4 8 -8 -4 -8 -4
6	32 4 -4 -8 8 0 4 0 4 8 8 0 -8 4 8 8 -4 8 8 4 -8 0 8 8 4 0 4 0 8 -8 -4 4
7	32 8 0 -4 -4 -8 -8 -4 0 4 -4 0 -4 0 4 4 0 4 4 0 -4 0 -4 4 0 -4 -8 -8 -4 -4 0 8
8	32 -4 4 8 -12 0 4 -8 8 0 4 8 0 0 4 -4 8 -4 4 0 0 8 4 0 8 -8 4 0 -12 8 4 -4
9	32 -8 -4 4 8 -8 4 0 4 0 0 -8 4 -8 0 -8 8 -8 0 -8 4 -8 0 0 4 0 4 -8 8 4 -4 -8

Таблица 3.4

Результаты отбора пар последовательностей по ПФВК

№	Значение ПФВК / Сигналы
1	0 0 0 -4 0 0 -8 0 0 0 0 -8 -8 -4 4 8 8 0 -4 -4 -8 -4 4 4 8 -4 0 0 8 0 -4 4 Сигналы (1, 2): 01111011000011010001110001111010 01100000001000101111010000010111
2	4 4 0 4 -8 -8 4 -8 0 4 -8 4 -8 -4 4 0 -4 0 -8 8 8 0 0 -4 0 -4 -4 4 4 -4 0 -8 Сигналы (1, 4): 01111011000011010001110001111010 01010010000000100100111100100000
3	4 0 -4 -4 -4 0 4 0 4 4 0 0 -4 0 0 4 0 -4 0 -4 -4 -4 0 0 8 0 4 0 -8 -4 -4 4 Сигналы (1, 17): 01111011000011010001110001111010 00100001010111100010000001011110
4	4 8 -8 -4 -4 -8 8 4 4 4 -4 0 4 -4 4 4 4 0 -8 -4 0 -4 0 4 4 0 -4 -4 -4 -8 4 4 Сигналы (1, 23): 01111011000011010001110001111010 00111001001101110011000000110101
5	-4 4 0 4 0 -4 0 -4 -4 8 4 4 0 -4 -4 0 0 0 8 4 0 -8 0 -8 4 -4 4 8 4 -8 -4 -4 Сигналы (1, 27): 01111011000011010001110001111010 00100101010101110010011001000111
6	4 0 0 0 4 8 -4 4 4 -8 -4 -4 0 0 4 0 4 4 4 4 4 8 0 4 0 -4 -4 -4 4 -4 8 0 Сигналы (3, 17): 00000001010101100100111100100101 00100001010111100010000001011110
7	4 4 0 0 4 -4 4 0 4 4 0 -4 4 -4 -8 -4 8 4 0 0 -8 0 -4 4 4 0 0 4 0 -4 -4 8 Сигналы (24, 30): 00110101001100110011101000001001 00001110010101110001110000110001

В таблицах 3.5 – 3.6 приведены результаты исследований, позволяющие проиллюстрировать возможности практического использования представленного выше метода синтеза сигналов. Так в таблице 3.5, в соответствии с описанным выше методом, представлены результаты синтеза дискретных последовательностей для некоторых значений периода последовательности, в частности, приведе-

ны: граничные значения для максимальных выбросов корреляционных функций, удовлетворяющие границам (3.14); количество пар последовательностей, составляющих полный ансамбль сигналов (для оценки взаимно-корреляционных свойств сигналов); количество сигналов, удовлетворяющих граничным значениям для различных корреляционных функций.

В таблице 3.6 приведены оценки числа пар последовательностей различного класса (М-последовательности, последовательности с трехуровневой функцией взаимной корреляции - ПФВКТ, криптографические последовательности (КП)), удовлетворяющих границе «плотной упаковки» для соответствующего периода.

Синтез криптографических дискретных последовательностей различного периода осуществлялся посредством использования выходной последовательности криптографического алгоритма размерностью 20000 двоичных символов.

Таблица 3.5

Корреляционные свойства криптографических дискретных последовательностей

№ п/п	Размерность сегмента КП	Граничные значения функции неопределенности	ПФАК			АФАК	ПФВК			АФВК
			Число КП удовлетво--ряющих границе	Наименьшее значение Rбmax	Количество КП с наименьшим Rбmax	Количество КП, удовлетворяющих границе	Общее количество пар	Количество пар, удовлетво--ряющих границе	Наименьшее значение Rбmax	Количество пар, удовлетворяющих границе
1	31	9	7 743	5	155	3 622	29 977 024	1 465 137	5	14 537 423
2	63	17	10 868	9	14	7 166	59 056 712	12 214 869	11	54 822 445

Продолжение Таблицы 3.5.

1	2	3	4	5	6	7	8	9	10	11
3	127	23	3482	17	51	1302	6 062 162	47 053	19	1 619 780
4	511	59	3819	45	6	1951	7 292 380	122 835	51	3 466 713
5	1 023	100	8 513	77	9	6 194	36 235 584	5 293 538	79	35 083 491

Анализ данных таблицы 3.5 – 3.6 показывает, что для периода последовательности, например, 63 число пар криптографических последовательностей, удовлетворяющих установленному граничному значению– 17, составляет более 12 10^6 (12 214 869). Для последовательностей с трехуровневой функцией взаимной корреляции (это лучшие с точки зрения функций взаимной корреляции линейные сигналы), число пар удовлетворяющих данной границе составляет – 975. Таким образом, ансамбль нелинейных криптографических сигналов (КС) более чем на 5 порядков превышает ансамбль указанных линейных сигналов. Превышение объема криптографических сигналов над ансамблем, составленного из М-последовательности составляет более чем на 7 порядков.

Таблица 3.6

Ансамблевые свойства различных систем сложных сигналов

Класс сигналов	Период последовательности	Значение границы «плотной упаковки»	Число пар последовательностей, удовлетворяющих границе
М-последовательности	31	9	3
ПФВКТ	31	9	495
КП	31	9	1465137
М-последовательности	127	27	36
ПФВКТ	127	17	11610

Продолжение Таблицы 3.6

КП	127	23	47 053
М-последовательности	255	36	28
ПФВКТ	_	_	_
КП	255	36	17599
М-последовательности	511	63	276
ПФВКТ	511	33	147500
КП	511	63	2666671
М-последовательности	1023	100	435
ПФВКТ	1023	65	338000
КП	1023	100	5293538

Таблица 3.7

Значения максимальных боковых пиков корреляционных функций при различных значениях границ

№ п/п	Размерность сегмента КП	Граничные значения функции неопределенности	ПФАК		АФАК		ПФВК		
			Число КП удовлетворяющих границе	Наименьшее значение Rбmax	Количество КП с наименьшим Rбmax	Количество КП, удовлетворяющих границе	Общее количество пар	Количество пар, удовлетворяющих границе	Наименьшее значение Rбmax
1	64	17	9 545	8	14	4 931	45 553 512	5 451 589	10
2	1 024	90	2 209	72	3	1 149	2 439 840	26 638	82
3	30	9	2 479	2	2	973	3 072 720	95 722	6
4	31	9	7 743	5	155	3 622	29 977 024	1 465 137	5
5	63	17	10 868	9	14	7 166	59 056 712	12 214 869	11
6	127	25	6 798	17	51	3 636	23 106 402	1 266 098	19
7	127	27	10 006	17	51	6 491	50 060 018	9 006 648	19
8	511	63	7 662	45	6	4 783	29 353 122	2 666 671	51
9	1 023	100	8 513	70	4	6 194	36 235 584	5 293 538	81

В таблице 3.7 приведены значения максимальных боковых пиков корреляционных функций криптографических последовательностей для различных значений периода и при различных значениях границ для отбора сигналов. При незначительном снижении требований к граничному значению максимального бокового пика ВКФ, в соответствии с которым осуществляется отбор сигналов (по сути, - снижение помехоустойчивости приема), могут быть существенно улучшены показатели имитостойкости функционирования ТКС. Так, для периода последовательности N = 127, увеличение значения границы на 1,2 дБ, позволит увеличить объем ансамбля с M = 11610 при границе $R_{бmax}$ = 17, до 9 006 648 сигналов, при граничном значении 27, т.е. в 776 раз.

Таким образом, разработанный метод синтеза нового класса нелинейных дискретных сигналов позволяет, изменяя граничные значения уровня боковых лепестков соответствующей функции корреляции, в зависимости от помеховой обстановки, а так же требований, предъявляемых к телекоммуникационной системе, достигать необходимые значения помехоустойчивости приема сигналов, имитостойкости и информационной скрытности сообщений абонентов системы.

В ходе исследований была разработана имитационная (программная) модель, реализующая предложенный метод синтеза дискретных последовательностей для различных периодических и апериодических корреляционных функций [103]. В Приложении В приведены блок - схема алгоритма синтеза систем нелинейных криптографических сигналов, подпрограммы и примеры реализации этапов полученного впервые метода синтеза указанной системы нелинейных сигналов.

Разработанные и програмно-реализованные алгоритмы позволяют: генерировать псевдослучайные последовательности символов практически любой длительности; получать минимальные и максимальные значения боковых выбросов периодической и апериодической функций авто - и взаимной корреляции последовательностей; сравнивать полученные значения с известными границами «плотной упаковки»; считывать отобранные, удовлетворяющие границам, последовательности; присваивать выбранным последовательностям уникальные идентификаторы с целью использования последовательностей в различных приложе-

ниях широкополосных систем. Кроме того, предлагаемый метод синтеза позволяет находить псевдослучайные последовательности с нулевыми значениями боковых пиков периодической функции автокорреляции вблизи основного пика, что является важным фактором поддержания устойчивого синхронизма в системе.

3.4 Разработка усовершенствованного метода синтеза нелинейных криптографических дискретных сигналов на основе направленного перебора

Как показали исследования [62-64] обеспечение требуемых показателей помехозащищенности, скрытности функционирования ТКС в условиях внутренних и внешних воздействий возможно на основе разработки методов анализа и синтеза нелинейных сложных дискретных криптографических сигналов с необходимыми корреляционными, ансамблевыми и структурными свойствами. В частности, при использовании таких сигналов в качестве физического переносчика информации временные затраты на раскрытие структуры используемых сигналов возрастают и постановка «оптимальных» помех становится проблематичной [63].

В разделе 3.3 сформулирована и решена задача синтеза нелинейных дискретных последовательностей, обеспечивающих требуемые значения помехозащищенности, информационной и структурной скрытности функционирования телекоммуникационной системы. Сложные сигналы, полученные на основе таких последовательностей (например, с применением системы расширения спектра методом прямой последовательности), обладают, с одной стороны, как будет показано в разделе 4, структурными свойствами, аналогичными свойствам случайных (псевдослучайных) последовательностей, а, с другой, - требуемыми ансамблевыми и корреляционными свойствами. Кроме того, системы криптографических сигналов существуют и обладают указанными выше свойствами для широкого спектра значений длин последовательностей.

Для практического использования указанных систем сигналов в целях улучшения общесистемных показателей эффективности систем, реализующих динамические принципы передачи данных, необходимо формировать большие масси-

вы сигнальных конструкций и осуществлять смену соответствия бит сообщения – сложный сигнал в установленное время по закону специальных управляющих последовательностей (радиоданных). В таких условиях становятся весьма критичными, в том числе, вопросы разработки методов синтеза и анализа (исследования) систем дискретных сложных сигналов с необходимыми свойствами, способы и средства их формирования и обработки. При этом методы и средства синтеза таких систем сигналов должны обеспечивать необходимую производительность формирования сигналов.

Отметим, что в целом ряде работ, посвященных синтезу и выбору дискретных последовательностей, приводятся верхние и нижние оценки распределения максимальных и минимальных лепестков функций авто - и взаимной корреляции [15,27]. Нахождение дискретных последовательностей с необходимыми характеристиками корреляционных функций сводится, по сути, к перебору всех возможных последовательностей, принадлежащих некоторому множеству, и отбору тех последовательностей, которые удовлетворяют известным оценкам. При этом вычислительная сложность таких методов весьма значительна.

Известно, что существует большая группа методов улучшенного перебора, объединенных общим названием «метод ветвей и границ» [23,143]. Основная идея таких методов состоит в использовании конечности множества решений и в замене их полного перебора сокращенным (направленным) перебором. Таким образом, суть методов улучшенного перебора состоит в нахождении оптимальных решений различных задач оптимизации, в частности, дискретной и комбинаторной оптимизации. Для реализации методов используют процедуру нахождения оценок (границ). Процедура нахождения оценок заключается в установлении границы для решения задачи нахождения допустимых значений. Если оценка подмножества (параметра) окажется больше, чем граница значений функции подмножества, то значение исключается из дальнейшего рассмотрения.

Идея данного метода достаточно проста. Допустим необходимо решить задачу нахождения минимума f(x) по x ∈ A. Пусть имеется некоторое разбиение множества A

S: $A = A_0||A_1||A_2||\ldots..A_k$. Известно, что в множестве A_0 оптимальных решений быть не может. Тогда

$$\{f(x) \mid x \in A\} = \min\{\min\{f(x)) \mid x \in A_i\} \mid i \in 1{:}k\}.$$

Разбиение множества А (процедура ветвления) на подмножества преследует несколько целей. Прежде всего выделение множества A_0 сокращает задачу, и естественно при этом стремятся большую часть множества А передать в A_0. Таким образом, осуществляется «отсев» подмножеств допустимых решений, заведомо не содержащих оптимальных решений. Далее, разбиение на подмножества A_i оставшейся части А может упростить задачу нахождения искомого значения задачи (в данном примере, минимума f(x)).

Реализация описанного выше общего принципа имеет определенные сложности, определяемые спецификой решаемой задачи оптимизации.

В ходе исследований получен усовершенствованный метод синтеза нелинейных криптографических последовательностей, основанный на использовании сокращенного (направленного) перебор на основе применения метода «ветвей и границ», и позволяющий повысить производительность (быстродействие) процесса синтеза сигналов, обладающих необходимыми свойствами.

Задача выбора дискретных последовательностей, удовлетворяющих известным граничным оценкам, может быть записана в виде аналитических выражений ограничений [63]:

$$Ra_1^1(l) \le \sum_{i=1}^{N} W_i^1 (W_{i+l}^{\ 1})^* \le Ra_2^1(l), l = \overline{0, N},$$

$$Ra_1^2(l) \le \sum_{i=1}^{N} W_i^{\ 2} (W_{i+l}^{\ 2})^* \le Ra_2^2(l), N' = \frac{N-1}{2}, \text{ если N- нечетное,} \qquad (3.15)$$

$$Ra_1^j(l) \le \sum_{i=1}^{N} W_i^{\ j} (W_{i+l}^{\ j})^* \le Ra_2^j(l), N' = \frac{N}{2}, \text{ если N- четное,}$$

$$\vdots$$

$$Ra_1^N(l) \le \sum_{i=1}^{L} W_i^{\ N} (W_{i+l}^{\ N})^* \le Ra_2^N(l),$$

где $Ra_1^i(e), Ra_2^i(e)$ - граничные значения боковых лепестков ФАК, N - период последовательности W_i^{υ}, $\upsilon = \overline{1, N}$.

Утверждение 3.1. Пусть максимальные (минимальные) значения реализаций функций $Ra_1^1(l)$ и $Ra_2^1(l)$ в (1) являются таковыми, что величина δ, определенная как

$$\delta = |Ra_1'(l) - Ra_1(l)| \quad \text{либо} \quad \delta = |Ra_2'(l) - Ra_2(l)|,$$

$$\delta \neq 0,1,2,\ldots P-1,P \tag{3.16}$$

больше P, а W^j - сигнал определен над полем $GF(P)$ или над кольцом чисел по модулю P, тогда множество значений циклической свертки (функции автокорреляции (ФАК)) $Ra^Z(l)$ может принадлежать интервалу

$$(\min Ra_1(l), \max Ra_2(l)), \tag{3.17}$$

по крайней мере при “отбрасывании” r последних и “добавлении” r первых символов сигнала W, где

$$r = \frac{\delta}{P}, \text{ если } \delta | P \text{ и } r = \frac{\delta + t}{P}, \text{ если } \delta \neq P.$$

Доказательство утверждения 3.1.

Предположив, что $Wa_1'(l) < \min Ra_1(l)$, рассмотрим функцию автокорреляции сигнала. Так как символы W^j определены в кольце чисел по модулю P, либо над полем $GF(P)$, то при «отбрасывании» W_1 и «добавлении» W_{L+1}, Ra_1' возрастает по крайней мере на P. Аналогично при «отбрасывании» символа W_2 и «добавлении» W_{L+2}, Ra_1' возрастает не более чем на P и, таким образом, после r «отбрасываний» $\min Ra_1'(l)$ и добавлений r символов каждый с максимальным расстоянием P:

$$\min Ra'(l) \geq Ra_1'(l) + P \cdot r, \tag{3.18}$$

поэтому

$$r' \geq \frac{\min Ra'(l) - Ra'_1(l)}{P} \qquad (3.19)$$

В действительности величина $r > r'$, а вероятность того, что за r шагов $Ra'(l)$ станет равной значению $\min Ra'(l)$ достаточно мала.

Рассмотрим второй случай, когда

$$Ra'_2(l) > \max Ra_2(l).$$

Рассуждая аналогично вышеприведенному, после r шагов получим

$$\max Ra_2(l) < \max(Ra'_2(l) - P \cdot r)$$

и

$$r \geq \frac{\max Ra'_2(l) - Ra_2(l)}{P} \qquad (3.20)$$

С учетом (3.18) и (3.20), дополняя их величиной t, но так, чтобы $(\delta + t)$ являлось делителем P, имеем $r = \frac{\delta}{P}$, если $\delta | P$ и $r = \frac{|\delta| + t}{P}$, если δ не делит P.

Следствие утверждения 3.1. Если $W_i \in GF(P)$, то $r = \frac{\delta}{2}$, если δ - четное и $r = \frac{\delta + 1}{2}$, если δ - нечетное.

Подчеркнем, что утверждение 3.1 и ее следствие имеют важное значение, т.к. из них следует, что за $r < r'$ «отбрасываний» и r «дополнений» $\min Ra'(l)$, и $\max Ra'_2(l)$ не может попасть в интервал $(\min Ra_1(l), \max Ra_2(l))$.

В ходе исследований было проведено имитационное моделирование приведенного выше метода синтеза последовательностей. Были выполнены оценки производительности (быстродействия) такого метода. В качестве источника нелинейных криптографических сигналов был использован стандарт шифрования данных Украины «Калина» [68]. В качестве криптографической последовательности были использованы сегменты последовательностей размерностью 10000 и 20000 символов. В процессе моделирования, с помощью представленного выше метода, были выбраны последовательности с различным периодом следования символов (от 256 до 1024), функция автокорреляции которых отвечают границе «плотной

упаковки» для указанных периодов. Анализ результатов исследований показал, что данный метод обеспечивает выигрыш в производительности синтеза дискретных последовательностей от 40 до 60 процентов по отношению к методу синтеза системы сигналов, основанному на переборе всех возможных вариантов последовательностей. При реализации рассматриваемого метода возможны пропуски (потери) в нахождении лучших сигналов. Но как показали исследования, процент таких потерь – незначителен, и для указанных периодов составляет не более 8 процентов.

Выводы к разделу 3

В третьем разделе диссертации решены **четвертая и седьмая** задачи исследования.

1. В условиях интенсивного противодействия сторон, интересы и конкуренция которых могут быть проявляться в различных сферах, в том числе, как показали последние события, в сфере ведения информационных и гибридных войн, особое значение приобретает наличие и применение защищенных телекоммуникационных систем. В существенной мере такие системы базируются на применении защищенных радиоканалов. При этом под защищенностью систем необходимо понимать, в широком смысле, прежде всего, их способность обеспечивать необходимые показатели по помехозащищенности, имитостойкости, информационной, энергетической и структурной скрытности.

2. В ТКС в качестве физическиого переносчика информации нашли применение различные системы (множества линейных рекуррентных последовательностей, Касами, Голда, Камалетдинова и др.), обладающие сравнительно небольшими значениями боковых лепестков авто и взаимно - корреляционных функций [51,21,18-19,]. Однако указанные сигналы обладают низкой структурной скрытностью, ограниченными ансамблевыми свойствами, а также существуют только для ограниченного числа значений периода сигнала. В случае усечения (увеличения) периода таких сигналов их корреляционные свойства ухудшаются. Поэтому актуальной является задача разработки теории и практики синтеза и анализа систем

дискретных сигналов с требуемыми корреляционными, структурными, ансамблевыми свойствами.

Исследования показали [59-60,82,84,86], что требуемые (в тех или иных условиях) показатели эффективности функционирования системы могут быть реализованы, в том числе, посредством применения широкополосных радиосистем, для которых расширение спектра осуществляется с применением нелинейных дискретных последовательностей.

3. Необходимость применения защищенных радиоканалов вынуждает исследователей по-новому посмотреть как на режимы функционирования защищенных радиоканалов, так и на аспекты формирования и применения сложных сигналов. Поэтому, на наш взгляд, необходимы новые подходы и новые взгляды на процессы применения и функций непосредственно самих сложных сигналов. Основополагающим здесь, на наш взгляд, является новое понимание методов обеспечения информационной скрытности и имитостойкости, то есть функций, которые в традиционных системах возлагаются на системы и средства криптографической защиты информации. Поэтому, продуктивным шагом, с точки зрения нового направления использования систем сложных сигналов, является синтез так называемых систем криптографических сигналов. Синтез таких сигналов основывается на применении ключевых данных, и при этом, сигналы должны обладать: абсолютной структурной скрытностью относительно законов их формирования и смены сигналов в динамическом режиме; улучшенными ансамблевыми свойствами (существовать практически для любого значения периода, иметь значительный объем системы сигналов); необходимыми, для обеспечения требуемого значения помехоустойчивости, корреляционными свойствами. Для защищенных радиоканалов рассматриваемые системы сигналов определяются приложениями, в которых они применяются. В частности, это могут быть как отдельные сигналы или пары сигналов, так и большие множества дискретных последовательностей с необходимыми, но объективно ограниченными значениями «плотной упаковки», взаимно-корреляционными и ансамблевыми свойствами.

Под криптографическим дискретным сигналом предлагается понимать последовательность символов произвольного алфавита и произвольного периода, единственным правилом построения которого есть случайность или псевдослучайность. Такой дискретный сигнал обладает необходимыми, но ограниченными значениями «плотной упаковки», корреляционными и ансамблевыми свойствами. При таком подходе структурная скрытность сигнала обеспечивается посредством случайности или псевдо случайности. Также необходимо отметить особое свойство таких систем сигналов – возможность их восстановления в пространстве и времени с применением ключей и ряда других параметров, которые используются в процессе синтеза сигналов.

4. С учетом требований криптографической стойкости и сложности генерирования криптографического сигнала в качестве генератора сигналов обоснован выбор алгоритма симметричного блочного шифрования со счетчиком. В качестве блочного шифра предложено использовать национальный стандарт ДСТУ 7624:2014 [68]. Также в качестве альтернативы можно использовать алгоритм AES из международного стандарта ISO/IEC 18033 [1]. Предпочтение при выборе отдано ДСТУ 7624:2014, так как, по нашему мнению, он относится к пост квантовым алгоритмам, т.е. - будет обеспечивать (при выборе соответствующих параметров) криптографическую стойкость против атак с применение квантовых компьютеров.

5. В общем случае задача синтеза оптимальных бинарных криптографических сигналов заданного периода, формулируется следующим образом. Необходимо найти множество дискретных двоичных последовательностей с заданным числом битов, обладающих допустимым уровнем максимальных боковых лепестков периодической функции автокорреляции. Далее, решение задачи синтеза сводится к предварительному отбору некоторого ограниченного множества дискретных последовательностей, которое кажется многообещающим в плане обеспечения необходимых взаимно - корреляционных свойств.

6. Впервые получен метод синтеза сложных нелинейных дискретных сигналов, использующий случайные или псевдослучайные процессы, (в частности, реа-

лизуемые одним из режимов блочного симметричного шифра «Калина»), позволяющий формировать большие ансамбли дискретных последовательностей практически любого периода с заданными, но физически реализуемыми, значениями боковых лепестков функций авто – взаимной и стыковой функции корреляции в периодическом и апериодическом режимах работы, а так же статистическими характеристиками корреляционных функций, не уступающих аналогичным характеристикам лучших, с точки зрения корреляционных функций, линейных классов сигналов. Так для периода последовательности 63 число пар криптографических дискретных последовательностей, удовлетворяющих установленному граничному значению – 17, составляет 12 214 869. Для представителя класса линейных последовательностей - последовательностей с трехуровневой функцией взаимной корреляции (это лучшие с точки зрения функций взаимной корреляции сигналы), число пар удовлетворяющих данной границе составляет – 975 пар. Таким образом, ансамбль криптографических сигналов более чем в 10^5 раз превышает ансамбль указанных линейных сигналов. Превышение объема криптографических сигналов над ансамблем, составленного из М-последовательности составляет более чем 10^7 раз. Для периода последовательности 1023, число пар криптографических дискретных последовательностей, удовлетворяющих установленному граничному значению для боковых лепестков функций взаимной корреляции (ФВК) – 100, составляет 5 293 538, тогда как для представителя класса линейных последовательностей - М-последовательностей число пар, удовлетворяющих данной границе, составляет – 435, т.е. превышение объема системы сигналов составляет более чем 10^5 раз. Кроме того, построенные таким образом сигналы являются самосинхронизирующимися, а также обладают идеальной (абсолютной) структурной скрытностью. Абсолютная структурная скрытность таких сигналов состоит в том, что ни один последующий бит, даже последний, такого сигнала не может быть однозначно определен при известных предыдущих символах. Необходимо подчеркнуть, что закон формирования каждого из криптографических сигналов определяется ключом, причем длина ключа может быть существенно меньше периода (длины) самого сигнала.

7. Приведенные характеристики систем сигналов, синтезируемых с применением разработанного метода, позволяют говорить об улучшении качественных показателей функционирования телекоммуникационной системы: помехозащищенности и информационной безопасности. Более детальная оценка показателей эффективности телекоммуникационной системы будет приведена на основе результатов исследований свойств систем сигналов (раздел 4), синтезированных с применением методов синтеза, представленных в разделах 2 и 3 данной диссертационной работы, и разработанного усовершенствованного метода информационного обмена (раздел 5).

8. Разработан усовершенствованный метод синтеза нелинейных дискретных криптографических систем сигналов, основанный на оптимизации процесса синтеза системы сигналов с использованием метода ветвей и границ, позволяющий уменьшить, по сравнению с полным перебором, объем вычислительных процедур синтеза систем сигналов и, следовательно, повысить производительность процесса синтеза систем сигналов с необходимыми, для тех или иных приложений телекоммуникационных систем, свойствами.

9. Разработанные программные реализации позволяют: генерировать криптографические сигналы практически любого периода; получать минимальные и максимальные значения боковых выбросов периодической и апериодической функций авто - и взаимной корреляции последовательностей; сравнивать полученные значения с известными границами «плотной упаковки»; считывать отобранные, удовлетворяющие границам, последовательности; присваивать выбранным последовательностям уникальные идентификаторы с целью оптимальной обработки сигналов в различных приложениях широкополосных систем. Кроме того, предлагаемый метод синтеза позволяет синтезировать псевдослучайные последовательности с нулевыми значениями боковых пиков периодической функции авто и взаимной корреляции вблизи основного пика, что является важным фактором поддержания устойчивого синхронизма в системе.

РАЗДЕЛ 4
ИССЛЕДОВАНИЯ СВОЙСТВ СЛОЖНЫХ НЕЛИНЕЙНЫХ ДИСКРЕТНИХ СИГНАЛОВ

К телекоммуникационным системам предъявляются все более жесткие требования по обеспечению эффективности функционирования в условиях сложных внешних воздействий: естественных и преднамеренных помех, помех от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот. Значительное число современных систем относятся к многопользовательским системам. В таких системах множество каналов размещаются в пределах общего частотно-временного ресурса, так что каждый абонент имеет возможность передавать и принимать информацию одновременно с другими абонентами и независимо от них. Один из наиболее широко применяемых в настоящее время методов множественного доступа (уплотнения или разделения), т.е. возможности одновременного использования многими абонентами канала связи с минимальным взаимным влиянием абонентов в таких многопользовательских системам, является метод, основанный на кодовом разделении каналов. Поскольку кодовое разделение основано на том, что каждому абоненту (пользователю) выделяется персональная адресная сигнатура (сигнал), то построение таких многопользовательских систем и их характеристики определяются выбором систем сигналов и их свойствами.

Как было показано в разделе 1, большое значение при решении задач обеспечения требуемой помехозащищенности и информационной безопасности имеют исследования, связанные с использованием новых видов сигналов, получивших название сложных, широкополосных, многомерных и шумоподобных. Применяемые в ТКС способы информационного обмена, основанные на фиксированном соответствии: бит сообщения (m бит) - сигнал (2^m сигналов) в информационном канале, и использование (в течение продолжительного времени) в канале синхронизации одного и тот же широкополосного сигнала (причем используемые сигналы построены с применением линейных законов), не позволяют достичь необхо-

димых значений помехозащищенности и информационной безопасности функционирования телекоммуникационной системы.

Комплексное решение проблемы обеспечения помехозащищенности и информационной безопасности функционирования телекоммуникационной системы может быть достигнуто, в том числе, на основе реализации динамического режима передачи информации, при котором соответствие: бит сообщения – сигнал меняется с течением времени по закону, предсказание которого возможно с вероятностью не превышающей допустимого в системе значения, и применения сигналов с необходимыми корреляционными, ансамблевыми, статистическими, структурными свойствами. При этом системы сигналов должны основываться на нелинейных правилах построения.

Появление в последние годы новых областей использования дискретных сигналов потребовало дополнительного и более тщательного изучения их ансамблевых, корреляционных, структурных и других свойств.

В настоящем разделе приведены результаты исследований свойств различных классов нелинейных дискретных сигналов

4.1 Ансамблевые свойства нелинейных дискретных сигналов в конечных полях

Из соотношения (1.34) следует, что имитостойкость телекоммуникационной системы со сложными каналами зависит от размерности ансамбля используемых сигналов. В дальнейшем размерность ансамбля (объем системы) сигналов будем оценивать мощностью изоморфного, автоморфного и изоморфно-зеркального кодирования [140,144,146], а для производных сигналов, образованных по правилу (2.52) – мощностью производного авто - изоморфного кодирования.

Для исследования мощности системы характеристических дискретных сигналов образуем множество из чисел, равных порядковым номерам символов кода μ, принимающих значения 1. Множество

$$B = \{i : \mu_i = 1, i = 0, 1, \ldots, p^n - 2\}, \qquad (4.1)$$

есть разностное множество, сбалансированное на два уровня, с параметрами (2.3), если μ определяется правилом кодирования (2.22).

Мощность метода кодирования равна числу классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы $T = \{t\}\,(t, N) = 1$ на смежные классы по классу автоморфных коэффициентов. Докажем, что числа $p^k \pmod N, k = 0, 1, \ldots, n-1$, являются автоморфными коэффициентами (4.1) множества B. Согласно (4.1)

$$B_{p^k}(N, K^+, \lambda_1, \lambda_2) \equiv p^k B(N, K^+, \lambda_1, \lambda_2) \pmod N \equiv p^k \{i : \mu_i = 1, i = 0, 1, \ldots, p^n - 2\} \pmod N \equiv$$
$$\equiv \{i\, p^k : \mu_i = 1, i = 0, 1, \ldots, p^n - 2\} \pmod N.$$

Обозначим $n = i\, p^k$, тогда $i = n\, p^{-k}$ и $B_{p^k}(N, K^+, \lambda_1, \lambda_2) \equiv \{n : \mu_{np^{-k}} = 1,$

$n = 0, 1, \ldots, p^n - 2\} \pmod N,$

где, по определению (2.3), $\mu_{np^{-k}} = \psi[\Theta^{np^{-k}} + 1] = \psi[(\Theta^n)^{p^{-k}} + 1]$.

В поле характеристики p $\psi[(\Theta^n)^{p^{-k}} + 1] = \psi[(\Theta^n + 1)^{p^{-k}}] = [\psi(\Theta^n + 1)]^{p^{-k}}]$.

Так как для всякого нечетного $p, p > 2$,

$$[\psi(\Theta^n + 1)]^{p^{-k}} = \psi(\Theta^n + 1), \qquad (4.2)$$

то $\mu_{np^{-k}} = \mu_n$ и

$$B_{p^k}(N, K^+, \lambda_1, \lambda_2) = \{n : \mu_n = 1, \quad n = 0, 1, \ldots, p^n - 2\} \pmod N. \qquad (4.3)$$

Сопоставляя (4.1) и (4.3), легко видеть, что $B = B_{p^k}$. Тем самым доказано, что числа $p^k, k = 0, 1, \ldots, n-1$ являются автоморфными коэффициентами множества $B(N, K^+, \lambda_1, \lambda_2)$ (4.1).

Множество коэффициентов $T = \{t\}, (t, N) = 1$ разбивается на $\phi(N)/n$ непересекающихся классов. Действительно, так как множество $T = \{t\}$, содержащее $\phi(N)$ коэффициентов, есть мультипликативная группа по модулю N, а класс автоморфных коэффициентов $T_1 = \{p^k, k = 0, 1, \ldots, n-1\}$, содержащий n коэффициентов,

является подгруппой T, разбивая группу T на смежные классы по подгруппе T_1, получим $\phi(N)/n$ смежных классов, каждый из которых содержит n коэффициентов. Таким образом, число изоморфных множеств (4.1) равно $\phi(N)/n$.

Методика построения всех классов коэффициентов T_k, $k = 1, \dots, \phi(N)/n$, состоит в следующем. Класс автоморфных коэффициентов, как уже указывалось, содержит все степени числа p:

$$T_1 = \{t_{1,i} \equiv p^i (\mathrm{mod}\, N), i = 0, 1, \dots, n-1\}. \qquad (4.4)$$

Классы T_k состоят из элементов $t_{k,i}$, определяемых следующим образом:

$$\begin{aligned} &T_k = \{t_{k,i} \equiv \tilde{t}_k t_{1,i} (\mathrm{mod}\, N), \tilde{t}_k \in T_k, \\ &\tilde{t}_k \notin T_1, T_2, \dots, T_{k-1}\}, \\ &k = 2, 3, \dots, \phi(N)/n, i = 0, 1, \dots, n-1 \end{aligned} \qquad (4.5)$$

Для каждого коэффициента $t_{k,i}$ можно найти такой коэффициент $t_{l,u}$, чтобы

$$t_{k,i} + t_{l,u} \equiv 0 (\mathrm{mod}\, N).$$

Классы T_k и T_l являются инверсно-изоморфными. Взяв по одному коэффициенту из каждого инверсно-изоморфного класса, получим множество T неинверсно-изоморфных коэффициентов, приводящих к $\phi(N)/2n$ неинверсно-изоморфным разностным множествам, сбалансированным на два уровня. Таким образом, мощность каждого из методов кодирования (2.3) и (2.4) равна $\phi(N)/2n$.

Заметим, что природа изоморфизма связанна с использованием для построения множества $B(N, K^+, \lambda_1, \lambda_2)$ различных первообразных элементов поля $GF(p)$ (если $N = p-1$) или различных первообразных неприводимых над полем $GF(p)$ полиномов степени n (если $N = p^n - 1, n > 1$).

Действительно, если θ_1 и θ_2 - различные первообразные элементы поля GF(p), то $\theta_2 \equiv \theta_1^k$, (k,p-1)=1 и, следовательно,

$$\begin{aligned} &B_{\theta_1} = \{i : \varphi(\theta_1^i + 1) = 1, i = 0, 1, \dots, p^n - 2\}, \\ &B_{\theta_2} = \{i : \varphi(\theta_1^{ki} + 1) = 1, i = 0, 1, \dots, p^n - 2\} = \{uk^{-1} (\mathrm{mod}\, N) : \varphi(\theta_1^u + 1) = 1, u = 0, 1, \dots, p^n - 2\}, \end{aligned} \qquad (4.6)$$

откуда видно, что B_{θ_1} и B_{θ_2} не автоморфны.

Аналогично доказывается, что если θ_1 и θ_2 - корни различных первообразных неприводимых над полем GF(p) полиномов степени n, то B_{θ_1} и B_{θ_2} не автоморфны [43,126].

С другой стороны, если использовать для построения разностного множества, сбалансированного на два уровня, различные первообразные элементы поля $GF(p^n)$, являющиеся корнями одного и того же преобразования неприводимого над GF(p) полинома f(x) степени n, то соответствующие разностные множества будут автоморфными.

Действительно, пусть θ - первообразный элемент поля $GF(p^n)$ и f(x)=0, тогда p - сопряженные элементы поля $GF(p^n)$, θ^{p^k}, k=1,2,...,n-1, также первообразные элементы этого поля.

Обозначим через B_θ и $B_{\theta^{p^k}}$ разностные множества, сбалансированные на два уровня, построенные соответственно по первообразным элементам θ и θ_{p^k}, k=1, 2,..., n-1. Тогда

$$B_{\theta^{p^k}} = \{i : \varphi(\theta^i + 1) = 1, i = 0,1,..., p^n - 2\} = B_\theta.$$

Мультипликативно обратные первообразные элементы, если N=p-1, и взаимные первообразны неприводимые над полем GF(p) полиномы степени n, если $N=p^n-1$, n>1, приводят к инверсным изоморфизмам. Действительно, пусть B_θ и $B_{\theta^{-1}}$ - разносные множества, сбалансированные на два уровня, построенные соответственно по мультипликативно обратным элементам θ и θ^{-1} поля GF(p).

Тогда

$$B_\theta = \{i : \varphi(\theta^i + 1) = 1, i = 0,1,..., p^n - 2\}$$

и

$$B_{\theta^{-1}} = \{i : \varphi(\theta^{-i} + 1) = 1, i = 0,1,..., p^n - 2\} = \{p^n - 1 - i(\mathrm{mod}\, N) : \varphi(\theta^i + 1) = 1, i = 0,1,..., p^n - 2\}.$$

Очевидно, что B_θ и $B_{\theta^{-1}}(\mathrm{mod}\ N)$ автоморфны, и, следовательно, B_θ и $B_{\theta^{-1}}$ - инверсно-изоморфны. Аналогично доказывается, что взаимные полиномы приводят к инверсному изоморфизму. Изложение позволяет построить все неинверсно-

изоморфные множества $B(N,K+,\lambda_1,\lambda_2)$ и, следовательно, все неинверсно-изоморфные усеченные коды μ^{t_n}, которые можно получить при помощи методов кодирования (2.22) и (2.23). Для каждого из кодов μ^{t_n} следует, путем циклической перестановки его символов, найти оптимальные по минимаксному критерию импульсные коды и отобрать среди них наилучшие.

Как следует из приведенного объем системы сигналов, составленной из характеристических дискретных сигналов, составляет $M = \phi(N)/2n$. Таким образом, мощность изоморфного кодирования пропорциональна функции Эйлера и обратно пропорциональна степени расширения n поля $GF(p^n)$.

Исследование мощности изоморфного кодирования, предпочтительно выполнять на основе изучения изоморфизмов разностных множеств. В [144] показано, что каждому коэффициенту разностных множеств может быть поставлен в соответствие первообразный элемент поля $GF(p^n)$. Алгоритмы, программы и примеры расчета первообразных элементов поля для заданной характеристики поля P, функции Эйлера приведены в Приложениях А и Б.

В таблице 4.1 приведены значения объем системы сигналов M для некоторых значений периода последовательности L характеристических дискретных сигналов (ХДС).

Таблица 4.1

Значения объема системы ХДС

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

Важной составляющей ансамблевых свойств системы сигналов является спектр значений периода сигналов, для которых могут быть синтезированы сигналы данной системы. Как отмечалось выше, ХДС могут быть синтезированы для значений периода, определяемого из соотношений: $N = 4x+2 = p^n - 1$ и $N = 4x = p^n - 1$. В таблице приведены значения числа ХДС, которые могут быть синтезированы в некотором интервале ς периода сигналов.

Таблица 4.2

Значения числа ХДС, которые могут быть синтезированы в некотором интервале ς

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

В табл. 4.3 Приведены обобщенные данные о числе значений длин сигналов и объеме системы сигналов для М - последовательностей и характеристических дискретных сигналов

Таблица 4.3

Обобщенные сведения о ансамблевых свойствах М - последовательностей и характеристических дискретных сигналов

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

Анализ приведенных выше аналитических соотношений данных табл. 4.1 – 4.3 свидетельствует о том, что характеристические дискретные сигналы с точки зрения ансамблевых свойств являются более предпочтительными по сравнению целым рядом широко используемыми в различных приложениях телекоммуникационных систем, такими как М- последовательности, последовательности Лежандра и другие. Например, на интервале длин от 50 до 1500, М - последовательности существуют только для пяти значений периода, доступное число последовательностей Лежандра составляет 114, число характеристических сигналов для этого интервала длин составляет 225. Более того, мощность метода кодирования

для данных последовательностей (объем системы $M = \Psi(N)/2n$ для заданного $N = P^n - 1$) определяется числом классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы $T = \{t\}\ \{t, N\} = 1$ на смежные классы по классу автоморфных коэффициентов и равна $\Psi(N)/2n$. Так для характеристического кода с числом элементов $N = 2052$ существует 515 изоморфизмов данного кода, в то время как для М-последовательностей ($N = 2047$) только 88 изоморфизмов. Объем системы, составленной из ХДС в интервале длительностей до 10000 символов более чем 3 10^3 раз превышает объем системы, составленной из М-последовательностей. Кроме того, ХДС могут быть построены (в указанном выше интервале) более чем в 115 раз большего числа значений N по сравнению с М-последовательностями.

Система сигналов может быть расширена за счет привлечения автоморфизмов (циклических сдвигов) изоморфных сигналов. Указанное становится возможным в том случае, если все множество циклических сдвигов (или отдельные автоморфизмы) обладают необходимыми корреляционными свойствами. Более детально этот вопрос будет исследован в следующем разделе.

Таким образом, мощность авто - и изоморфного кодирования $M_{аи}$ в классе характеристических дискретных сигналов при заданном периоде последовательности L может быть определена из соотношения

$$M_{аи} = N\varphi(N)/2n. \qquad (4.7)$$

В классе производных характеристических сигналов, построенных по правилу (2.22) при k = 2, мощность производного авто - и изоморфного кодирования ($M_{паи)}$ равна:

$$M_{паи} = (N+2)\varphi(N)(\varphi(N) - 2n)/8n^2. \qquad (4.8)$$

В таблице 4.4 приведены значения $M_{паи}$ для некоторых значений L, вычисленных с использованием соотношения (4.8).

Таблица 4.4

Мощность производного авто и изоморфного кодирования в классе характеристических сигналов

N	66	100	130	256	508	1018	2098
M_a	$3{,}1\ 10^3$	$1{,}9\ 10^4$	$3{,}7\ 10^4$	$5{,}2\ 10^5$	$4{,}0\ 10^6$	$3{,}3\ 10^7$	$2{,}9\ 10^8$
N	3000	4000	5002	6010	7012	8008	9010
M_a	$2{,}4\ 10^8$	$1{,}3\ 10^8$	$3{,}6\ 10^9$	$4{,}3\ 10^9$	$1{,}1\ 10^{10}$	$8{,}3\ 10^9$	$1.2\ 10^{10}$

В разделе 3 приведены теоретические основы синтеза нелинейных криптографических дискретных сигналов. Проведем оценку ансамблевых свойств данной системы сигналов. Необходимо отметить, что нелинейные дискретные криптографические сигналы, в отличие от известных классов сигналов, применяемых в различных приложениях телекоммуникационных систем, могут быть синтезированы для любых значений периода дискретных сигналов. Синтез данного класса сигналов основывается на ограничениях, связанных с граничными значениями функций авто – и взаимной корреляции сигналов в периодическом и апериодическом режимах передачи информации. Подходы к выбору граничных значений изложены в ряде работ [15,27,33,145] и приведены в разделе 1.

Объем системы нелинейных криптографических сигналов (мощность кодирования) определяется, во-первых, требованиями, обусловленными применением данного класса сигналов (обнаружение и измерение параметров сигнала, режим передачи данных пользователей и др.), и, во-вторых, требованиями, предъявляемыми к системе с точки зрения таких показателей эффективности функционирования телекоммуникационной системы, как помехоустойчивость приема сигналов, информационная скрытность и имитостойкость системы. Пользователю (владельцу) системы, исходя из указанных ограничений, необходимо принимать компромиссные решения о выборе того или иного ансамбля нелинейных криптографических сигналов с необходимыми свойствами.

Для большинства приложений ТКС интерес представляют большие множества сигналов с хорошими взаимно-корреляционными свойствами. Именно по-

этому проблема синтеза системы сигналов рассматривалась как комплексная проблема, включающая синтез сигналов, обладающих необходимыми (для определенных условий) ансамблевыми, корреляционными и структурными свойствами.

Таблица 4.5

Ансамблевые свойства различны классов сигналов

Класс сигналов	Период последовательности	Значение границы «плотной упаковки»	Число пар последовательностей, удовлетворяющих границе
М-последовательности	31	9	3
ПФВКТ	31	9	495
КС	31	9	1465137
М-последовательности	127	27	36
ПФВКТ	127	17	11610
КС	127	23	47 053
М-последовательности	255	36	28
ПФВКТ	_	_	_
КС	255	36	17599
М-последовательности	511	63	276
ПФВКТ	511	33	147500
КС	511	63	2666671
М-последовательности	1023	160	435
ПФВКТ	1023	65	338000
КС	1023	100	5293538

В таблице 4.5 приведена сравнительная характеристика объема системы различных классов сложных сигналов (в том числе, нелинейных криптографических сигналов (КС)) для различных значений периода сигнала. В данной таблице указаны предельные значения максимальных боковых пиков периодической функции взаимной корреляции (ПФВК), которые имеют место для лучших с точки зрения взаимнокорреляционных свойств сигналов (последовательности с 3-уровневой

ПФВК - ПФВКТ) [140]. В качестве одной из составляющих, характеризующих ансамблевые свойства приведенных в таблице систем сигналов, приводится число пар сигналов, удовлетворяющих границе «плотной упаковки».

Анализ данных таблицы 4.5 показывает, что нелинейные криптографические последовательности обладают существенно улучшенными по сравнению с М-последовательностями ансамблевыми свойствами. Так число пар криптографических последовательностей, которые могут быть синтезированы для периода последовательности 31, отвечающих предельно допустимому значению максимальных боковых пиков ПФВК, более чем на пять порядков превышает число пар для М – последовательностей и на более чем четыре порядка - для последовательностей с 3-уровневой ПФВК. Для периода последовательности L = 1023, выигрыш в объеме системы сигналов, при незначительном увеличении значений боковых пиков ПФВК по отношению к граничному значению, в сравнении с последовательностями с 3-уровневой ПФВК, составляет более чем 15 раз, а по сравнению с М – последовательностями (при меньших значениях боковых лепестков ПФВК криптографических последовательностей) – более чем три порядка.

4.2 Математическая модель структуры дискретных последовательностей в конечных полях. Структурные свойства нелинейных дискретных сигналов

В разделе 1 было показано, что скрытность функционирования телекоммуникационной системы в значительной мере определяется структурной скрытностью используемой системы сигналов. Известно, что вследствие низкой структурной скрытности линейных классов сигналов, они не могут быть использованы в приложениях ТКС, для которых предъявляются повышенные требования с точки зрения скрытности функционирования.

Выполним оценку структурной скрытности нелинейных дискретних сигналов, теоретические основы синтеза котрого приведены в разделе 2. Для этого, сформули рем и докажем утверждения, определяющие связи элементов конечного поля [61].

Утверждение 4.1. Пусть a_1, a_2,..., $a_{(P-1)/2}$ — элементы поля GF(P), тогда элементы поля $a_{(P-1)/2+1}$, $a_{(P-1)/2+2}$,..., a_{P-1} зависят от (P-1)/2 первых элементов и определяются из выражения:

$$a_{(P-1)/2+i} = P - a_i, \qquad (4.9)$$

где $i = \overline{1,(P-1)/2}$.

Доказательство. Известно, что i-й элемент поля может быть представлен как $a_i = \Theta^{i-1} \bmod (P)$, а ((P-1)/2+ i)-й элемент имеет вид: $a_{(P-1)/2+i} = \Theta^{(P-1)/2+i-1}$.

Тогда (4.9) можно записать следующим образом:

$$\Theta^{i-1} + \Theta^{(P-1)/2+i-1} = P \equiv 0 \,(\text{mod } P).$$

Вынеся за скобки Θ^{i-1}, получим:

$$\Theta^{i-1}(1+\Theta^{(P-1)/2}) = P \equiv 0 \,(\text{mod } P). \qquad (4.10)$$

В соответствии с теоремой Ферма:

$$\Theta^{P-1} \equiv 1 \,(\text{mod } P); \text{ и } (\Theta^{(P-1)/2}-1)(\Theta^{(P-1)/2}+1) \equiv 0 \,(\text{mod } P). \qquad (4.11)$$

В (4.11) только один из сомножителей левой части делится на P. В противном случае их разность, равная 2, должна делится на P. Поэтому имеет место одно и только одно из сравнений

$$\Theta^{(P-1)/2} \equiv 1 \,(\text{mod } P) \qquad (4.12)$$

$$\Theta^{(P-1)/2} \equiv -1 \,(\text{mod } P). \qquad (4.13)$$

Сравнение (4.12) не может выполняться, так как в поле Галуа лишь $\Theta^{P-1} \equiv 1 \,(\text{mod } P)$ и $\Theta^0 \equiv 1 \,(\text{mod } P)$. Поэтому выполняется сравнение (4.13). В этом случае справедливо и (4.10). Тогда ((P-1)/2+ i)-й элемент поля может быть найден из соотношения $a_{(P-1)/2+i} = P - a_i$. Утверждение доказано.

Проиллюстрируем на примере возможность построения ((P-1)/2+i)-х элементов поля по известным первым (P-1)/2 элементам.

Пусть характеристика поля GF(P) P = 13, первообразный элемент поля $\Theta = 2$.

Запишем элементы данного поля:

$$a_1 = 2^0 \bmod 13 = 1; a_2 = 2^1 \bmod 13 = 2; a_3 = 2^2 \bmod 13 = 4; a_4 = 2^3 \bmod 13 = 8;$$
$$a_5 = 2^4 \bmod 13 = 3; a_6 = 2^5 \bmod 13 = 6; a_7 = 2^6 \bmod 13 = 12; a_8 = 2^7 \bmod 13 = 11; \quad (4.14)$$
$$a_9 = 2^8 \bmod 13 = 9; a_{10} = 2^9 \bmod 13 = 5; a_{11} = 2^{10} \bmod 13 = 10; a_{12} = 2^{11} \bmod 13 = 7.$$

Воспользуемся выражением (4.14) для получения ((P-1)/2+ i)-х элементов поля ($i = \overline{1,(P-1)}$):

$$a_7 = a_{(P-1)/2+1} = P - a_1 = 12; a_8 = a_{(P-1)/2+2} = P - a_2 = 11; a_9 = a_{(P-1)/2+3} = P - a_3 = 9; \quad (4.15)$$
$$a_{10} = a_{(P-1)/2+4} = P - a_4 = 5; a_{11} = a_{(P-1)/2+5} = P - a_5 = 10; a_{12} = a_{(P-1)/2+6} = P - a_6 = 7.$$

Сравнение соответствующих элементов поля, приведенных в (4.14) с элементами поля (4.15) показывает, что они идентичны.

Рассмотрим более подробно, чем это сделано в теореме 2, конструкцию поля Галуа.

Для произвольно выбранного первообразного элемента Θ_l поля произведение

$$(\Theta_l^i \Theta_l^{P-1-i}) \bmod P \equiv 1 (\bmod P). \quad (4.16)$$

Справедливость (4.16) вытекает из того, что для простого P $\phi(P) = P - 1$. Из теоремы Эйлера следует, что $\Theta^{\phi(P)} = \Theta^{P-1} \equiv 1 (\bmod P)$, поэтому $(\Theta_l^i \Theta_l^{P-i-1}) \bmod P = \Theta^{P-1} \equiv 1 (\bmod P)$. Ввиду того что сравнение (4.16) выполняется при любом Θ_l и P, при i =1 элемент поля a_2 однозначно связан с элементом a_{P-1}, при i=2 элемент поля a_3 связан с элементом a_{P-2} и т.д. Анализ (4.16) показывает, что элементы поля a_1 и a_{P-2}, a_2 и a_{P-2} являются мультипликативно обратными.

В связи с указанным свойством поля Галуа зависимыми оказываются, очевидно, и характеры элементов поля или символы ХДС, построенные в поле. Эта зависимость определяется утверждением 4.2.

Утверждение 4.2. Пусть характер элементов $\psi(a_i)$ поля (символы ХДС в поле GF(P)) определяются из соотношения

$$W_i = \psi(a_i) = \exp(j\pi u_i), \quad (4.17)$$

а индексы элементов поля U_i находят из решения сравнения:

$$a_i = \Theta_l^i + 1 = \Theta_l^{U_i} (\bmod P),$$

тогда характеры $(P-1)/2+1+i\,(i=\overline{1,(P-1)/2-1})$ элементов поля (символы сигнала) зависят от характеров (P-1)/2-i первых элементов поля, причем

$$W_{P-i} = (-1)^i W_{i+1}. \qquad (4.18)$$

Доказательство. Рассмотрим произвольный элемент поля $a_i = \Theta^i + 1$. По теореме Ферма $\Theta^{P-1} \equiv 1 (\mathrm{mod}\, P)$. Тогда элемент поля

$$\Theta^i + 1 = \Theta^i + \Theta^{P-1} = \Theta^i (1 + \Theta^{P-i-1}). \qquad (4.19)$$

Найдем индексы элементов поля (4.19):

$$\mathrm{ind}(\Theta^i + 1) = \mathrm{ind}(\Theta^i (1 + \Theta^{P-i-1})). \qquad (4.20)$$

Учитывая свойства индексов ($\mathbf{ind(a \cdot b) = ind\ a + ind\ b}$ [1]), (4.20) можно представить в виде:

$$\mathrm{ind}(\Theta^i + 1) = \mathrm{ind}\Theta^i + \mathrm{ind}(1 + \Theta^{P-i-1}). \qquad (4.21)$$

Так как основание индекса (логарифма) Θ_l, то $\mathrm{ind}\,\Theta^i (\mathrm{mod}\,(P-1)) = \log_\Theta \Theta^i (\mathrm{mod}\,(P-1)) = i$ и соотношение (4.21) имеет вид:

$$\mathrm{ind}(\Theta^i + 1)(\mathrm{mod}\,(P-1)) = u_i = i + \mathrm{ind}(1 + \Theta^{P-i-1}) \mathrm{mod}(P-1).$$

Символы ХДС (характеры элементов поля) могут быть найдены из (4.17) и (4.21):

$$\begin{aligned} W_i &= \exp(j\pi u_i) = \exp(j\pi(i + \mathrm{ind}(1 + \Theta^{P-i-1})) \mathrm{mod}(P-1) = \\ &= \exp j\pi i\,(\mathrm{mod}(P-1)) \exp j\pi(1 + \Theta^{P-i-1})) \mathrm{mod}(P-1). \end{aligned} \qquad (4.22)$$

Анализ (4.22) показывает, что при i четном (i=2k) характер индексов не изменяется. Действительно в этом случае:

$$W_i = \exp(j\pi\, \mathrm{ind}(1 + \Theta^{P-i-1})), \qquad (4.23)$$

т.е. символы совпадают по знаку.

При i нечетном (i=2k+1):

$$W_i = -\exp(\mathrm{ind}(1 + \Theta^{P-i-1})) \mathrm{mod}\,(P-1). \qquad (4.24)$$

В этом случае символы W_i и W_{P-i-1} противоположны по знаку. Приведеное выше подтверждает справедливость (4.18).

Утверждение доказано.

Проиллюстрируем справедливость утверждения 4.2 на примере.

Пусть характеристика поля GF(P) P =13, а первообразный элемент поля $\Theta = 2$. Изоморфизм ХДС в данном поле $W = \{-11-111-1111-1-1-1\}$.

Установим зависимость характеров (символов ХДС) в поле GF(13). При $i = 1$ $W_2 = -W_2$, $i = 2$ $W_{11} = W_3$, $i = 3$ $W_{10} = -W_4$, $i = 4$ $W_9 = W_5$, $i = 5$ $W_8 = -W_6$. Результат будет таким же, если для установления зависимости символов НС применить (4.18).

Использование утверждения 4.2 позволяет определить (P-1)/2 + i символы ХДС ($i = \overline{1,(P-1)/2}$) по известным первым (P-1)/2- i символам. В этом случае не определены лишь первый и ((P-1)/2+ i)-й символы ХДС, но ((P-1)/2 + i)-й символ ХДС определяется правилом кодирования (2.22). Действительно, известно, что элемент поля $\Theta^{(P-1)/2} = L$, тогда $\Theta^{(P-1)/2} + 1 = L + 1 (\mathrm{mod}\, P) \equiv 0 (\mathrm{mod}\, P)$. В соответствии с правилом кодирования (2.22), если $\Theta^i + 1 \equiv 0 (\mathrm{mod}\, P)$, то символ сигнала равен 1. Для ХДС число символов К, принимающих значение «1», равно K=L/2. Это означает, что первый символ ХДС может быть доопределен, если известны P - 2 символов сигнала.

Нетрудно убедиться в том, что утверждения 4.1 – 4.2 справедливы и для расширенного поля Галуа, т.е. для случая, когда n >1.

Выявленные и описанные в утверждениях 4.1 – 4.2 связи элементов и характеров элементов поля позволяют в два раза повысить быстродействие устройств формирования ХДС. Достигается указанное формированием, согласно правилу (4.14), лишь половины символов сигнала, остальные символы могут быть получены путем реализации правила (4.15).

4.3 Корреляционные свойства нелинейных дискретных сигналов в конечных полях Галуа

При использовании в качестве множественного доступа кодового разделения абонентов требуемое для информационного обмена число сигналов равно произведению числа абонентов на число сигналов в алфавите (при этом полагают, что все абоненты используют алфавиты одного объёма). Минимальное число сигналов равно числу абонентов. Если число абонентов в системе велико, то выбор сигналов является главным вопросом при разработке ТКС.

Сигналы, входящие в систему, должны обеспечивать минимально возможный уровень взаимных помех, который, в основном, определяется допустимым уровнем максимальных боковых лепестков взаимнокорреляционной функции.

В настоящее время не существует алгоритмов (правил построения) больших систем фазоманипулированных (ФМ) сигналов, у которых пик-фактор достигал бы значений нескольких единиц. Например, если $B = 10^4$, то может оказаться необходимой система с $N = 10^8 \ldots 10^{12}$ и $\alpha = 2,\ldots,5$ [51]. Но такие сигналы пока неизвестны, хотя факт их существования не отрицается. Таким образом, в настоящее время существует следующая нерешённая проблема – разработка методов построения больших систем ФМ ШПС с хорошими корреляционными свойствами. Алгоритмы построения систем ФМ сигналов должны быть детерминированными, поскольку сигналы должны быть известными в точке приёма.

Применение сложных сигналов позволяет повысить защищённость ТКС при воздействии структурных и некоторых других типов помех в пределах полосы частот, занимаемой сигналом. В связи с этим важной задачей является выбор сигналов, обеспечивающих минимально возможный уровень взаимных помех, который в основном определяется допустимым уровнем максимальных пиков взаимно корреляционных функций (ВКФ). Для режима обнаружения важно иметь систему, составленную из сигналов, обладающих малыми пиками периодических и апериодических автокорреляционных функций (ПФАК и АФАК).

В многоканальных системах связи в качестве манипулирующих (расширяющих спектр) широко используются М-последовательности (последовательности максимального периода) с числом элементов $N = 2^m - 1$, или немаксимального периода с трехуровневой функцией корреляции (последовательности Голда), генерируемые m - каскадным или $2m$-каскадным двоичным регистрами сдвига с линейной обратной связью. Объём системы, составленной из М-последовательностей составляет $M = \phi(N)/m$ ($\phi(N)$ - функция Эйлера).

Известно [140], что объем системы, составленной из М-последовательностей, ограничен. Например, количество различных сигналов (изоморфизмов), которые можно синтезировать с использованием линейного регистра при $m = 10$, составляет $M = 60$. Максимальные значения модуля боковых выбросов функции взаимной корреляции таких систем больше, чем у ряда других систем сигналов [51]. Использование в многоканальных системах связи последовательностей Голда позволяет увеличить объём системы, однако такие системы обладают значительным частотным пик-фактором и относительно большим уровнем боковых лепестков ПФАК и АФАК. Названные линейные последовательности существуют только для значений длительностей $N = 2^m - 1$. При усечении числа символов последовательностей их авто - и взаимно корреляционные свойства значительно ухудшаются [51]. Кроме того, линейные последовательности обладают низкой кодовой устойчивостью [142,55,71], причём закон формирования на периоде $N = 2^m - 1$ определяется по любым $2m$ для М-последовательностей и $4m$ для последовательностей Голда подряд следующим символам. По этим причинам применение линейных сигналов в многоканальных системах связи ограничено.

Среди множества классов сложных сигналов в широкополосных системах (частотно-модулированные, многочастотные, дискретные частотные, частотно-манипулированные и др.) важное место занимают периодические дискретные сигналы, получаемые манипуляцией начальных фаз радиоимпульсов по закону некоторой дискретной последовательности (ДП) периода N (фазоманипулированные сигналы).

Процесс выбора рациональных по тем или иным критериям структур сложных сигналов тождественен синтезу соответствующих манипулирующих ДП.

Применение широкополосных сигналов (ШПС) позволяет повысить помехоустойчивость телекоммуникационных систем (ТКС) при воздействии структурных (взаимных) и организованных помех. Реальная помехоустойчивость будет ниже потенциальной. Причинами снижения помехоустойчивости при вхождении в синхронизм и при различении сигналов является наличие боковых пиков корреляционных функций (КФ).

В качестве критерия выбора класса ДКС как правило, ориентируются на критерий минимума взаимных помех (минимаксный критерий). Такой критерий подразумевает построение ансамблей сигналов объема М, манипулированных ДП, как можно заметнее отличающихся друг от друга при возможных циклических сдвигах.

Количественной мерой отличия манипулирующих ДП служат максимальные по ансамблям уровни бокового лепестка периодической функции автокорреляции (ПАКФ) и уровня бокового лепестка периодической функции взаимной корреляции (ПВКФ), определяемые как [15]:

$$p_p(m) = \frac{1}{\|a^2\|}\sum_{i=0}^{n-1} a_i \cdot a^*_{i-m}, \quad \rho_p, k_l(m) = \frac{1}{\|a_k\|\|a_l\|}\cdot\sum_{i=0}^{N-1} a_{k,i}\cdot a^*_{l,i-m}, \qquad (4.25)$$

где a_k, a_l – комплексная амплитуда $k(l)$ -й дискретной последовательности.

Исходя из этого, применяемые в ТКС широкополосные сигналы (ШПС) должны обладать такими корреляционными свойствами, когда боковые пики корреляционных функций ШПС являются как можно меньшим, т.е. в идеальном случае должны стремиться к нулю. Однако требование идеальности (нулевые значения боковых пиков) авто и взаимнокорреляционных функций между всеми циклическими сдвигами К последовательностей и различными изоморфизмами системы сигналов с периодом N не выполнимо, поскольку значения боковых пиков не может опуститься ниже $1/2\sqrt{B}$ [51].

Указанное объясняется следующим. Оптимальный прием сигналов осуществляется с помощью согласованного фильтра (СФ) или коррелятора. Нормированный отклик СФ определяется с помощью интеграла свертки [51]

$$R_{ij} = 1/E \int U_j(t)\, U_k(t - \tau)dt \qquad (4.26)$$

где $U_j(t)$ – сигнал на входе фильтра, согласованного с сигналом $U_k(t)$.

В зависимости от того, согласован или не согласован сигнал с фильтром, имеется ли дополнительное доплеровское смещение частоты сигнала, корреляционная функция имеет различные представления. Одним из таких представлений является взаимная функция неопределенности (ВФН) $R_{jk}(\tau,\Omega)$ сигналов с номерами j и k. ВФН выражается через комплексные огибающие сигналов и через их спектры следующим образом

$$R_{jk}(\tau,\Omega) = 1/2E \int_{-\infty}^{\infty} U_j(t)\, U^*_k(t - \tau)\, e^{i\Omega t}dt = 1/4E \int_{-\infty}^{\infty} G_j(\omega - \Omega)\, G^*_k(\omega)\, e^{i\omega t}d\omega \quad (4.27)$$

где τ – сдвиг по времени между сигналами; Ω - доплеровский сдвиг частоты.

Отклик согласованного фильтра связан с ВФН соотношением

$$r_{jk}(\tau,\Omega) = \mathrm{Re}\, R_{jk}(\tau,\Omega)\, \exp(i\omega_0\tau). \qquad (4.28)$$

Объем взаимной функции неопределенности (ВФН) $R_{jk}(\tau,\Omega)$ сигналов j и k (объем, заключенный между поверхностью, описываемой квадратом модуля ВФН, и плоскостью неопределенности), равен единице, т.е.

$$1/2\pi \int\int_{-\infty}^{\infty} \left| R_{jk}(\tau,\Omega)\right|^2 d\tau\, d\Omega = 1 \qquad (4.29)$$

и не зависит от номеров и формы сигналов. Другими словами получить тело неопределенности с нулевыми боковыми лепестками невозможно. Тело неопределенности при условии, что все боковые пики равны и равномерно распределены в квадрате (2T,2F) (в этом случае боковые пики минимальны по амплитуде) изображено на рисунке 4.1. Узкий основной пик стоит на основании высотой $R_0 = ½\sqrt{B}$ (B - база сигнала).

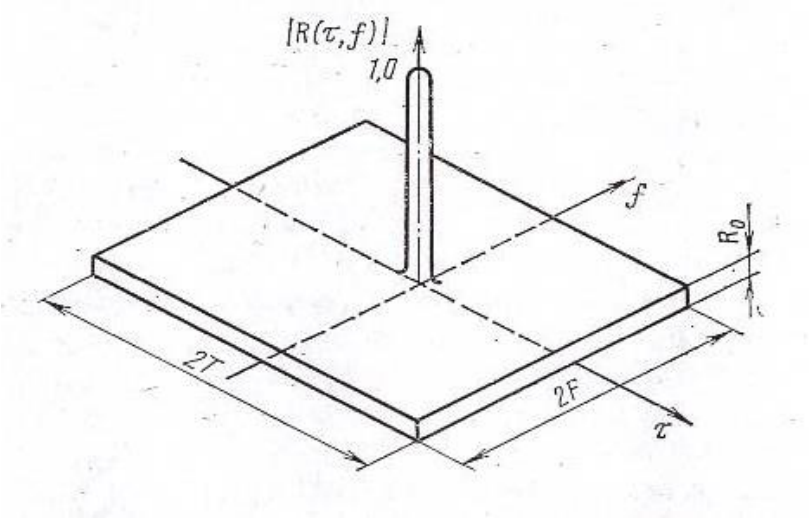


Рис.4.1 Тело неопределенности

Наличие в N - мерном линейном пространстве не более N ортогональных векторов (сигналов) делает гипотетическим идеальный с точки зрения минимаксного критерия ансамбль дискретных последовательностей с нулевыми боковыми лепестками функции авто - и взаимной корреляции, и ограничивает потенциал снижения корреляционного выброса R при фиксированных N и числе абонентов K.

В Разделе 3 приведены границы для среднеквадратичных и максимальных (пиковых) значений авто - и взаимно-корреляционных функций (выражение 3.14). В [144] указаны принципиально достижимые значения максимальных боковых пиков периодической функции автокорреляции (границы плотной упаковки) для заданного периода последовательности:

$$R^{a}_{max} \geq \begin{cases} 0, \text{ если } N \equiv 0 (\text{mod } 4); \\ 0, \text{ если } N \equiv 1 (\text{mod } 4); \\ 0, \text{ если } N \equiv 2 (\text{mod } 4); \\ 0, \text{ если } N \equiv 3 (\text{mod } 4), \end{cases} \qquad (4.30)$$

Приведенные границы устанавливают критерий синтеза множества ДП (сигнатур). Ансамбли, со значениями R_{max} достигающие предела, предсказываемого границами (3.14) и (4.30), являются оптимальными по критерию корреляционного пика, и называются минимаксными. К числу таких ансамблей можно отнести

криптографические дискретные сигналы, метод синтеза которых приведен в разделе 3.

Для идеального гипотетического ансамбля R_{max} равно нулю, а для любого реального ансамбля максимальное значение корреляционной функции может служить адекватной мерой его близости к идеальному.

К настоящему времени нет единой теории синтеза ДП с «плотно упакованной» по ПАКФ для произвольных длин последовательностей. В то же время, для решения задач как цикловой синхронизации, так и обеспечения требуемой помехоустойчивости, скрытности функционирования системы передачи информации, необходимо использовать дискретные сигналы с произвольными значениями длительностей последовательностей и минимальными значениями боковых лепестков ПФАК.

Синтез семейств сигналов с необходимыми авто и взаимно корреляционными свойствами заключается в отыскании семейства дискретных последовательностей, обладающего соответствующими авто и взаимно корреляционными функциями. Искусство проектирования широкополосных систем во многих аспектах базируется на нахождении сигналов с соответствующими корреляционными свойствами.

Рассмотрим кодовую последовательность $(a_0, a_1, \ldots, a_{N-1})$. Если она используется для формирования импульсного сигнала S, комплексная огибающая которого имеет вид: $S(t) = \sum_{i=-\infty}^{\infty} a_i * S_0(t - i\Delta)$, апериодическая или импульсная автокорреляционная функция (АКФ) вычисляется как [15]

$$Ra(m) = \left\{ \begin{array}{l} \frac{1}{\left\| a^2 \right\|} \sum_{i=m}^{N-1} a_i * a_{i-m}^*, m \geq 0 \\ \frac{1}{\left\| a^2 \right\|} \sum_{i=0}^{N-1+m} a_i * a_{i-m}^*, m \leq 0 \end{array} \right\}, \qquad (4.31)$$

где, $\|a\|$ - длина (эвклидова норма) кодового вектора $a = \{a_0, a_1, \ldots, a_{n-1}\}$, или $\left\| a^2 \right\| = \sum_{i=0}^{N} |a_i|^2$ энергия N – элементарной последовательности $\{a_0, a_1, \ldots, a_{n-1}\}$;

m – число тактов сдвига кодовой последовательности относительно копии;

* - знак комплексного сопряжения.

В разделе 3 было отмечено, что последовательности с хорошей апериодической АКФ могут быть найдены среди последовательностей с хорошей периодической АКФ. С учетом указанного вызывает интерес определение потенциала минимизации максимального бокового лепестка ПАКФ бинарных кодов.

Очевидно, что в отсутствии бинарных кодов с идеальной ПАКФ следующими по привлекательности являются бинарные последовательности, для которых $R_p(m)$ принимает значения ± 1, при $m = 1,2,\ldots,N-1$, т.е. обладают $R_{p,max} = 1/N$ могут иметь только два возможных значения ненормированных ПАКФ, либо:

$$R_p(m) = \begin{Bmatrix} N, m = 0 \bmod N \\ +1, m \neq 0 \bmod N \end{Bmatrix}, \qquad (4.32)$$

при длине $N = 4h+1$, либо

$$R_p(m) = \begin{Bmatrix} N, m = 0, \bmod N \\ -1, m \neq 0, \bmod N \end{Bmatrix}, \qquad (4.33)$$

при длине $N = 4h-1$.

Последовательности, удовлетворяющие соотношениям (4.32) - (4.33) и, следовательно, обладающие теоретически минимальным уровнем боковых лепестков ПАКФ ($R_{p,max} = 1/N$) для бинарных кодов нечетной длины, называются минимаксными. Известны только два примера ($N = 5$ и $N = 13$) последовательностей, подчиняющихся соотношению (4.32), тогда как существуют регулярные правила формирования минимаксных последовательностей, удовлетворяющих (4.33). К указанным типам последовательностей относят m-последовательности или последовательности максимальной длины, последовательности Лежандра.

Возможные приложения нелинейных сигналов в конечных полях, обладающих хорошими автокорреляционными свойствами будут рассмотрены в разделе 6.

В многопользовательских системах с кодовым разделением необходимы системы дискретных сигналов с особенными взаимными корреляционными свойствами. Синтез семейств с необходимыми взаимно корреляционными свойствами

заключается в отыскивании семейства последовательностей, обладающего соответствующими взаимно корреляционными функциями (ВКФ).

При рассмотрении ВКФ двух последовательностей (k и l) одинаковой длины можно выделить апериодическую ВКФ $R_{a},k_{l}(m)$ и периодическую $R_{p},k_{l}(m)$, определяемые соответственно как [15]:

$$R_{a},k_{l}(m)=\begin{cases}\dfrac{1}{\|a_{k}\|\|a_{l}\|}\cdot\sum\limits_{i=m}^{N-1}a_{k,i}\cdot a_{l,i-m}^{*},\ m\geq 0,\\ \dfrac{1}{\|a_{k}\|\|a_{l}\|}\cdot\sum\limits_{i=0}^{N+m-1}a_{k,i}\cdot a_{l,i-m}^{*},\ m<0,\end{cases} \tag{4.34}$$

$$R_{p},k_{l}(m)=\frac{1}{\|a_{k}\|\|a_{l}\|}\cdot\sum_{i=0}^{N-1}a_{k,i}\cdot a_{l,i-m}^{*}\ . \tag{4.35}$$

где: R – коэффициент корреляции последовательностей k и l, характеризует близость или подобие последовательностей.

При кодовом разделении в системах связи имеют место взаимные помехи, которые являются следствием одновременной работы абонентов в общей полосе частот. Параметры сигналов при кодовом разделении следует выбрать так, чтобы уровень взаимных помех был сколь угодно малым. В этом случае, как следует из (1.39 – 1.42) может быть обеспечена заданная помехоустойчивость.

Актуальной задачей является выбор систем сигналов, свободных от указанных недостатков.

К числу привлекательных с точки зрения корреляционных функций относятся характеристические коды с числом позиций $N=4x+2$ и $N=4x, x=1,2$,…[144]. Построение данных кодов базируется на использовании характера мультипликативной группы ($\Psi(x)$) поля $GF\left(P^{n}\right), n\geq 1$. Теоретические основы синтеза данного класса сигналов представлены в разделе 2.

Для размерности кода $N=4x+2$ максимальные боковые лепестки ПАКФ принимают значение $\{-2,2\}$. В случае применения характеристических кодов с числом позиций $N=4x$ боковые лепестки ПАКФ $R_{a,max}$ принимают значения

$\{0,-4\}$. Объём системы характеристических сигналов определяется из соотношения [144]: $M=\phi(N)/n$, (n - степень расширения поля $GF(P^n), n \geq 1$).

Естественно полагать, что данный класс кодов, обладая хорошими корреляционными свойствами в части ПАКФ, будет иметь и малые значения боковых лепестков АФАК. Как было показано выше, любой циклический сдвиг последовательности $a_0, a_1, \ldots a_{N-1}$ длины N обладает такой же периодической АКФ, что и исходная последовательность, поскольку периодическая АКФ – инвариантна к циклическому сдвигу.

Факт отличия АФАК циклически сдвинутой копии от АФАК первоначальной последовательности вместе с границей (4.34) составляет основу метода поиска характеристических последовательностей с приемлемой АФАК. Суть метода состоит в следующем. Из множества значений длин, для которых существуют характеристические коды, выбираются последовательности с требуемыми периодом и значениями боковых лепестков функции корреляции (- 4, 0, либо +2, - 2). Затем осуществляется поиск по критерию наименьшего уровня максимума АФАК среди всех одноперiодных сегментов последовательностей кандидатов (изоморфизмов характеристического кода). В частности, берется одноперiодный сегмент первой последовательности кандидата, вычисляется его апериодическая АКФ и запоминается в памяти уровень максимального бокового лепестка наряду с номерами последовательности кандидата (типа) и его сдвига. Затем осуществляется циклический сдвиг сегмента на одну позицию, и производятся необходимые вычисления. Если новое значение максимума апериодического токового лепестка окажется ниже предыдущего, то его значение и номер нового сдвига заменяют ранее записанные в памяти данные, в противном случае зарегистрированные значения сохраняются без изменения. Данная процедура повторяется N раз, т.е. для всех циклических сдвигов первой последовательности кандидата (для всех автоморфизмов исходного изоморфизма). Подобному исследованию подвергается следующая последовательность кандидат (изоморфизм выбранного кода). Результатом

поиска является последовательность с минимальным значением $R_{a,max}$ среди всего ансамбля последовательностей.

В таблице 4.6 представлены значения боковых лепестков АФАК для всех циклических сдвигов одного из изоморфизмов характеристического кода с периодом $N=130$.

В таблице 4.7 приведены результаты поиска циклических сдвигов характеристических последовательностей с периодом $N=130$ и $N=256$, при которых боковые лепестки АФАК имеют наименьшие значения.

Таблица 4.6

Значения боковых лепестков АФАК для нелинейных сигналов с периодом $N=130$

Максимальный боковой лепесток	Соответствующие сдвиги
17	{76, 82}
18	{38, 56, 89, 102}
19	{3, 13, 50, 129}
20	{8, 19, 22, 40, 42, 43, 90, 108}
21	{2, 10, 30, 31, 36, 57, 68, 87, 96, 116, 119, 125}

Таблица 4.7

Значения наименьших боковых лепестков АФАК

N	Максимальные боковые лепестки	Соответствующие сдвиги
130	17	$\{76, 82\}$
256	27	$\{41, 114\}$

Как следует из данных таблиц 4.6 и 4.7, минимальное значение боковых лепестков АФАК для периода $N = 130$ (при $m = 76, 82$) составляет 17, а при $N = 256$ и $m = 41, 114$ — равно 27.

Данный метод может быть использован для формирования ансамбля сигналов для различных приложений широкополосных систем. На первом этапе для заданной длины N некоторым образом формируется множество последовательностей с хорошей ПФАК. Полученное может включать все известные последовательности заданной длины N, уровень боковых лепестков ПФАК которых согласно (4.35) позволяет надеяться на получение низкого значения $R_{a,max}$. В такое множество, в качестве кандидатов, могут войти, как свидетельствуют представленные результаты, и нелинейные сигналы, синтез которых основан на использовании свойств элементов конечного поля. Затем, для каждой последовательности - кандидата, путем циклической перестановки его символов, находят оптимальные по минимаксному критерию апериодические коды и отбирают из них наилучшие.

Известно [2], что оценка качества обнаружения и различения выполняется с использованием следующих статистических характеристик ФАК и ФВК: математическое ожидание выбросов (m_R); математическое ожидание максимальных боковых выбросов ($m_{R_{макс}}$); математическое ожидание модулей максимальных боковых выбросов ($m_{|R_{макс}|}$); среднеквадратичное отклонение боковых выбросов ($D_R^{1/2}$); среднеквадратичное отклонение модулей боковых выбросов ($D_{|R|}^{1/2}$), значение максимального бокового выброса $R_{макс}$, а также количество максимальных боковых пиков функции корреляции.

С использованием разработанного специального программного обеспечения, были выполнены исследования корреляционных свойств сложных нелинейных дискретных сигналов в конечных полях Галуа. Указанное программное обеспечение позволяет расчитывать статистических характеристики корреляционных функций, определять минимальные и максимальные значения (и их количество)

боковых пиков функций корреляции. Пакет программ, примеры, реализующие оценки корреляционных свойств нелинейных дискретных сигналов в конечных полях Галуа приведены в Приложении А.

На рисунке 4.1 в качестве примера приведен вид ПФАК ХДС длительностью N = 256 символов. С ростом периода последовательности ПФАК таких сигналов приближается к идеальной, когда боковые выбросы по сравнению с основным становятся пренебрежимо малыми.

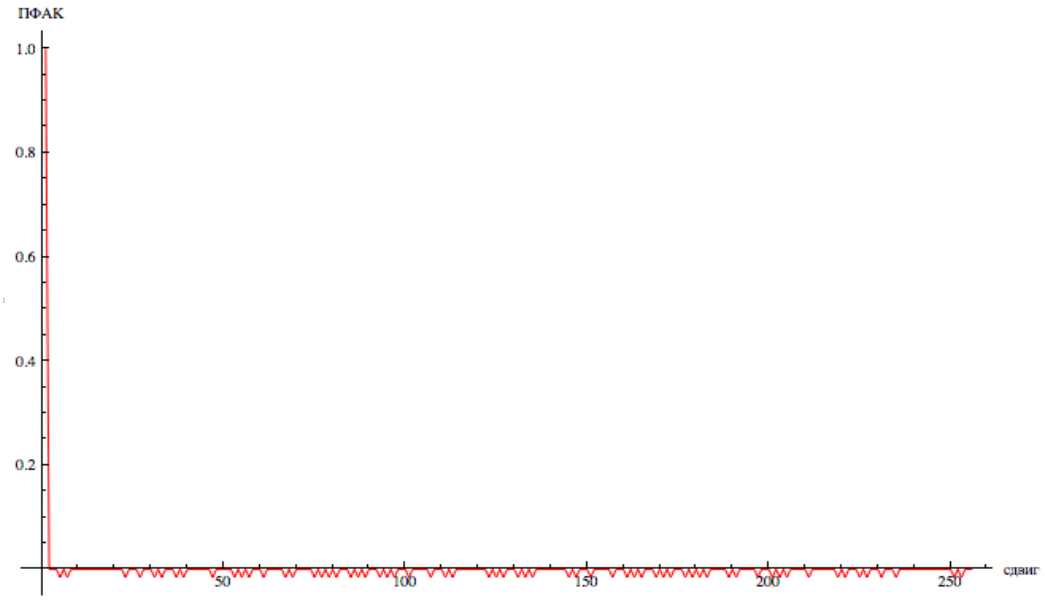


Рисунок 4.1 - ПФАК ХДС при N = 256

Нормированная апериодическая функция автокорреляции ХДС длительностью N будет иметь наибольшие боковые выбросы, равные примерно $1/\sqrt{N}$. На рисунке 4.2 в качестве примера приведен вид АФАК ХДС длительностью N = 256 символов. Значения ненормированного максимального бокового выброса, равное $\sqrt{N}$, вытекает из псевдослучайного характера последовательности, в которой содержится одинаковое число элементов +1 и – 1. Так как боковой выброс автокорреляционной функции является суммой произведений разнополярных элементов (1 и – 1), то математическое ожидание бокового выброса за время длительности последовательности рано нулю, а дисперсия равна $\sqrt{N}$.

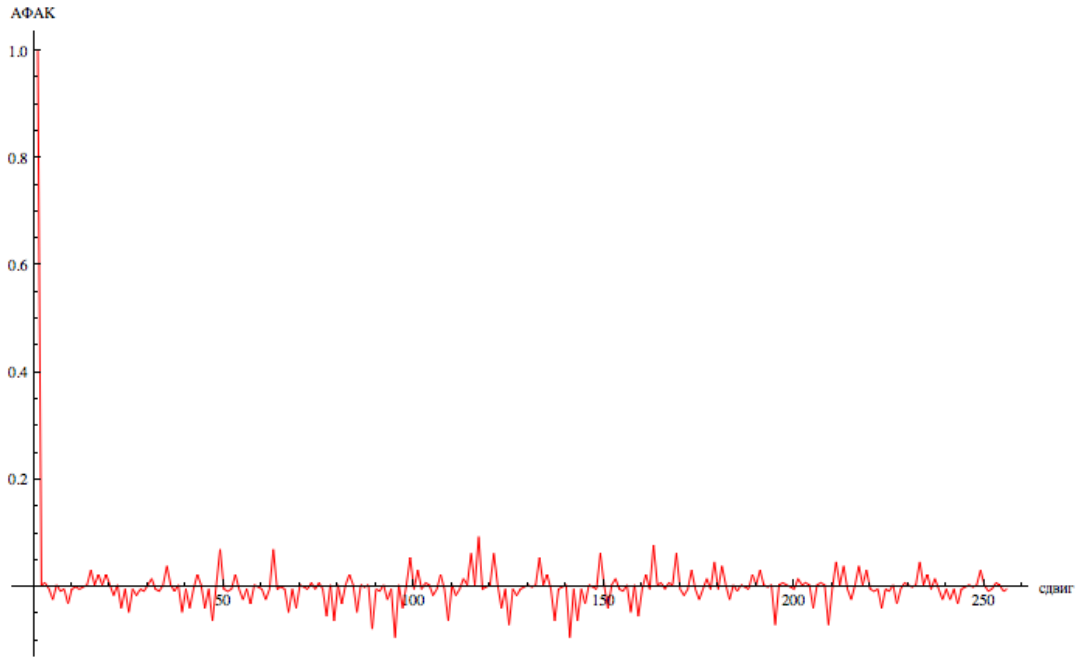


Рисунок 4.2 - АФАК ХДС при N = 256

В таблице 4.8 приведены результаты расчета некоторых из большого числа рассчитанных на ЭВМ АФАК и ПФАК ХДС различной длительности.

После статистической обработки многочисленных результатов расчета АФАК ХДС сделан ряд выводов:

- величина наибольших боковых выбросов при различных длительностях N может принимать значения $R_{бmax}$ = (1,1-1,8) $\sqrt{N}$;

- математическое ожидание модуля выбросов оценивается как m($|R_{бmax}|$) = 0,28 $\sqrt{N}$;

- среднеквадратичное отклонение модуля выбросов D ($|R_{бmax}|$) = 0,32 $\sqrt{N}$;

- математическое ожидание выбросов равно нулю;

- среднеквадратичное отклонение выбросов D ($R_{бmax}$) = 0,43 $\sqrt{N}$.

По виду функции взаимной корреляции (ФВК) можно судить о степени ортогональности сигналов. ХДС, так же как и m – последовательности, не являются ортогональными сигналами, поэтому можно говорить лишь о квазиортогональности при длительностях последовательностей, при которых уже обеспечивается необходимое отношение боковых выбросов ФВК к основному выбросу ФАК. Именно этим отношением характеризуется степень ортогональности анализируемых сигналов. Разработчиков и пользователей информационных систем интере-

суют различные ФВК: периодические ФВК (ПФВК), апериодические, (АФВК), меандро инвертированные функции авто – и взаимной корреляции (МИФАК и МИФВК) [140].

На рис. 4.3 в качестве примера приведен вид АФВК для ХДС периода L = 256, полученных путем децимации последовательности по коэффициентам децимации k = 1 и k = 7.

Таблица 4.8

Результаты расчета некоторых АФАК и ПФАК ХДС различной длительности

Число элементов в сигнале	Характеристика	$\frac{R_{бmax}}{\sqrt{N}}$	$N_{бmax}$	$\frac{m(R_{бmax})}{\sqrt{N}}$	$\frac{m(\lvert R_{бmax}\rvert)}{\sqrt{N}}$	$\frac{D^{1/2}_{(R_б)}}{\sqrt{N}}$	$\frac{D^{1/2}_{(\lvert R_б\rvert)}}{\sqrt{N}}$
66	АФАК	1,2	2	-0,06	0,31	0,44	0,32
	ПФАК	0,2	65	-0,12	0,25	0,21	0,00
	АФВК	2,0	1	-0,00	0,54	0,71	0,45
	ПФВК	2,6	2	-0,01	0,81	1,02	0,61
126	АФАК	1,4	1	-0,04	0,31	0,43	0,30
	ПФАК	0,2	125	-0,09	0,18	0,15	0,00
	АФВК	2,3	1	-0,00	0,54	0,71	0,46
	ПФВК	2,9	2	-0,00	0,80	1,01	0,60
256	АФАК	1,5	3	-0,03	0,26	0,42	0,33
	ПФАК	0,3	64	-0,06	0,06	0,11	0,11
	АФВК	2,6	1	-0,00	0,54	0,71	0,47
	ПФВК	3,1	3	-0,00	0,79	1,00	0,61
522	АФАК	1,6	2	-0,02	0,25	0,41	0,33
	ПФАК	0,1	521	-0,04	0,09	0,08	0,00
	АФВК	2,8	1	-0,00	0,53	0,71	0,47
	ПФВК	3,2	2	-0,00	0,80	1,00	0,60
1018	АФАК	1,8	1	-0,02	0,25	0,41	0,32
	ПФАК	0,1	1017	-0,03	0,06	0,05	0,00
	АФВК	2,9	1	0,00	0,53	0,71	0,47
	ПФВК	3,3	2	0,00	0,80	1,00	0,60
2052	АФАК	1,8	1	-0,01	0,23	0,40	0,32
	ПФАК	0,1	513	-0,02	0,02	0,04	0,04
	АФВК	3,2	1	0,00	0,53	0,71	0,47
	ПФВК	3,6	2	-0,00	0,80	1,00	0,60

Расчеты АФВК проводились для N = 30, 66, 126, 256, 522, 1018, 2052. Результаты расчетов АФВК ХДС для указанных периодов последовательностей приведены в таблице 4.8. Статистическая обработка результатов расчета показала следующее:

- значения максимальных боковых выбросов $R_{бmax}$ находятся в пределах (1,9-3,2) $\sqrt{N}$;

- количество наибольших выбросов $R_{бmax}$ редко бывает больше одного;

- математическое ожидание модуля выбросов оценивается как $m(|R_{бmax}|) = 0{,}54\sqrt{N}$;

- среднеквадратичное отклонение модуля выбросов $D(|R_{бmax}|) = 0{,}47\sqrt{N}$;

- математическое ожидание выбросов равно нулю;

- среднеквадратичное значение $D(R_{бmax}) = 0{,}72\sqrt{N}$.

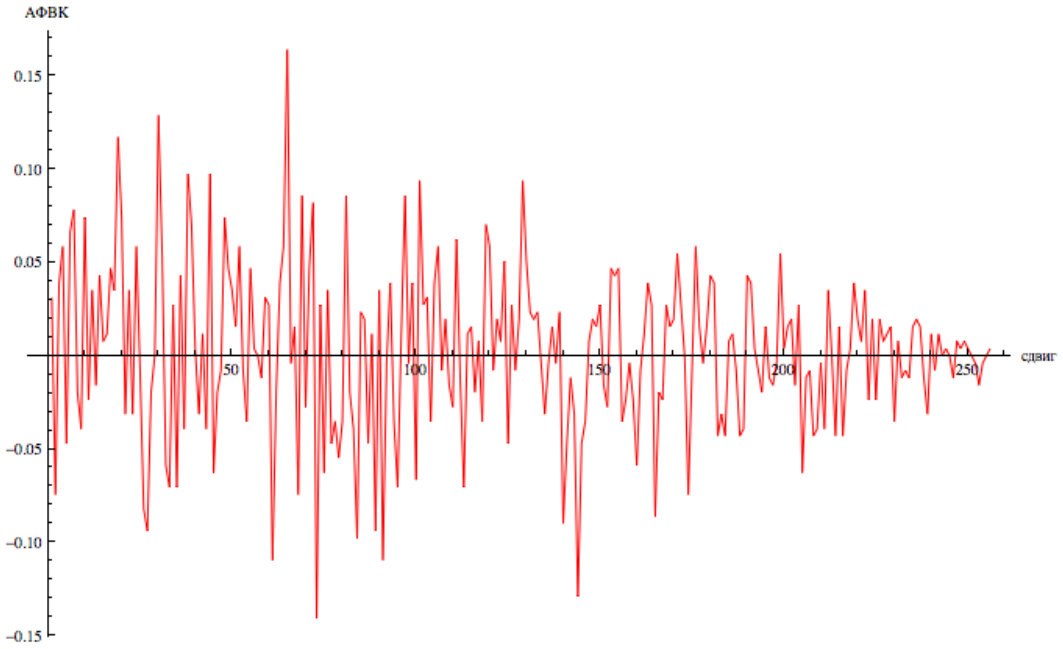


Рисунок 4.3 - АФВК для ХДС при N = 256

Были проведены исследования ПФВК ХДС (таблица 4.8). На рисунке 4.4 приведен типичный вид ПФВК ХДС с периодом N = 256. Обобщение результатов расчетов ПФВК показало:

- значения наибольших боковых выбросов $R_{бmax}$ находятся в пределах (2,5-3,6) $\sqrt{N}$;

- количество наибольших выбросов ПФВК $R_{бmax}$ может быть большим, но при этом не превышает $2\sqrt{N}$;

- математическое ожидание модуля выбросов оценивается как $m(|R_{бmax}|) = 0{,}81\sqrt{N}$;

- среднеквадратичное отклонение модуля выбросов $D(|R_{бmax}|) = 0{,}61\sqrt{N}$;

- математическое ожидание выбросов равно нулю;

- среднеквадратичное значение $D(R_{бmax}) = 1{,}01\sqrt{N}$.

В таблице 4.9 приведены обобщенные статистические характеристики различных корреляционных функций наиболее широко применяемых дискретных последовательностей. Анализ данных таблицы показывает, в частности, что статистические характеристики ХДС близки к аналогичным характеристикам m-последовательностей.

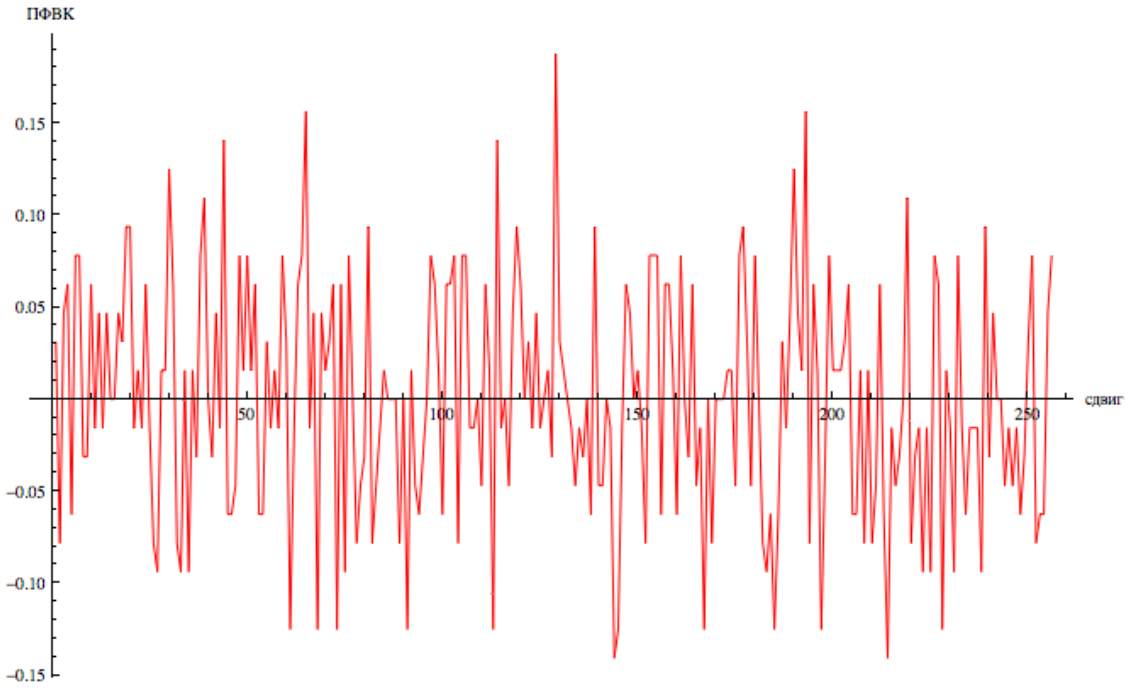


Рисунок 4.4 - ПФВК ХДС при N = 256

Характеристические последовательности, в отличие от другого класса последовательностей, - m-последовательностей, не могут быть отнесены к так называемым трехуровневым последовательностям (последовательности Голда [2]).

Последовательности Голда и последовательности Касами – по существующему предположению – наиболее протноупакованные по ПФВК, т.е. они обладают наилучшими среди других систем (с объёмом, приблизительно равным базе)

взаимокорреляционными свойствами [13,21]. В таблице 4.10 приведены значения максимальных боковых выбросов ПФАК (R_{amax}), ПФВК (R_{bmax}) для указанных систем в зависимости от значений длительности сигналов. Символ G означает, что сигнал выбран из системы (множества) Голда, символ K из множества Касами. Проведенные исследования ПФВК ХДС опровергли это предположение. В таблице 4.11 представлены значения R_{amax}, R_{bmax} для ХДС, рассчитанные с использованием ЭВМ для значений длительностей, близким к указанным в таблице 4.9. Здесь, Θ_1, Θ_2 - значения первообразных элементов конечного поля, по которым синтезированы пары ХДС.

Из анализа таблиц 4.10 – 4.11 следует, что существуют пары ХДС, для которых нормированные значения максимальных боковых выбросов ПФВК меньше максимальных боковых выбросов ПФВК последовательностей Голда и Касами. Например, для пары ХДС длительностью $N=1060$, построенных с использованием первообразных элементов $\Theta_1=2$, $\Theta_2=8$, максимальные значения боковых выбросов ПФВК не превышают $|R_{В.макс}|=64$, в то время как для последовательностей Голда длительностью $N=1023$ $|R_{В.макс}|=65$. Таким образом, даже при больших значениях длительностей ХДС обеспечиваются меньшие значения максимальных боковых пиков ПФВК чем у систем Голда и значение $|R_{В.макс}|=65$ нельзя считать, как полагали, достигнутой границей плотной упаковки. Далее, для ХДС длительностью $N=256$ максимальные значения боковых выбросов ПФВК не превышают $|R_{В.макс}|=32$, в то время как для последовательностей, выбранных из большого множества Касами, $|R_{В.макс}|=33$. Как показали исследования, пары ХДС длительностью $N=256$ имеют указанное значение $R_{В.макс}$. Кроме того, данные табл. 4.10 – 4.11 свидетельствуют о том, что максимальные боковые пики ПФАК ХДС значительно меньше максимальных боковых выбросов ПФАК систем Голда и Касами.

Таблица 4.9

Статистические характеристики различных корреляционных функций для некоторых классов сигналов

Характеристики	$\frac{m_R}{\sqrt{N}}$	$\frac{m_{\lvert R_{макс}\rvert}}{\sqrt{N}}$	$\frac{D^{1/2}_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D_R}{\sqrt{N}}$
Характеристические дискретные сигналы				
АФАК	1,1-1,8	0,28	0,32	0,43
ПФАК	0,1-1,9	0,15	0,02	0,14
АФВК	1,9-3,2	0,54	0,47	0,72
ПФВК	2,5-3,6	0,81	0,61	1,01
М-последовательности				
АФАК	0,7-1,25	0,32	0,26	0,41
ПФАК	$1/\sqrt{L}$	$1/\sqrt{L}$	0	0
Меандро-инвертированные ФАК	1,3-2,3	0,66	0,49	0,82
АФВК	1,4-5	0,54	0,48	0,73
ПФВК	1,9-6	0,80	0,62	1
Стыковые ФВК	2,0-5,1	0,83	0,62	1
Случайные последовательности				
АФАК	1,5-3,1	0,51	0,65	0,70
ПФАК	2-4	0,83	0,68	1
АФВК	2,4-4,3	0,54	0,48	0,70
ПФВК	2,75-4,5	0,82	0,62	1
Сегменты М-последовательностей				
АФАК	1,45-4,1	0,52	0,90	0,71
ПФАК	1,6-4,3	0,79	0,58	1
АФВК	1,4-4,3	0,52	0,49	0,72
ПФВК	1,6-5,0	0,80	0,60	1

Таблица 4.10

Максимальные боковые пики ПФАК ХДС

L	m	$R_{a\,max}$	$R_{b\,max}$
63 G	6	17	17
127 G	7	17	17
255 K	8	33	33
1023 G	10	65	65

Таблица 4.11

Максимальные боковые выбросы ПФАК систем Голда и Касами

L	Θ_1, Θ_2	$R_{a\,max}$	$R_{b\,max}$
66	2, 10	4	14
256	2, 27	4	32
1060	2, 90	4	64

Приведенные результаты исследований корреляционных свойств ХДС указывают на целесообразность применения нелинейных дискретных сигналов в конечных полях в многопользовательских телекоммуникационных системах и на возможность улучшения показателей эффективности (в частности, помехоустойчивости) таких систем. Оценки показателей эффективности систем при применении в них систем нелинейных дискретных сигналов в конечных полях приведены в разделе 6.

4.4 Корреляционные свойства нелинейных криптографических сложных дискретных сигналов

Для большинства приложений, в частности, для широкополосных систем с многостанционным доступом, интерес представляют не пары, а большие множества последовательностей с хорошими взаимно-корреляционными свойствами. В некоторых системах число одновременно используемых последовательностей

может превышать несколько сотен. Известны большие множества периодических последовательностей (множества Касами, Голда), обладающие корреляционными функциями со сравнительно небольшими значениями боковых пиков корреляционных функций. Среди фазоманипулированных сигналов особое место занимают М-последовательности, что обусловлено рядом замечательных свойств данного класса сигналов: простота устройств формирования, хорошие корреляционные и «шумоподобные» свойства, существование пар последовательностей, которые приводят к сигналам с улучшенными взаимно-корреляционными свойствами и др. При этом необходимо отметить, что М-последовательности порождаются двоичным полиномом степени m

$$h(x) = h_0 x^m + h_1 x^{m-1} + \ldots + h_{m-1} x + h_m$$

где $h_0 = h_m = 1$, а другие h_i принимают значения 0 или 1.

Такие последовательности получают с помощью m - каскадного сдвигового регистра с линейной цепью обратной связи, к которым подключены отводы от каскадов с номерами, для которых $h_i = 1$. Правило построения М-последовательностей обусловило одно из свойств данного класса сигналов (и других классов сигналов, в основе построения которых лежат линейные законы построения) – низкая структурная скрытность сигнала. Известно, что для определения правила построения М-последовательности (двоичного полинома степени n) необходимо знать сегмент из 2m подряд следующих символов. Например. Если степень полинома $m = 256$ (период такой последовательности $2^{256} - 1 = 1{,}16*10^{77}$), то для определения правила построения последовательности, полученной с использованием данного полинома, необходимо знать сегмент из 512 двоичных символов. Кроме того, объем системы данного класса сигналов ограничен и составляет величину $M = \phi(L/m)$, ($\phi(L)$ - функция Эйлера).

Вместе с тем для ряда приложений телекоммуникационных систем требуются сигналы, обладающие высокой структурной скрытностью, необходимыми корреляционными свойствам и значительным объемом системы сигналов.

В разделе 3 представлены теоретические основы синтеза нелинейных дискретных криптографических сигналов. Приведем результаты исследования свойств данного класса сигналов.

В качестве иллюстраций на рисунках 4.5 – 4.7 приведены различные функции корреляции криптографических сигналов (КС).

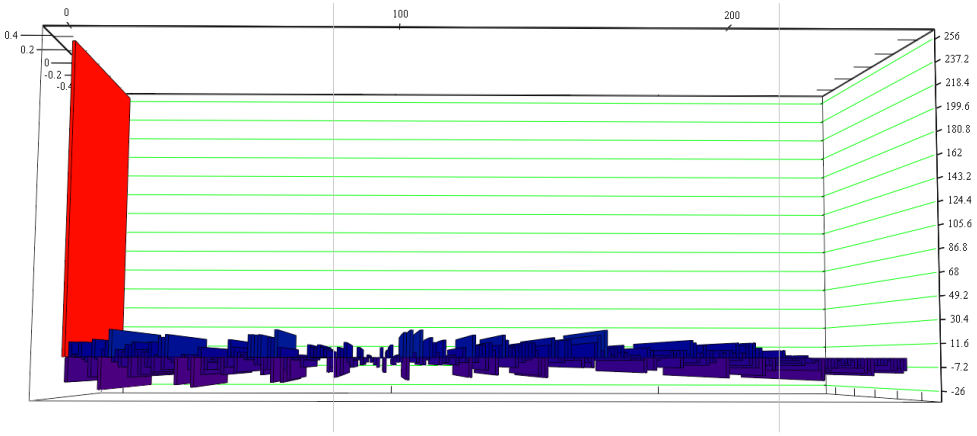


Рис. 4.5 - Вид АФАК для КС периода N = 256

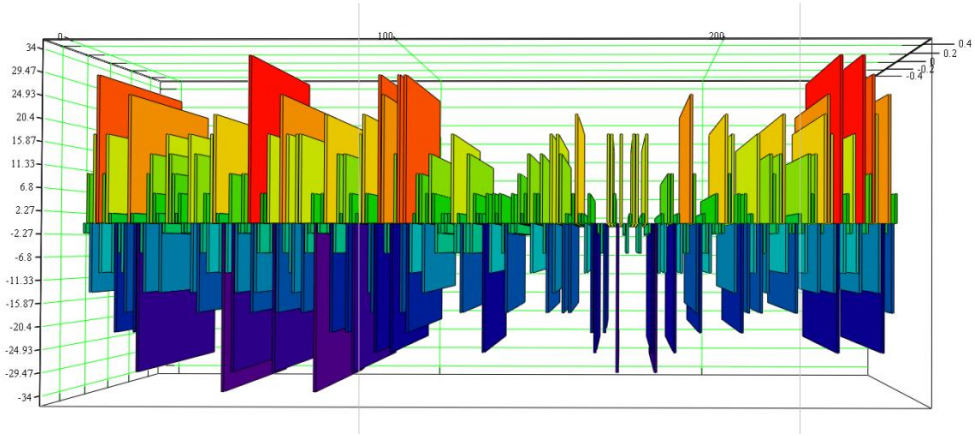


Рис. 4.6 - Вид ПФВК для КС периода N = 256

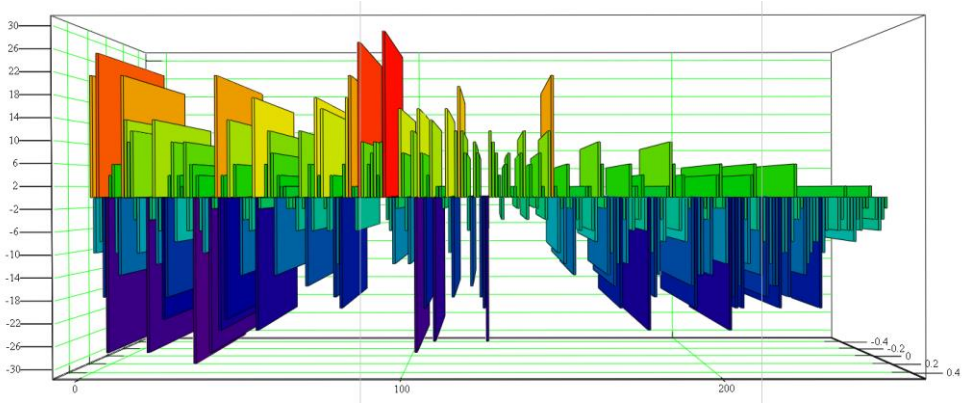


Рис. 4.7 - Вид АФВК для КС периода N = 256

Функционирование некоторых ТКС осуществляется в условиях воздействия мощных взаимных помех. При этом отношение сигнал/помеха на выходе согласованного фильтра зависит от значений боковых пиков функции взаимной корреляции. Из этого следует правило выбора сигналов, образующих систему: необходимо выбирать сигналы, у которых максимальные пики функции взаимной корреляции минимальны.

Таблица 4.12

Статистические характеристики корреляционных функций дискретных сигналов

Тип сигналов	Характеристики	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D_{\lvert R\rvert}^{1/2}}{\sqrt{N}}$	$\frac{D_{(R)}^{1/2}}{\sqrt{N}}$
ХДС	АФАК	1,0 - 1,8	0,5	0,4	0,5
	ПФАК	0,1 – 1,9	0,2	0,1	0,2
	МИФАК	1,4 - 2,6	0,6	0,5	0,8
	АФВК	1,9 - 3,2	1,0	0,8	1,0
	ПФВК	2,5 – 3,6	1,0	0,8	1,2
	СФВК	2.1 – 5,0	0,9	0,7	1,1
М - последовательности	АФАК	0,7...1,25	0,32	0,26	0,41
	ПФАК	$1/\sqrt{N}$	$1/\sqrt{N}$	0	0
	МИФАК	1,3...2,3	0,66	0,49	0,82
	АФВК	1,4...5,0	0,54	0,48	0,73
	ПФВК	1,9...6,0	0,8	0,62	1,0
	СФВК	2,0...5,1	0,83	0,62	1
Криптографические сигналы	АФАК	1,2 – 1,9	0,5	1	1,1
	ПФАК	0,2 - 1,9	0,6	0,4	0,7
	АФВК	1,4 – 3,4	0,5	0,4	0,6
	ПФВК	1,9 – 5,2	0,7	0,5	0,8

В табл. 4.12 приведены примеры расчета статистических характеристик различных корреляционных функций для широко используемых в системах связи дискретных сигналов и, в том числе, характеристики криптографических ДП. Указанные характеристики были получены с использованием разработанного специального программного обеспечения (Приложения В и Г). Расчеты проводи-

лись для различных значений периода ДП. В качестве статистических характеристик корреляционных функций были использованы:

- значения наибольших боковых выбросов R_{max};

- величина математического ожидания модуля выбросов $m_{|R|}$;

- значение среднеквадратического отклонения модуля выбросов $D_{|R|}^{1/2}$ и значения выбросов $D_{R}^{1/2}$.

Анализ данных, приведенных в табл. 4.12, свидетельствует о том, что значения максимальных боковых выбросов КС, а также статистические характеристики данного класса сигналов не уступают соответствующим характеристикам сигналов, построенных на использовании М-последовательностей.

Таблица 4.13

Корреляционные свойства криптографических дискретных последовательностей

№ п/п	Размерность сегмента КП	Граничные значения функции неопределенности	ПФАК			АФАК	ПФВК			АФВК
			Число КП удовлетворяющих границе	Наименьшее значение Rбmax	Количество КП с наименьшим Rбmax	Количество КП, удовлетворяющих границе	Общее количество пар	Количество пар, удовлетворяющих границе	Наименьшее значение Rбmax	Количество пар, удовлетворяющих границе
1	31	9	7 743	5	155	3 622	29 977 024	1 465 137	5	14 537 423
2	63	17	10 868	9	14	7 166	59 056 712	12 214 869	11	54 822 445
3	127	23	3482	17	51	1302	6 062 162	47 053	19	1 619 780
4	511	59	3819	45	6	1951	7 292 380	122 835	51	3 466 713
5	1 023	100	8 513	77	9	6 194	36 235 584	5 293 538	79	35 083 491

В таблице 4.13 приведены данные, характеризующие корреляционные свойства КС различного периода. В частности, приведены: граничные значения боковых пиков автокорреляционных функций, достигаемых в классе М – последовательностей и число сигналов, удовлетворяющих данной границе в классе КС для различных функций корреляции; наименьшие значения боковых пиков различных функций корреляции и их количество; объем системы сигналов (в том числе, количество пар КС, удовлетворяющих граничным значениям для соответствующего периода последовательности) и другие.

В разделе 6 приведены результаты расчетов и исследований показателей эффективности телекоммуникационных систем при применении в них в качестве переносчиков данных пользователей нелинейных криптографических дискретных сигналов.

4.5 Метод оценки свойств нелинейных дискретных сложных сигналов

Известные методы синтеза ДС с заданными корреляционными функциями практически всегда основаны на проведении операций перебора множества вариантов для выбора лучшего результата и при значительном периоде ДП применение таких методов становится проблематичным.

В ходе исследований сформулированы и доказаны утверждения, позволившие разработать усовершенствованный метод, основанный на алгебраических свойствах элементов конечных полей, реализация которого приводит к существенно меньшему (по сравнению с известными методами перебора) объему вычислений по нахождению ДП с заданными значениями корреляционных функций в целях синтеза системы сигналов с необходимыми свойствами.

Исследование корреляционных, спектральных и статистических свойств характеристических дискретных сигналов (ХДС) показали, что данный класс сигналов по указанным свойствам весьма близок к широко используемым в телекоммуникационных системах в качестве расширяющих спектр М-последовательностям. Вместе с тем ХДС по сравнению с М-

последовательностями обладают улучшенными ансамблевыми и структурными свойствами.

Утверждение 4.3. Пусть W_μ и W_ν есть ХДС с числом символов L, построенные посредством децимации исходного сигнала W_1 (сигнал, построенный по наименьшему из значений первообразных элементов поля) соответственно по коэффициентам μ и ν, а μ' и ν' новые коэффициенты децимации, причём $\mu' = \mu \cdot x \pmod L$; $\nu' = \nu \cdot x \pmod L$, где x - целое число, такое, что наибольший общий делитель (НОД) чисел X и L равен 1. Тогда децимация исходного ХДС W_1 по коэффициентам μ' и ν' даёт новые пары, реализации ПФВК которых (значения боковых лепестков функции корреляции), есть результат децимации значений боковых лепестков ПФВК пары ХДС W_μ и W_ν.

Доказательство. Значение кодов ХДС, полученных путём децимации исходной последовательности по коэффициентам μ и ν, могут быть описаны выражениями:

$$\mu_i = \begin{cases} \psi\left(\Theta_a^{\mu_i} + 1\right), \text{если} \left(\Theta_a^{\mu_i} + 1\right) \equiv 0 \pmod P; \\ 1, \text{если} \left(\Theta_a^{\mu_i} + 1\right) \equiv 0 \pmod P; \end{cases} \tag{4.36}$$

$$\nu_i = \begin{cases} \psi\left(\Theta_m^{\nu_i} + 1\right), \text{если} \left(\Theta_m^{\nu_i} + 1\right) / \equiv 0 \pmod P; \\ 1, \text{если} \left(\Theta_m^{\nu_i} + 1\right) \equiv 0 \pmod P, i = \overline{0, N-1}. \end{cases} \tag{4.37}$$

Поскольку всегда можно найти такое k, что $\Theta_1 = \Theta^k$, где $\Theta = \Theta_1^\mu$, $\Theta_1 = \Theta_1^\nu$, и НОД $(k, L) = 1$, то (4.36) и (4.37) можно записать в следующем виде:

$$\mu_i = \begin{cases} \psi\left(\Theta^i + 1\right), \text{если} \left(\Theta^i + 1\right) \equiv 0 \pmod P; \\ 1, \text{если} \left(\Theta^i + 1\right) \equiv 0 \pmod P; \end{cases}$$

$$\nu_i = \begin{cases} \psi\left(\Theta_1^i + 1\right), \text{если} \left(\Theta_1^i + 1\right) \equiv 0 \pmod P; \\ 1, \text{если} \left(\Theta_1^i + 1\right) \equiv 0 \pmod P. \end{cases}$$

Для сигналов, полученных по коэффициентам децимации μ' и ν', имеем

$$\mu_i^{'} = \begin{cases} \psi\left(\Theta^{i_1 x}+1\right), \text{если}\left(\Theta^{i_1 x}+1\right)/\equiv 0\left(\mathrm{mod}\,P\right); \\ 1, \text{если}\left(\Theta^{i_1 x}+1\right)\equiv 0\left(\mathrm{mod}\,P\right); \end{cases}$$

$$\nu_i = \begin{cases} \psi\left(\Theta_1^{i_1 x}+1\right), \text{если}\left(\Theta_1^{i_1 x}+1\right)/\equiv 0\left(\mathrm{mod}\,P\right); \\ 1, \text{если}\left(\Theta_1^{i_1 x}+1\right)\equiv 0\left(\mathrm{mod}\,P\right). \end{cases}$$

Выражения для ПФВК пар ХДС, построенных соответственно по μ, ν и $\mu^{'}$, $\nu^{'}$ имеют вид:

$$R_{\mu,\nu}\left(m\right)=\sum_{i=0}^{L-1}\psi\left(\Theta^{i}+1\right)\cdot\psi\left(\Theta_1^{i+m}+1\right);$$

$$R_{\mu^{'},\nu^{'}}\left(m\right)=\sum_{i=0}^{L-1}\psi\left(\Theta^{i_1 x}+1\right)\cdot\psi\left(\Theta_1^{(i+m_1)x}+1\right).$$

И с учётом (4.37)

$$R_{\mu,\nu}\left(m\right)=\sum_{i=0}^{L-1}\psi\left(\Theta^{i}+1\right)\cdot\psi\left(\Theta^{k(i+m)}+1\right);$$

$$R_{\mu^{'},\nu^{'}}\left(m\right)=\sum_{i=0}^{L-1}\psi\left(\Theta^{i_1 x}+1\right)\cdot\psi\left(\Theta^{kx(i_1+m_1)}+1\right).$$

Введём произвольные переменные $\left\{a,b,b^{'}\right\}\in GF\left(P^n\right)$. Пусть для сигналов, построенных путём децимации исходного сигнала, выполняются условия $a=\Theta^{k(i+m)}$, $b=\Theta^{i}$. Тогда $a/b=\Theta^{ki+km-i}$. Для пары сигналов, полученных путём децимации исходного сигнала по коэффициентам $\mu^{'}$ и $\nu^{'}$, найдём некоторое значение $\Theta^{kx(i_1+m_1)}$ равное a, т.е.

$$\Theta^{kx(i_1+m_1)}=\Theta^{k(i+m)}=a\,. \qquad (4.38)$$

Для выполнения равенства (3) необходимо, чтобы

$$kx\left(i_1+m_1\right)\equiv k\left(i+m\right)\left(\mathrm{mod}\,L\right). \qquad (4.39)$$

Поскольку НОД $\left(k,L\right)=1$, выражение (4.39) можно переписать в виде

$$x\left(i_1+m_1\right)\equiv i+m\left(\mathrm{mod}\,L\right);\; xi_1+xm_1\equiv i+m\left(\mathrm{mod}\,L\right);$$
$$xi_1\equiv i\left(\mathrm{mod}\,L\right);\; xm_1\equiv m\left(\mathrm{mod}\,L\right).$$

Найдём отношение a/b', где $b' = \Theta^{i_1 x}$ для пары ХДС, построенной в соответствии с коэффициентами μ' и ν'.

$$a/b' = \frac{\Theta^{kx(i_1+m_1)}}{\Theta^{i_1 x}} = \Theta^{kxi_1+kxm_1-i_1 x}. \qquad (4.40)$$

С учётом (4.40) можно заключить, что $a/b' = a/b$ и, следовательно, $b' = b$, а это означает, что в выражении для $R_{\mu',\nu'}(m_1)$ ПФВК изменится лишь порядок набора суммы для некоторого фиксированного отсчёта ПФВК пары ХДС, построенной по μ' и ν'. Другими словами, значения функции ПФВК для пары ХДС, построенной путём децимации исходного сигнала по коэффициентам μ' и ν' будут такими же, как для ПФВК последовательностей, полученных по μ и ν. Но, с учётом того, что $m = xm_1$, $R_{\mu',\nu'}(m_1)$ - есть результат децимации $R_{\mu,\nu}(m)$ по коэффициенту x, т.е. реализация $R_{\mu',\nu'}(m_1)$ ПФВК будет результатом децимации ПФВК $R_{\mu',\nu'}(m)$. Утверждение доказано.

С учётом утверждения 4.3 могут быть определены все предпочтительные пары ХДС, т.е. пары, имеющие минимальные значения боковых лепестков функции корреляции.

Для приложений важным является знание значений максимальных боковых выбросов ПФВК для данной системы сигналов с объёмом M. С тем, чтобы оценить значения, которые принимают выбросы ПФВК сигналов с помощью традиционных методов вычисления ПФВК, необходимо провести расчёты значений выбросов для всех возможных сочетаний пар сигналов.

Ниже приводится утверждение, которое приводит к уменьшению объема вычислений для нахождения ДП, обладающих требуемыми взаимно корреляционными свойствами.

Введем ряд ограничений. В качестве ДП будем рассматривать характеристические дискретные сигналы, а в качестве корреляционной функции – периодическую ФВК (ПФВК). Будем называть ПФВК различных пар ХДС функциями одно-

го типа в случае, если реализации ПФВК (например, значения максимальных боковых лепестков ПФВК) для них одинаковы. Назовём $\|R\|$ взаимно корреляционной матрицей, номерами строк и столбцов которой являются коэффициенты децимации, в соответствии с которыми формируются ХДС. На пересечении строк и столбцов матрицы размещены значения максимальных боковых выбросов ПФВК ХДС.

Утверждение 4.4. Пусть $\|R\|$ есть матрица максимальных значений боковых лепестков ПФВК пар ХДС w_i и w_j, $i,j=\overline{1,M}$ размерности $M\times M$, причём M - число изоморфизмов ХДС, а строки и столбцы матрицы обозначены значениями упорядоченных по возрастанию коэффициентов децимации. Тогда строка матрицы (первая строка), содержащая значения боковых лепестков ПФВК исходного изоморфизма со всеми оставшимися $(M-1)$ изоморфизмами, содержит все возможные значения боковых лепестков ПФВК, которые дают пары w_i и w_j, $i,j=\overline{1,M}$.

Утверждение указывает на тот факт, что для знания значений максимальных боковых выбросов ПФВК сочетаний всех пар ХДС достаточно рассчитать реализации ПФВК исходного сигнала w_1 со всеми w_2, w_3, …, w_{M-1} изоморфизмами, т.е. реализации ПФВК для первой строки матрицы $\|R\|$.

Доказательство. Для доказательства утверждения достаточно доказать, что ПФВК двух ХДС, построенных по коэффициентам децимации, например, k_1 и k_2 (коэффициенты, принадлежащие первой строке матрицы и один из коэффициентов децимации равен 1), всегда существует некоторое число $\nu\in L$, являющееся взаимно простым с периодом характеристического кода L и можно вычислить коэффициенты $k_1^{'}=k_1\cdot\nu\left(\mathrm{mod}\,L\right)$ и $k_2^{'}=k_2\cdot\nu\left(\mathrm{mod}\,L\right)$. При этом пара коэффициентов k_1 и k_2 переходит в пару коэффициентов $k_1^{'}=1$ и $k_2^{'}$, находящуюся в первой строке взаимно корреляционной матрицы $\|R\|$.

Утверждение о том, что существует такое ν, для которого $k_1 \cdot \nu = 1 \cdot (\mathrm{mod}\, L)$ следует из теоремы Эйлера [43,52], в соответствии с которой, если есть такое k_1, что $(k_1, L) = 1$, то

$$k_1^{\phi(L)} \equiv 1 \cdot (\mathrm{mod}\, L), \qquad (4.41)$$

где $\phi(L)$ - функция Эйлера.

Из (4.45) следует, что для каждого коэффициента из множества коэффициентов децимации есть обратный - $k_1^{\phi(L)-1}$, при этом

$$k_1^{\phi(L)} = k_1 \cdot k_2 \cdot \ldots \cdot k_L = 1 (\mathrm{mod}\, L). \qquad (4.42)$$

Число сомножителей в (4.42) определяется функцией Эйлера.

Пары ХДС, построенные по коэффициентам децимации k_1, k_2 и $k_1' = 1$, k_2', дают ПФВК одного типа, а это значит, что в первой строке матрицы $\|R\|$ содержатся все возможные типы ПФВК, существующие для системы сигналов с объёмом M. Утверждение доказано.

Проиллюстрируем на примере возможности, которые предоставляет данное утверждение по нахождению пар ХДС, имеющих заданные характеристики (например, значения максимальных боковых лепестков ПФВК).

В таблице 4.15 приведена взаимно корреляционная матрица, содержащая значения боковых лепестков ПФВК для ХДС с числом элементов $L = 60$. Первая строка матрицы включает в себя значения боковых лепестков ПФВК исходного изоморфизма ХДС (коэффициент децимации $k_1 = 1$) со всеми другими изоморфизмами, полученными путём децимации исходного ХДС по множеству коэффициентов децимации $k_i \in \phi$ (L). Исходя из данных таблицы, минимальное значение максимальных боковых лепестков ПФВК имеет место для пар ХДС, полученных по коэффициентам децимации 1 и 7.

В соответствии с приведенной выше теоремой, могут быть установлены все пары ХДС, приводящие к таким же значениям боковых лепестков. Например, умножая коэффициенты децимации $k = 1$ и $k = 7$ на x = 7, мы получим новую па-

ру изоморфизмов ХДС, для которой $k = 7$ и $k = 49$. Как следует из таблицы 1, данная пара ХДС имеет такое же значение максимальных боковых лепестков ПФВК как и для исходной пары, т. е. 16.

Нетрудно убедиться в том, что знание значений первой строки взаимокорреляционной матрицы является исчерпывающим для расчёта статистических характеристик ПФВК системы ХДС.

Таблица 4.14

Взаимно корреляционная матрица для ХДС с числом элементов $N = 60$

Коэф. децимации	1	7	11	13	17	19	23	29	31	37	41	43	47	53	59	49
1	60	16	24	20	20	16	20	36	32	20	36	16	20	20	16	28
7	16	60	20	16	24	20	36	20	20	32	20	28	36	16	20	16
11	24	20	60	20	16	36	20	16	36	20	32	20	20	16	28	16
13	20	16	20	60	36	16	24	20	16	28	20	32	16	36	20	20
17	20	24	16	36	60	20	16	20	20	36	20	16	32	28	16	20
19	16	20	36	16	20	60	20	24	28	16	16	20	20	20	36	32
23	20	36	20	24	16	20	60	16	20	16	16	36	28	32	20	20
29	36	20	16	20	20	24	16	60	16	20	28	20	16	20	32	36
31	32	20	36	16	20	28	20	16	60	16	24	20	20	20	36	16
37	20	32	20	28	36	16	16	20	16	60	20	16	24	36	20	20
41	36	20	32	20	20	16	16	28	24	20	60	20	16	20	16	36
43	16	28	20	32	16	20	36	20	20	16	20	60	36	24	20	16
47	20	36	20	16	32	20	28	16	20	24	16	36	60	16	20	20
53	20	16	16	36	28	20	32	20	20	36	20	24	16	60	16	20
59	16	20	28	20	16	36	20	32	36	20	16	20	20	16	60	24
49	28	16	16	20	20	32	20	36	16	20	36	16	20	20	24	60

Приведем количественную оценку выигрыша (К) в производительности предложенного метода синтеза системы сигналов по сравнению с методом полно-

го перебора возможных сочетаний пар последовательностей для создания системы сигналов с необходимыми корреляционными свойствами.

Нетрудно убедиться, что выигрыш в производительности синтеза системы сигналов, может быть определен из выражения

$$К = (C_{\varphi(L)}^2/2)/ \varphi(L), \qquad (4.43)$$

где $\varphi(L)$ – функция Эйлера.

Так для периода ХДС L = 10098, $\varphi(L) = 2880$ и выигрыш К в производительности синтеза системы сигналов с заданными свойствами при использовании разработанного метода по сравнению с известными методами составляет 720 раз. Разработана имитационная (программная) модель, реализующая предложенный метод оценки свойств нелинейных дискретных сигналов. Блок схема алгоритма, примеры реализации и расчета характеристик корреляционных функций сигналов приведены в Приложении Г.

4.6 Структурная скрытность нелинейных дискретных криптографических сигналов

Достижение требуемых значений помехозащищенности, скрытности, криптографической стойкости, ввода системы в синхронизм, смены режимов работы телекоммуникационной системы может быть достигнуто на основе использования принципов распределения спектра или широкополосной связи. При этом указанные характеристики могут быть реализованы за счет использования в радиоканалах динамического режима передачи данных в сочетании с применением дискретных сложных сигналов, обладающих заданной структурной скрытностью. Динамический режим предполагает такой способ передачи информации по радиоканалу, при котором осуществляется динамическая смена по определенному (случайному) закону соответствия: «информационный бит (2^m бит) – сложный сигнал». Момент смены соответствия должен определяться некоей управляющей последовательностью (УП) или гаммой.

Очевидно, что для достижения высоких показателей помехозащищенности, скрытности, криптографической стойкости телекоммуникационной системы, необходимо, чтобы УП отвечали определенным требованиям, а дискретные сигналы обладали соответствующими ансамблевыми, структурными, корреляционными и другими специальными свойствами.

В настоящем разделе проводится обоснование выбора критериев и показателей оценки качества (структурной скрытности) УП (гамм) и криптографических сигналов.

Идеальная структурная скрытность сигнала (в соответствии с критерием (1.29) означает, что методы синтеза сигнала должны реализовывать сигналы, отвечающие определенным требованиям. Вполне очевидно, что такие требования соответствуют требованиям, предъявляемым к генераторам, которые формируют случайные (псевдослучайные) последовательности. Кроме того, должна существовать возможность выполнить оценку соответствия свойств синтезированных сигналов определенным требованиям.

Методы формирования последовательностей символов для приложений управляющих сигналов и сигналов-переносчикеов информации, можно разделить на два больших класса - случайные (физические) и псевдослучайные [56,73,76,81,91,109]. Средства, обеспечивающие генерацию случайных последовательностей чисел или битов, будем называть генераторами случайных последовательностей (ГСП), а генераторы, обеспечивающие генерацию псевдослучайных последовательностей (ПСП) - детерминированными генераторами случайных последовательностей (ДГСП) Генератор случайных последовательностей - это механизм генерации случайных последовательностей, в котором для генерации случайного потока используется источник энтропии, основанный на физически случайных явлениях или случайном явлении [65].

Детерминированный генератор случайных последовательностей (ДГСП) является одним из базовых примитивов для большинства криптографических приложений, он обеспечивает генерацию последовательностей, которые называют псевдослучайными. Одним из основных свойств и преимуществ ДГСП является

обеспечение восстанавливаемости последовательности в пространстве и времени. В то же время ПСП должны иметь гарантированные свойства относительно периода повторения, восстановление отрезков ПСП в пространстве и времени, возможность проведения предварительного исследования их свойств и т.п. [65]. При этом необходимо учитывать, что никакой детерминированный алгоритм не может генерировать полностью случайные последовательности, он может только аппроксимировать некоторые свойства случайных последовательностей

Клод Шеннон показал [28], что симметричная схема шифрования (например, шифр Вернама) является теоретически недешифруемой только в том случае, если ключевая последовательность k имеет равномерный закон распределения (она генерируется случайно, однородно, имеет равновероятное распределение), а биты (числа) являются независимыми.

Большинство ДГСП имеют ряд серьезных недостатков, а последовательности, которые генерируются такими генераторами, не соответствуют требованиям, предъявляемым криптографическими приложениями, и приложениями, связанными с реализацией динамического режима функционирования систем связи со сложными сигналами. Основными недостатками ДГСП являются:

- недопустимо короткий или недоказанный период повторения последовательности Yi;

- недостаточный уровень необратимости относительно нахождения ключа Ki (УП), что позволяет решать задачу нахождения Yi с полиномиальной или субэкспоненциальной сложностями;

- недостаточная неразличимость Y_i, что также делает ее определенным образом предсказуемой «вперед и назад»;

- свойства случайности, равновероятности, независимости и однородности не соответствуют требованиям и другие.

Существует несколько подходов к определению требований к уровням гарантий ДГСП. Первый подход связан с тестированием ПСП на неразличимость, для чего, например, применяются федеральные стандарты FIPS 140-1, FIPS 140-2,

FIPS 140-3. Более детальные требования и механизмы реализации определены в AIS 20, что позволяет реализовать различные уровни гарантий: К1, К2, К3, К4 [3].

В AIS 31 относительно случайных последовательностей определены два уровня гарантий Р1 и Р2, в которых, по сути, Р1в определенной степени эквивалентен К1, К2, а Р2 - эквивалентен К3, К4. В случае уровня гарантий К4, требуется, чтобы ПСП имели статистические свойства, подобные статистическим свойствам последовательностей, генерируемым идеальным ДГСП, а также была задана энтропия источника ключей (то есть наличие и определенная длина ключа генератора обязательны), а также должна быть практически исключена возможность вычисления предыдущих и последующих последовательностей генератора при знании текущего состояния, т.е. заданные неразличимость, необратимость и непредсказуемость.

Под критерием будем понимать признак, на основе которого осуществляется оценка, определение или классификация чего-либо, то есть, по сути, будем понимать мерило оценки. Рассматривают две совокупностей критериев: безусловные и условные. Оценку свойств ДГСП (УП) рекомендуется выполнять в два этапа. На первом этапе проверяется их соответствие безусловным критериям, а на втором получают соответствующие интегральные оценки с использованием условных критериев.

К безусловным критериям относят те критерии, выполнение которых для ДГСП является обязательным, то есть безусловным. Анализ применения, опыт разработки и оценки свойств ДГСП, достигнутые результаты при практическом решении задач крипто анализа и реализации различных атак позволяют в качестве основных выбрать, как минимум, такие безусловные критерии оценки:

- надежность математической базы, применяемой в ДГСП;
- практическая защищенность ДГСП от известных атак;
- реальная защищенность ДГСП от всех известных и возможных крипто аналитических атак;
- статистическая безопасность ДГСП;
- непредсказуемость ПСП, генерируемых ДГСП;

- отсутствие слабых тайных (личных) ключей;

- сложность генерирования составляет не выше полиномиального характера.

Рассмотрим более подробно эти критерии, как в части понятий и определений, так и в части особенностей применения [109].

1. Надежность математической базы связывают с отсутствием у нарушителя возможностей совершать атаки типа «универсальное раскрытие» за счет несовершенства математической базы ДГСП или слабостей, которые могут быть заложены в виде специфических свойств общих параметров и ключей. При этом критерием оценки надежности математической базы является тот факт, что сложность атаки «универсальное раскрытия» имеет экспоненциальное характер, а критерием ненадежности - субэкспоненциальный или полиномиальный характер сложности. Будем обозначать этот критерий $W_{б1}$.

2. Практическая защищенность ДГСП от известных силовых и аналитических атак, которая достигается за счет выбора размеров общих параметров и ключей. Критерием практической защищенности ДГСП является выбор таких размеров общих параметров и ключей, при которых сложность атаки $W_{са}$ существенно (на необходимое число порядков) превышает существующую мощность крипто аналитических систем на уровне технологически развитых государств (нарушителя третьего уровня), в том числе с учетом прогноза увеличения мощности крипто аналитических систем за счет развития математического, программного обеспечения и т.д. Обозначим этот безусловный критерий $W_{б2}$.

3. Реальная защищенность ДГСП от всех известных и возможных крипто аналитических атак, где под защищенностью понимают тот факт, что все известные крипто аналитические атаки типа «полное раскрытие» имеют экспоненциальную сложность $W_{эс}$, а под критерием незащищенности - субэкспоненциальный $W_{сэ}$ и ниже характер сложности атаки «полное раскрытие». Будем обозначать этот безусловный критерий $W_{б3}$ и понимать под ним оценку необратимости.

4. Статистическая безопасность ДГСП, под которой понимают статистическую независимость исходных значений (выхода) генератора, например, от входных значений. Будем обозначать этот безусловный критерий $W_{б4}$.

5. Непредсказуемость «вперед и назад», под которой понимается отсутствие атак, связанных с определением как последующих, так и предыдущих ПСП. Этот безусловный критерий будем обозначать $W_{б5}$.

6. Отсутствие слабых личных (тайных) ключей ДГСП, при которых сложность крипто аналитических атак типа «полное раскрытие» и «универсальное раскрытия» меньше, чем сложность атаки «полное раскрытие» для других («не слабых») личных ключей. Обозначим этот безусловный критерий как $W_{б6}$.

7. Сложность генерирования $I_{ген}$ носит полиномиальный характер и не превышает допустимой величины $I_{д}$. Обозначим этот безусловный критерий также $W_{б7}$.

Так как приведенные частичные критерии являются безусловными, то интегральным критерием отбора является логическое изменение да / нет (1/0), и безусловный критерий можно записать в виде:

$$\left(w_{\delta 1}, w_{\delta 2}, w_{\delta 3}, w_{\delta 4}, w_{\delta 5}, w_{\delta 6}, w_{\delta 7}\right) \in (1,0). \qquad (4.44)$$

Таким образом, качество ДГСП (ПВП) может быть оценено с использованием безусловного интегрального критерия - функции соответствия ДГСП требованиям: $f_{фв}(.) \in (0;1)$.

Количественная оценка генераторов может быть сделана с использованием таких показателей, как:

- сложность обращения генератора ПСП, т.е. нахождение используемого ключа (УП);

- энтропия источника ключей (УП) $H_к$, в том числе для случая, когда ДГСП используется как источник ключей (УП);

- период $l_п$ (длина) повторения ПСП и безопасное время t_b;

- основание алфавита генерируемой УП;

- вероятность перекрытия в пространстве или во времени двух сегментов битов $Y_г$ и $Y_μ$, то есть в разных абонентах или у одного абонента в течение времени, так, что $Y_г = Y_μ$;

- расстояние равнозначности конкретной последовательности битов Y_0;

- пространственная $I_п$ и временная сложности $I_в$ формирования последовательности битов Y т.д.

Требованием минимальной защиты для ДГСП [9] является требование достаточно большой длины k случайного начального числа, такой, чтобы поиск по 2k - элементов был бы невыполнимым для нарушителя.

Основными общими требованиями к ДГСП являются [56]:

требование неразличимости исходных последовательностей ДГСП от истинно случайных последовательностей;

требование непредсказуемости выходных битов для нарушителя с ограниченными вычислительными ресурсами;

требование необратимости генератора в смысле предварительно заданной малой вероятности компрометации ключа самого ДГСП.

Таким образом, ПСП должна иметь некоторые статистические свойства [2], которые присущи для истинно случайных последовательностей.

Принципиальным отличием ДГСП и ГСП [2,56] для стохастических моделирований и криптографических приложений является то, что в криптографических системах, в системах связи, использующих динамическую смену соответствия «m бит - 2^m сложных сигналов», ДГСП дополнительно должны обеспечивать устойчивость против осуществления различного рода атак. Как показал анализ, атаки в системах, использующих ДГСП, могут осуществляться в целях [17]:

- нахождения неизвестных исходных данных (ключей, ключевой информации и параметров, генерируемых для других криптографических приложений);

- нахождения информации о внутреннем состоянии, в первую очередь значение ключа непосредственно самого генератора;

- манипулирования исходными данными генератора.

Потенциально возможные атаки можно разделить на три таких класса:

- крипто аналитические атаки, которые сводятся к решению математических задач обращения генератора, сложность которых меньше или существенно меньше атаки «грубая сила»;

- атаки, основанные на использования входных данных генератора;

- атаки, основанные на недостаточных показателях непредсказуемости.

По особенностям воздействия нарушителя потенциально возможные атаки можно разделить на две большие группы [17]:

- пассивные атаки, при осуществлении которых нарушитель отслеживает источник шума и части выходных данных генератора. Если он сможет обнаружить любые корреляции между этими двумя потоками, то он сможет использовать эти знания для прогнозирования предстоящих выходных данных, то есть ключей и / или параметров;

- активные атаки, при осуществлении которых нарушитель может повлиять на источник шума и, таким образом, иметь возможность влиять на последовательность битов, создаваемых генератором. Данный вид атаки особенно эффективен, так как злоумышленник может попытаться адаптировать входные шумы с характерными свойствами ДГСП для получения предполагаемых исходных данных.

ДГСП должны быть защищены от таких основных атак:

- крипто аналитические атаки, которые сводятся к решению математических задач, сложность которых меньше или существенно меньше атаки грубая сила;

- атаки, основанные на исходных данных генератора, которые осуществляются посредством определения или манипулирования исходными данными ДГСП с целью влияния на выходные данные (ключи, параметры и т.д. для других криптографических приложений);

- атаки, которые сводятся к распространению компрометируемого состояния генератора на другие состояния - предварительные или последующие.

Безусловным требованием к ДГСП является необходимость предотвращения любых атак, которые позволяют злоумышленнику получить информацию о его внутреннем состоянии.

Исследование статистических свойств осуществляются в рамках методики статистических испытаний на основе статистических тестов.

Наиболее приемлемыми (с точки зрения практического использования) методиками тестирования являются: NIST STS, FIPS PUB 140-1, AIS 20 и AIS 31, NIST 800-90b, NIST 800-22.

В состав NIST 800-22 входят 16 статистических тестов, вычисляются 188 значений вероятностей. Все тесты направлены на выявление различных дефектов случайности (не соответствие требованиям случайности).

Порядок тестирования.

1. Выдвигается нулевая гипотеза H_0 - предположение о том, что тестовая двоичная последовательность является случайной.

2. Для последовательности, формируемой генератором, рассчитывается статистика теста.

3. С использованием специальной функции и статистики теста рассчитывается значение вероятностей $P \in [0,1]$.

4. Значение вероятности P сравнивается с уровнем значимости α, $\alpha \in [0,001; 0,01]$. Если $P \geq \alpha$, то гипотеза H_0 - принимается. В противном случае - принимается альтернативная гипотеза.

В результате тестирования ПСП символов формируется вектор значений вероятности $P = \{P_1, P_2, ..., P_{188}\}$. В стандарте рекомендованной длиной является входной блок данных - 10^6 двоичных символов; в ходе одного тестирования используется 100 блоков такой длины (длина входных данных для одного цикла тестирования составляет 10^8 символов).

В NIST используются 2 порога для принятия решения о результатах тестирования - это 0.96 и 0.99, то есть для разных уровней значимости устанавливается, что из 100 блоков может не пройти четыре и один тест соответственно.

С использование NIST SP 800-22 было выполнено тестирование реализации криптографической последовательности символов. Результаты тестирования приведены в таблице 4.16.

Таблица 4.15

Оценка статистических свойств криптографических дискретных последовательностей с использованием NIST SP 800-22

№	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	Вероятность	Результат тестирования	Название теста
1	14	5	11	10	10	12	7	14	8	9	0,574903	0,99	Frequency
2	10	8	10	11	12	5	6	13	14	11	0,574903	0,99	BlockFrequency
3	13	6	5	14	18	10	9	5	12	8	0,058984	0,99	CumulativeSums
4	14	9	4	10	8	8	15	15	12	5	0,122325	1	CumulativeSums
5	9	8	8	12	10	10	14	7	8	14	0,759756	1	Runs
6	8	14	15	8	8	7	9	12	10	9	0,657933	1	LongestRun
7	12	10	11	7	11	7	6	15	11	10	0,678686	1	Rank
8	10	7	9	12	9	11	14	10	8	10	0,935716	1	FFT
9	10	10	6	10	7	10	11	9	9	18	0,419021	1	NonOverlapping Template
10	11	7	9	12	9	14	9	8	11	10	0,924076	0,98	NonOverlapping Template
11	17	11	14	10	10	6	10	7	7	8	0,319084	1	NonOverlapping Template
12	16	9	7	8	6	7	10	13	9	15	0,275709	0,98	NonOverlapping Template
13	12	6	7	8	11	7	12	10	13	14	0,616305	0,99	NonOverlapping Template
14	15	15	10	9	7	11	6	9	7	11	0,455937	0,98	NonOverlapping Template
15	11	9	13	7	11	14	9	12	8	6	0,719747	1	NonOverlapping Template
16	13	12	12	9	12	12	7	8	8	7	0,816537	0,97	NonOverlapping Template
17	11	11	14	8	10	8	10	10	9	9	0,971699	1	NonOverlapping Template
18	8	12	11	11	12	7	12	12	6	9	0,851383	1	NonOverlapping Template

Продолжение Таблицы 4.15

19	9	11	10	12	7	11	8	16	7	9	0,678686	1	NonOverlapping Template
20	14	10	13	10	12	12	6	7	11	5	0,494392	0,98	NonOverlapping Template
21	15	11	10	8	12	9	13	9	5	8	0,595549	0,95	NonOverlapping Template
22	9	5	14	10	7	6	14	9	13	13	0,334538	1	NonOverlapping Template
23	12	7	7	11	11	5	14	12	11	10	0,637119	0,99	NonOverlapping Template
24	10	12	12	11	15	10	7	10	6	7	0,657933	1	NonOverlapping Template
25	12	8	14	9	12	12	6	8	11	8	0,759756	0,98	NonOverlapping Template
26	6	7	7	10	14	7	8	15	15	11	0,249284	0,99	NonOverlapping Template
27	12	7	13	6	11	10	10	16	7	8	0,455937	0,98	NonOverlapping Template
28	12	9	9	12	9	10	6	7	17	9	0,474986	0,98	NonOverlapping Template
... 184	7	7	11	7	6	11	5	6	4	7	0,666838	0,9859	RandomExcursionsVariant
185	7	6	10	11	4	5	11	8	4	5	0,362174	1	RandomExcursionsVariant
186	6	11	11	1	9	11	4	4	6	8	0,076389	1	RandomExcursionsVariant
187	14	7	6	9	13	7	14	6	14	10	0,289667	1	Serial
188	11	8	13	5	6	11	14	8	14	10	0,419021	1	Serial
189	9	6	13	9	11	11	10	6	13	12	0,759756	0,99	LinearComplexity
											84,82113	186,0039	

Многочисленные исследования статистических свойств нелинейных криптографических последовательностей символов с применением NIST SP 800-22, показали, что указанные последовательности, формируемые с использованием раз-

работанного метода, удовлетворяют требованиям, предъявляемым к случайным последовательностям.

В таблице 4.16 приведены оценки (в соответствии с показателем (1.29)) выигрыша в структурной скрытности криптографических сигналов (КС) по отношению к линейным классам сигналов (М –последовательности).

Анализ данных таблицы 4.167 показывает, что криптографические сигналы обладают существенным выигрышем с точки зрения структурной скрытности по сравнению с линейными классами сигналов. Так при периоде сигнала 16383 элементов выигрыш составляет более 500 раз

Таблица 4.16

Оценка структурной скрытности различных классов сигналов

Класс сигналов	Период	Значение l	Выигрыш в структурной скрытности
М –последовательности	1023	20	51
криптографические сигналы	1023	1023	
М –последовательности	8191	26	315
криптографические сигналы	8191	8191	
М –последовательности	16383	28	585
криптографические сигналы	16383	16383	

Выводы к разделу 4

В четвертом разделе диссертации приведены результаты решения **третей, пятой, шестой и седьмой** задач исследования.

1. Проведенные исследования позволили сделать вывод о том, что комплексное решение проблемы обеспечения необходимых уровня помехозащищенности и информационной безопасности может быть достигнуто на основе реализации динамического режима передачи информации, при котором соответствие m бит - 2^m сложных сигналов меняется с течением времени по закону, предсказание которого возможно с вероятностью, не превышающей допустимой. Кроме того, приме-

нение в качестве сложных сигналов нелинейных систем сигналов, позволяет существенно повысить имитостойкость и структурную скрытность и, следовательно, - информационную безопасность ТКС.

2. В качестве расширяющих спектр дискретных последовательностей, в том числе в динамическом режиме, могут использоваться последовательности, которые формируют на основе авто – и изоморфизмов характеров конечных полей Галуа. При этом все множество таких сигналов может быть построено на основе применения методов децимации и разностных множеств. Важными свойствами таких систем дискретных сигналов является существенно большее (по сравнению с известными классами линейными сигналов) значение длин, для которых они могут быть построены. Соответствующие значения объема системы сигналов и спектра длин, для которых данные сигналы могут быть построены, приведены в таблицах 4.1- 4.3.

3. Информационная безопасность телекоммуникационной системы, в частности имитостойкость, в существенной мере зависит от объема системы сигналов, спектра значений периода, для которых могут быть синтезированы сигналы. Исследования свойств нелинейных дискретных сигналов в конечных полях и нелинейных криптографических сигналов показали, что данные классы сигналов обладают улучшенными по сравнению с известными классами линейных сигналов ансамблевыми свойствами. Объем системы нелинейных характеристических дискретных сигналов определяется числом классов неинверсно - изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы $T = \{t\} \ \{t, N\} = 1$ на смежные классы по классу автоморфных коэффициентов и значительно превышает объем системы линейных сигналов. Так, например, объем системы сигналов, составленной из нелинейных сигналов в конечных полях в интервале длительности последовательностей до десяти тысяч элементов в 4 тысячи раз превышает объем системы сигналов, составленной из М – последовательностей. На интервале длин от 50 до 1500, М - последовательности существуют только для пяти значений периода, доступное число последовательностей Лежандра составляет 114, число НС для этого интервала длин составляет 225, нели-

нейные криптографические сигналы могут быть построены для всех значений периода в указанном интервале. Ансамбль нелинейных криптографических сигналов более чем на 5 порядков превышает ансамбль, составленный из линейных сигналов - последовательностей с трехуровневой функцией взаимной корреляции. Превышение объема криптографических сигналов над ансамблем, составленным из М-последовательности, составляет более чем 7 порядков. Для характеристических сигналов с числом элементов $N = 2052$ существует 515 изоморфизмов, а для М-последовательностей с длиной $N = 2047$ - только 88 изоморфизмов.

4. Исследования структурной скрытности различных систем сигналов показали, что применение в телекоммуникационных системах линейных классов сигналов не позволяет достичь высоких показателей (по критерию) (1.29) структурной скрытности системы. Нелинейные классы сигналов в конечных полях обладают существенно большей структурной скрытностью. В работе получена математическая модель структуры нелинейной дискретной последовательности в конечном поле. Такая модель позволила определить зависимость характеров элементов поля (символов последовательности), и, таким образом, установить, что для нахождения закона формирования последовательности (сигнала) необходимо знать не менее половины символов сигнала. Криптографические нелинейные дискретные сигналы, как показали результаты проведенного тестирования, по своим статистическим свойствам, близки к свойствам случайных последовательностей, т.е. удовлетворяют свойствам непредсказуемости следования символов, необратимости, случайности, равно вероятности, независимости и однородности. Кроме того, сформулированные и доказанные в работе утверждения 4.1 и 4.2 позволяют аналитически определить структурную скрытность, в аддитивном и мультипликативном представлениях. Выявленные свойства элементов и характеров элементов конечных поля позволяют более чем в два раза повысить быстродействие устройств формирования характеристических дискретных сигналов.

5. В телекоммуникационных системах, в которых реализовано кодовое разделение абонентов имеют место взаимные помехи, которые являются следствием одновременной работы абонентов в общей полосе частот. Для таких приложений

телекоммуникационных систем следует выбирать сложные сигналы - физические переносчики данных таким образом, чтобы уровень взаимных помех был сколь угодно малым. При выполнении этого требования в системе может быть обеспечена заданная помехоустойчивость. В целом нелинейные дискретные сигналы, синтезированные на основе использования свойств характеров, могут быть отнести к минимаксным сигналам, т.е. значения максимальных боковых пиков периодической функции автокорреляции таких сигналов, не превышают границ «плотной упаковки». Максимальные боковые пики и статистические характеристики различных корреляционных функций (в частности и взаимно корреляционных) указанных сигналов близки к соответствующим характеристикам лучших, с точки зрения корреляционных функции, линейных дискретных сигналов.

6. В процессе исследований разработано специальное программного обеспечения, которое было использовано при исследовании корреляционных свойств сложных нелинейных дискретных сигналов в конечных полях Галуа. Указанное программное обеспечение позволяет рассчитывать статистические характеристики корреляционных функций, определять минимальные и максимальные значения (и их количество) боковых пиков функций корреляции. Пакет программ, примеры, реализующие оценки корреляционных свойств нелинейных дискретных сигналов в конечных полях Галуа, приведены в Приложении А. В качестве примера, на рисунке 4.1 приведен вид ПФАК ХДС длительностью N = 256 символов. С ростом периода последовательности ПФАК таких сигналов приближается к идеальной, когда боковые выбросы по сравнению с основным становятся пренебрежимо малыми.

7. Разработанное математическое и программное обеспечения позволяет синтезировать системы криптографических сигналов с необходимыми ансамблевыми, структурными и корреляционными свойствами (ПРИЛОЖЕНИЯ В и Г). Анализ данных, приведенных в табл. 4.12 – 4.14, позволяет сделать вывод о том, что криптографические сигналы обладают в целом улучшенными структурными, ансамблевыми, авто - и взаимными корреляционными свойствами, они могут быть построены для любых значений длины. При этом периодические и апериодиче-

ские функции их корреляции (в частности значения максимальных боковых пиков) могут быть заданы в процессе синтеза данного класса сигналов. Значения максимальных боковых выбросов корреляционных функций криптографических сигналов, а также статистические характеристики корреляционных функций данного класса сигналов не уступают соответствующим характеристикам сигналов, построенных на основе использовании М-последовательностей Пакет программ, примеры, реализующие оценки корреляционных свойств нелинейных криптографических сигналов, приведены в Приложении А.

8. Полученный в ходе диссертационных исследований усовершенствованный метод оценки свойств нелинейных дискретных сигналов в конечных полях Галуа, позволили существенно сократить время исследований корреляционных свойств сигналов, и, следовательно, уменьшить время синтеза систем сигналов с необходимыми (для тех или иных условий функционирования телекоммуникационной системы) свойствами. Так, для периода нелинейного сигнала L = 10098 (объем системы составляет 2880 сигналов), выигрыш в производительности синтеза системы сигналов с заданными свойствами при использовании усовершенствованного метода, по сравнению с известным, составляет 720 раз.

9. Исследования структурной скрытности различных систем сигналов показали, что применение в телекоммуникационных системах линейных классов сигналов не позволяет достичь высоких показателей структурной скрытности (по критерию (1.29)) телекоммуникационной системы. Нелинейные классы сигналов, методы синтеза которых получены в ходе диссертационных исследований, обладают существенно большей структурной скрытностью. В работе получена математическая модель структуры нелинейной дискретной последовательности в конечном поле. Такая модель позволила определить зависимость характеров элементов поля (символов последовательности), и, таким образом, установить, что для нахождения закона формирования последовательности (сигнала) необходимо знать не менее половины символов сигнала. Криптографические нелинейные дискретные сигналы, как показали результаты проведенного тестирования, по своим статистическим свойствам, близки к свойствам случайных последовательностей,

т.е. удовлетворяют свойствам непредсказуемости следования символов, необратимости, случайности, равно вероятности, независимости и однородности.

Таким образом, в разделе представлены результаты исследований свойств нелинейных дискретных последовательностей в конечных полях Галуа и нелинейных криптографических дискретных последовательностей, теоретические основы синтеза которых были представлены в разделах 2 и 3 диссертации. Показано, что сигналы, построенные путем манипуляции указанными нелинейными дискретными последовательностями информационных битов, обладают с одной стороны, структурными свойствами, аналогичными свойствам случайным последовательностей, а с другой, - корреляционными свойствами, близкими к свойствам лучших линейных классов сигналов, в частности, последовательностей с трехуровневой функцией взаимной корреляции. При этом ансамблевые свойства нового класса сигналов существенно превосходят ансамблевых свойств линейных классов сигналов. Указанное позволяет улучшить показатели помехозащищенности, имитостойкости, структурной скрытности телекоммуникационной системы, а так же помехоустойчивости приема сигналов в условиях воздействия структурных, заградительных, ретранслированных и других видов помех.

РАЗДЕЛ 5
МЕТОДЫ И СРЕДСТВА БЫСТРОЙ РЕАЛИЗАЦИИ МОДУЛЬНЫХ ОПЕРАЦИЙ

5.1 Принципы технической реализации модульных операций в модулярной системе счисления

Характерной чертой современного информационного общества является смещение вектора значимости интересов государства в сторону разработки и использования новых прогрессивных информационных технологий, которые в последние годы являются составляющими стратегических ресурсов любой страны. Достижение высоких экономических и социальных результатов, повышение доли Украины в мировой экономической системе в значительной мере зависит от масштабов и темпов проведения глобальной информатизации всего общества. Одним из наиболее важных направлений развития научно-технического прогресса в сфере создания и использования новых телекоммуникационных систем является развитие и внедрение эффективных компьютерных систем и компонентов вычислительной техники.

Ряд приложений телекоммуникационных систем, в частности мобильные телекоммуникационные системы, предполагают передачу данных от базовой станции к мобильным терминалам с высокой скоростью, в перспективе (сети четвертого поколения 4G) до 100 Мбит/с., что безусловно влечет за собой применение высокопроизводительных аппаратно-программных средств формирования и обработки сигналов, являющихся физическим переносчиком информации, передаваемой по каналам связи в таких системах.

Возрастающая сложность современных задач обработки цифровых сигналов данных опережает темпы повышения вычислительной мощности существующих универсальных позиционных компьютеров. В этом аспекте основным направлением совершенствования вычислительных устройств в позиционных системах счисления (ПСС) является удовлетворение требования неуклонного роста произ-

водительности реализации целочисленных вычислений. Проводимые теоретические, экспериментальные и промышленные исследования и разработки в этом направлении позволили обосновать перспективное направление роста производительности реализации целочисленных вычислений в ПСС, основанное на принципе распараллеливания вычислений [45].

Применение основных методов повышения производительности в ПСС, основанных на распараллеливании вычислений, путем использовании некоторых свойств решаемых задач и алгоритмов, не во всех случаях позволяет повысить производительность вычислений. Сфера применения их ограничивается классом решаемых задач. Кроме этого, сам процесс искусственного расчленения алгоритма, определение и выделение независимых вычислительных ветвей требует больших трудозатрат, причем, не всегда возможно распараллеливание произвольных алгоритмов вообще. Отметим, что все существующие методы повышения производительности в ПСС обладают общим недостатком: невозможность максимально распараллелить решаемые алгоритмы на уровне элементарных операций.

Одним из возможных направлений в решении задачи повышения производительности целочисленных вычислений является переход к машинной арифметике с нетрадиционным представлением операндов. В настоящее время из множества нетрадиционных машинных арифметик для практического применения в вычислительных компьютерных системах для формирования и обработки цифровых сигналов предлагаются следующие: модулярная система счисления (МСС) (арифметика в классе вычетов (КВ), система остаточных классов (СОК), модульная арифметика); коды Фибоначчи; биноминальная система счисления, модулярная комплексная арифметика Гаусса; арифметика в кольце полиномов.

Из перечисленных нетрадиционных машинных арифметик, для быстрой реализации операций, используемых при формировании и обработки сигналов в действительной числовой области вычислений, наибольшее практическое применение получила МСС. Малоразрядность остатков в представлении чисел в МСС дает возможность широкого выбора вариантов системотехнических решений при реализации модульных операций [45-46].

Известно, что в отличие от ПСС в МСС существует три принципа реализации модульных (арифметических) операций. Рассмотрим эти принципы.

Сумматорный принцип. Методы реализации модульных операций, основанные на сумматорном принципе, предполагают использование малоразрядных двоичных сумматоров по модулю m_i.

Принцип кольцевого сдвига (ПКС). Методы реализации модульных операций, основанные на этом принципе, предполагают использование кольцевых сдвигающих регистров.

Табличный (матричный) принцип реализации арифметических операций (ТП). Методы реализации модульных операций, основанные на табличном принципе, предполагают использование малоразрядных матричных ПЗУ (коммутаторов).

Рассмотрим методы и алгоритмы технической реализацию модульных арифметических операций, входящих в состав операций, используемых при формировании и обработке сигналов, основанные на перечисленных принципах реализации данных в МСС.

5.2 Методы реализации модульных операций, основанные на сумматорном принципе

В МСС действия производятся над числами, представленными в виде специальных машинных кодов в принятой системе счисления. Под системой счисления (СС) понимается способ обозначения чисел с целью определения их количественного значения посредством символов, имеющих определенные количественные признаки. Символы, применяемые для изображения чисел, называются цифрами. В зависимости от способа изображения чисел, посредством цифр, существующие СС условно делят на позиционные и непозиционные системы. Позиционной называется СС, в которой количественное значение каждой цифры разряда зависит от ее места (позиции) в исходном числе. В ПСС любое число изображается в виде последовательности цифр заданной СС

$$A = (a_{\rho-1}, a_{\rho-2}, \ \cdots \ , a_1, a_0), \qquad (5.1)$$

где ρ – разрядность операндов. Причем каждая цифра a_i (5.1) может принимать одно из возможных значений $0 \le a_i \le q-1$. Количество q различных цифр, используемых для изображения чисел в ПСС, называются основаниями q-ичной системы счисления ($q = 2$ – двоичная СС; $q = 3$ – троичная СС; $q = 10$ – десятичная СС и т.д.).

Наиболее просто реализуются процессы выполнения арифметических операций над операндами, представленными в двоичном коде ($q = 2$), т.е в двоичной позиционной системе счисления. В этом случае операнд представляется в виде

$$A = a_{\rho-1} \cdot 2^{\rho-1} + a_{\rho-2} \cdot 2^{\rho-2}, + \ \cdots \ +, a_1 \cdot 2 + a_0 \ , \qquad (5.2)$$

где $a_i = \overline{0,1}$ $(i = \overline{0, \rho-1})$.

Многоразрядные двоичные числа складываются, вычитаются, умножаются и делятся по тем же правилам, что и в десятичной СС. Так как операция сложения играет основную роль в вычислительном процессе, то рассмотрим ее более подробно.

В обычных двоичных позиционных системах счисления операция сложения двух чисел $A_{\text{ПСС}}$ и $B_{\text{ПСС}}$, где $A = a_{\rho-1} \cdot 2^{\rho-1} + a_{\rho-2} \cdot 2^{\rho-2}, + \ \cdots \ +, a_1 \cdot 2 + a_0,$ и $B = b_{\rho-1} \cdot 2^{\rho-1} + b_{\rho-2} \cdot 2^{\rho-2}, + \ \cdots \ +, b_1 \cdot 2 + b_0,$ осуществляется посредством использования сумматора. Сумматор – это узел, выполняющий операцию арифметического сложения (суммирования) двух чисел (слов). Под сложением понимается процесс образования слов с числовыми значениями $S = s_{\rho-1} \cdot 2^{\rho-1} + s_{\rho-2} \cdot 2^{\rho-2}, + \ \cdots \ +, s_1 \cdot 2 + s_0.$

Значение S_{i+1} суммы $(i+1)$-го разряда сумматора, а также значение C_{i+1} переноса в соседний старший разряд сумматора определяются следующими соотношениями

$$\begin{cases} C_{i+1} = a_{i+1} \wedge b_{i+1} \vee (a_{i+1} \vee b_{i+1}) \wedge c_i; \\ S_{i+1} = (a_{i+1} \oplus b_{i+1}) \bmod 2 \vee c_i. \end{cases} \qquad (5.3)$$

$$\begin{cases} C_0 = a_0 \wedge b_0; \\ S_0 = (a_0 \oplus b_0) \bmod 2, \end{cases} \tag{5.4}$$

где a_{i+1}, b_{i+1} - значение $(i+1)$-х разрядов чисел, соответственно, A и B;

a_0, b_0 – значения нулевых разрядов чисел, соответственно, A и B;

C_0 – значение сигнала переноса нулевого разряда сумматора;

S_0 – значение суммы нулевого разряда $(a_i, b_i, c_i, s_i \in 0,1)$.

Схема организации сложения в *i*-м двоичном разряде $a_{i+1} + b_{i+1} + c_i$ представлена на рисунке 5.1, а на рисунке 5.2 представлена схема сложения в двухразрядном двоичном позиционном сумматоре.

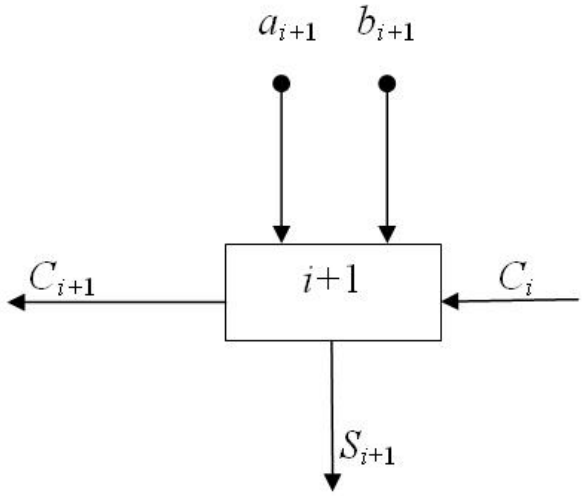


Рис. 5.1 Схема (i+1) – го разряда двоичного сумматора в ПСС

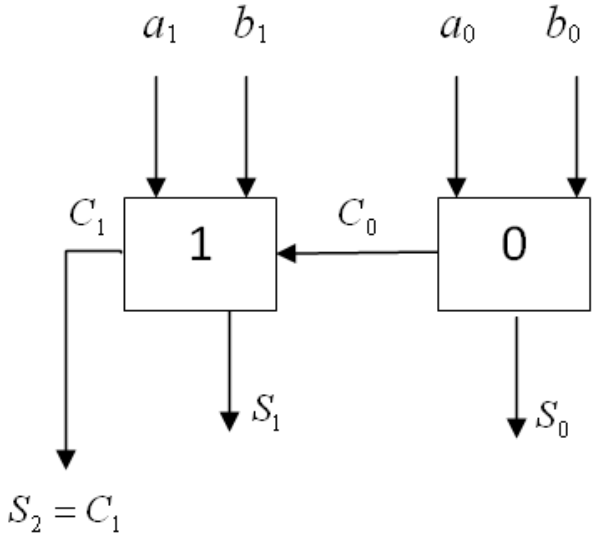


Рис. 5.2. Двухразрядный двоичный сумматор в ПСС

В таблицах 5.1 и 5.2 представлены алгоритмы реализации арифметической операции сложения, соответственно, для $(i+1)$- го разряда сумматора и для двух-разрядного двоичного сумматора в ПСС.

Таблица 5.1

Алгоритм обработки информации в i-м разряде сумматора в ПСС $(i=\overline{0,\rho-1})$

№ п.п.	a_{i+1}	b_{i+1}	C_i	S_{i+1}	C_{i+1}
1	0	0	0	0	0
2	0	0	1	1	0
3	0	1	0	1	0
4	0	1	1	0	1
5	1	0	0	1	0
6	1	0	1	0	1
7	1	1	0	0	1
8	1	1	1	1	1

Таблица 5.2

Алгоритм обработки информации двухразрядного двоичного сумматора в ПСС

A		B		S_2	S_1	S_0
a_1	a_0	b_1	b_0			
0	0	0	0	0	0	0
0	0	0	1	0	0	1
0	0	1	0	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	0	1
0	1	0	1	0	1	0
0	1	1	0	0	1	1
0	1	1	1	1	0	0
1	0	0	0	0	1	0
1	0	0	1	0	1	1
1	0	1	0	1	0	0
1	0	1	1	1	0	1
1	1	0	0	0	1	1
1	1	0	1	1	0	0
1	1	1	0	1	0	1
1	1	1	1	1	1	0

На рисунке 5.3 представлена общая схема обработки информации в $(i+1)$-м разряде двоичного сумматора в ПСС.

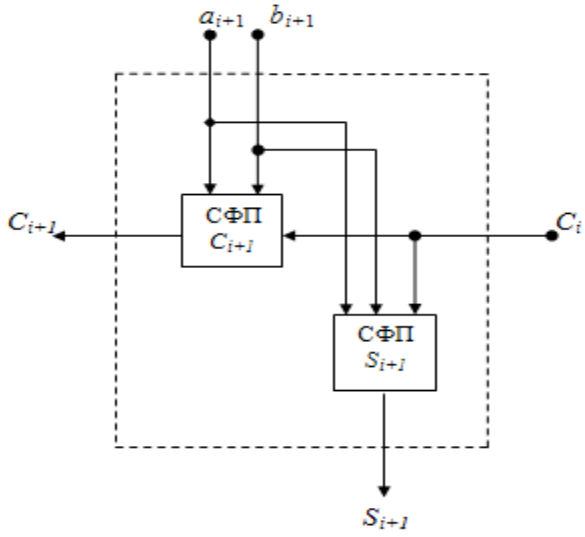


Рис. 5.3. Схема обработки информации в (i+1)-м разряде двоичного сумматора в ПСС

Схема обработки данных состоит из двух отдельных схем обработки информации: схема формирования признака C_{i+1} переноса (СФП C_{i+1}); схема формирования признака S_{i+1} суммы (СФП S_{i+1}). На рисунке 5.4 представлена принципиальная схема обработки информации в $(i+1)$- м разряде двоичного сумматора. Анализ процесса сложения двух чисел посредством позиционного сумматора показал, что основная сложность при реализации арифметических операций в ПСС – это организация процесса образования и распространения цифр C_i переноса от младшего разряда сумматора к старшему разряду.

Наличие межразрядных связей сумматора в ПСС обусловливает следующие недостатки:

- длительность выполнения арифметических операций, которая зависит от величины l разрядной сетки сумматора (для получения конечного результата операции приходится ожидать конца распространения переносов C_i на всю длину машинного слова);

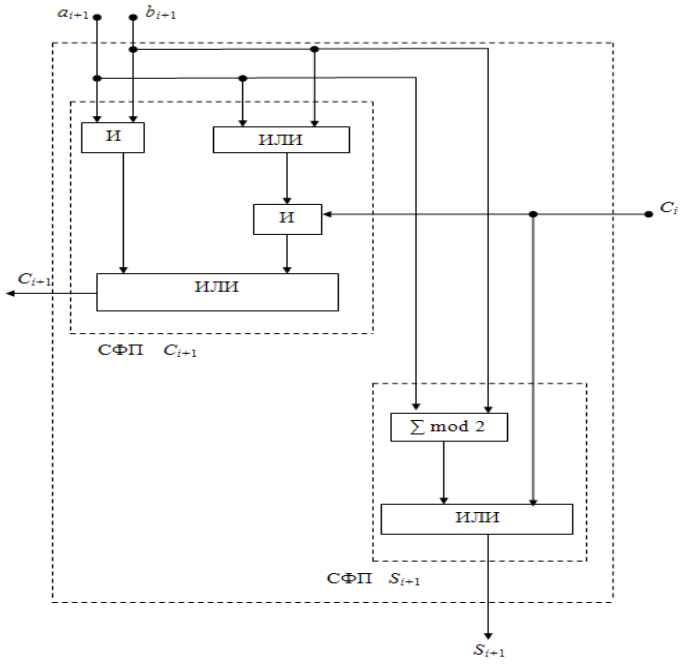


Рис. 5.4 Принципиальная схема обработки информации в $(i+1)$- м разряде двоичного сумматора в ПСС

- ошибка, возникшая в одном двоичном разряде сумматора, в процессе переноса от младших разрядов к старшим распространяется по всей длине машинного

слова; это обстоятельство обусловливает тот факт, что отказ (сбой) схемы обработки информации одного двоичного разряда сумматора способен вызвать не только однократные, но и многократные ошибки в полученном результате суммирования.

$$\begin{cases} C_{\rho-1} = S_\rho = a_{\rho-1} \wedge b_{\rho-1} \vee \left(a_{\rho-1} \vee b_{\rho-1}\right) \wedge c_{\rho-2} = a_{\rho-1} \wedge b_{\rho-1} \vee \left(a_{\rho-1} \vee b_{\rho-1}\right) \wedge \\ \wedge \left[a_{\rho-2} \wedge b_{\rho-2} \vee (a_{\rho-2} \vee b_{\rho-2}) \wedge c_{\rho-3} \right] = \overset{\rho-1}{\underset{i=1}{\vee}} (a_{\rho-i} \wedge b_{\rho-i} \vee a_{\rho-i} \vee b_{\rho-i}) \vee (a_0 \wedge b_0). \end{cases} \quad (5.5)$$

$$\begin{cases} S_{\rho-1} = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee c_{\rho-2} = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \wedge c_{\rho-3} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \vee (a_{\rho-3} \wedge b_{\rho-3} \vee a_{\rho-3} \vee b_{\rho-3}) \wedge c_{\rho-4} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \wedge (a_{\rho-3} \wedge b_{\rho-3} \vee a_{\rho-3} \vee b_{\rho-3}) \wedge \ldots \wedge (a_0 \wedge b_0) = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \cdot \overset{\rho-2}{\underset{i=1}{\vee}} (a_{\rho-1-i} \wedge b_{\rho-1-i} \vee a_{\rho-1-i} \vee b_{\rho-1-i}) \vee (a_0 \wedge b_0). \end{cases} \quad (5.6)$$

Искажение результата S_{i+1} операции $a_{i+1} + b_{i+1} + c_i$ в $(i+1)$- м двоичном разряде сумматора (т.е. $S_{i+1} \to \overline{S}_{i+1}$ $1 \to 0$ или $0 \to 1$) зависит от функционирования СФП S_{i+1} (см. выражение (5.3), рис. 5.4). Схема формирования признака C_{i+1} определяет сигнал переноса в $(i+2)$- й двоичный разряд сумматора. Таким образом, искажение результата (т.е. значений $S_{i+1} \to \overline{S}_{i+1}$ или $C_{i+1} \to \overline{C}_{i+1}$) операции суммирования в $(i+1)$- м двоичном разряде сумматора в ПСС происходит за счет отказов (сбоев) схем формирования значений S_{i+1} и C_{i+1} (см. рис. 5.4). Ошибка вида $C_{i+1} \to \overline{C}_{i+1}$) возникает как за счет переноса ошибки $\overline{C}_{i+1}$, возникшей в СФП C_{i+1}, так и в процессе переноса $(C_{i+1} \to \overline{C}_{i+1})$ значения $\overline{C}_{i+1}$ от $(i+1)$- го разряда к $(i+2)$- му разряду сумматора.

Отметим основные недостатки сумматорного принципа реализации арифметических операций:

- сложность синтеза двоичных сумматоров;

- большое время преобразования информации для значительных разрядных сеток, определяемое максимальным основанием МСС;

- сложность реализации операции умножения;

- неэффективное использование двоичных элементов, вследствие избыточности максимальных чисел, которые могут быть представлены сумматорами, по сравнению с величинами оснований МСС;

- низкая достоверность вычислений за счет ошибок, возникающих как в процессе вычислений, так и за счет переносов промежуточных значений поразрядного суммирования.

Техническая реализация устройств формирования и обработки сигналов, используемых в качестве переносчиков информации в телекоммуникационных системах, как и вообще схемная реализация любой системы счисления, определяется не только логической спецификой, но и применяемым оборудованием и организацией этого оборудования.

5.3 Методы реализации модульных операций, основанные на принципе кольцевого сдвига

Особенность ПКС заключается в том, что результат арифметической операции $(a_i \pm b_i) \bmod m_i$ по произвольному m_i модулю МСС, заданной совокупностью $\{m_j\}$ $(j = \overline{1,n})$ оснований, определяется без вычисления значений величин S_i и C_i, а только за счет циклических сдвигов заданной цифровой структуры. Действительно, известная теорема Кэли устанавливает изоморфизм между элементами конечной абелевой группы и элементами группы перестановок. В этом случае матрица сложения для произвольного m_i модуля МСС будет задана таблицей 5.3 (для m_i = 5 – таблицей 5.4).

Одно из следствий теоремы Кэли является вывод о том, что отображение элементов абелевой группы на группу всех целых чисел является гомоморфным. Это обстоятельство позволяет организовать процесс определения результата арифметических операций в МСС посредством использования ПКС. Так, операнд в МСС представляется набором из n остатков $\{a_i\}$, образованных путем последовательного деления исходного числа A на n попарно простых чисел $\{m_i\}$, $(i = \overline{1,n})$.

В этом случае совокупность остатков $\{m_i\}$ непосредственно отождествляется с суммой n простых полей Галуа вида $\sum_{i=1}^{n} GF(m_i)$. При рассмотрении метода реализации арифметических операций в МСС удобно и достаточно рассмотреть вариант для произвольного конечного поля Галуа $GF(m_i)$ при i=const, т. е. для конкретной приведенной системы вычетов по модулю m_i. Пусть для заданной операции модульного сложения $(a_i + b_i) \bmod m_i$ в поле $GF(m_i)$ составлена таблица Кэли (табл. 5.3). Вследствие наличия нейтрального элемента в поле $GF(m_i)$, в таблице 5.3 существует строка (столбец), в которой элементы данного поля стоят в порядке возрастания, а из того факта, что в поле вычетов $GF(m_i)$ эти элементы различны (порядок группы равен m_i), следует, что в каждой строке (столбце) таблицы 5.3 содержатся все элементы поля точно по одному разу. Использование перечисленных свойств позволяет реализовать операции модульного сложения и вычитания в МСС путем применения ПКС посредством n кольцевых $M = m_i([\log_2(m_i - 1)] + 1)$ - разрядных сдвигающих регистров (КСР).

Пусть произвольная алгебраическая система представлена в виде $S = \langle G, \otimes \rangle$,

где G - непустое множество; $\otimes$ - тип операции, определенной для любых двух элементов a_i, $b_i \in G$. Операция $\oplus$ сложения в множестве классов вычетов R, порожденных идеалом J, образует новое кольцо, называемое кольцом классов вычетов R/J. Его можно представить в виде Z/m_i, где Z - множество целых чисел $0, \pm1, \pm2, \ldots$. (Если основание МСС m_i - простое число, то Z/m_i - поле). Данное обстоятельство обусловливает возможность реализации арифметической операции сложения в МСС без межразрядных переносов (как в ПСС) путем только кольцевого сдвига содержимого разрядов КСР.

При двоичном кодировании операндов исходная цифровая структура для каждого модуля (основания) МСС представляется в виде содержимого первой

строки (столбца) таблицы модульного сложения (вычитания) $(a_i \pm b_i) \bmod m_i$ вида (5.6) (см. рис. 5.5).

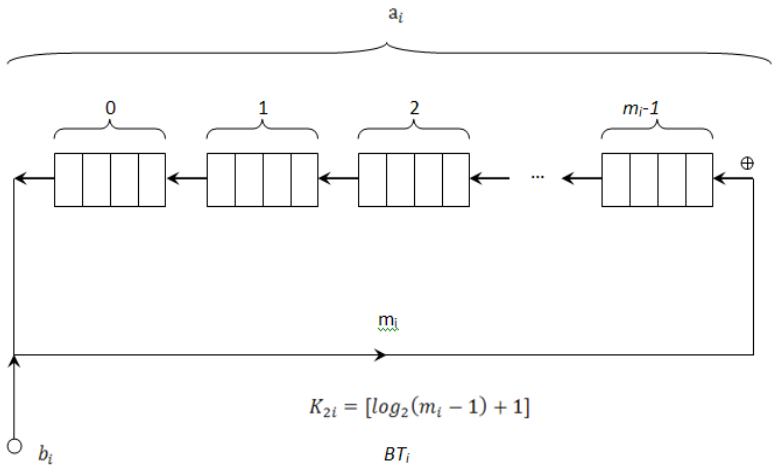


Рис. 5.5. Сумматор по модулю m_i в МСС (BT_i)

$$P_{\text{исх}}^{(m_i)} = \left[P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right], \qquad (5.6)$$

где $\|$ - операция конкатенации (присоединения, склеивание); $P_v(a_v)$ - k-разрядный двоичный код, соответствующий значению a_v - го остатка $(a_v = \overline{0, m_i - 1})$ числа по модулю m_i; $k = \left[\log_2(m_i - 1) + 1\right]$.

Таблица 5.3

Таблица Кэли для произвольного значения m_i

b_i	a_i				
	0	1	2	...	$m_i - 1$
0	0	1	2	...	$m_i - 1$
1	1	2	3	...	0
2	2	3	4	...	1
...	...	...	...	...	...
$m_i - 1$	$m_i - 1$	0	1	...	$m_i - 2$

Таблица 5.4

Таблица Кэли для $m_i = 5$

b_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Для заданного конкретного модуля m_i=5, исходная цифровая структура содержимого КСР имеет вид $P_{\text{исх}}^{(5)} = \left[000 \| 001 \| 010 \| 011 \| 100 \right]$.

Таким образом, посредством используемых в ПСС кольцевых регистров сдвига, легко реализовать целочисленные арифметические операции в МСС. При этом степени циклических перестановок, исходя из (5.6), определяется следующими выражениями:

$$\left[P_0(\alpha_0)\left\|P_1(\alpha_1)\right\|...\left\|P_{m_i-1}(a_{m_i-1})\right.\right]=\left[P_z(a_z)\left\|P_{z+1}(a_{z+1})\right\|...\left\|P_0(a_0)\right\|...\left\|P_{m_i-1}(a_{m_i-1})\right.\right]^z; \quad (5.7)$$

$$\left[P_0(a_0)\left\|P_1(a_1)\right\|...\left\|P_{m_i-1}(a_{m_i-1})\right.\right]^{-z}=\left[P_{m_i-1-z}(a_{m_i-1-z})\right\|...\left\|P_{m_i-z}(a_{m_i-z1})\right\|...\left\|...\right\|P_0(a_0)\left\|P_1(a_1)\right\|...\left\|P_{m_i-z-2}(a_{m_i-z-2})\right.\right]. \quad (5.8)$$

Отметим, что $\left[P_0(a_0)\,\|\,P_1(a_1)\,\|\,...\,\|\,P_{m_i-1}(a_{m_i-1})\right]^{m_i}=\varepsilon$, т.е. при $z = m_i$ все элементы упорядоченного множества $\{P_j(a_i)\}$ $(j=\overline{0,m_i-1})$ остаются на исходном месте. На рис. 5.6 представлена упрощенная схема операционного устройства в МСС на основе использования ПКС. При технической реализации данного метода первый операнд a_i определяет номер a_{a_i} разряда $P_{a_i}(a_{a_i})$, с содержимым результата модульной операции по модулю m_i, а второй операнд b_i - число разрядов КРС ($b_i k$ - двоичных разрядов), на которые необходимо провести сдвиги исходного (5.6) содержимого КРС в соответствии с алгоритмами (5.7), (5.8). На рис. 5.7 представлена упрощенная схема операционного устройства для однобайтового $(l=1)$ процессора в МСС.

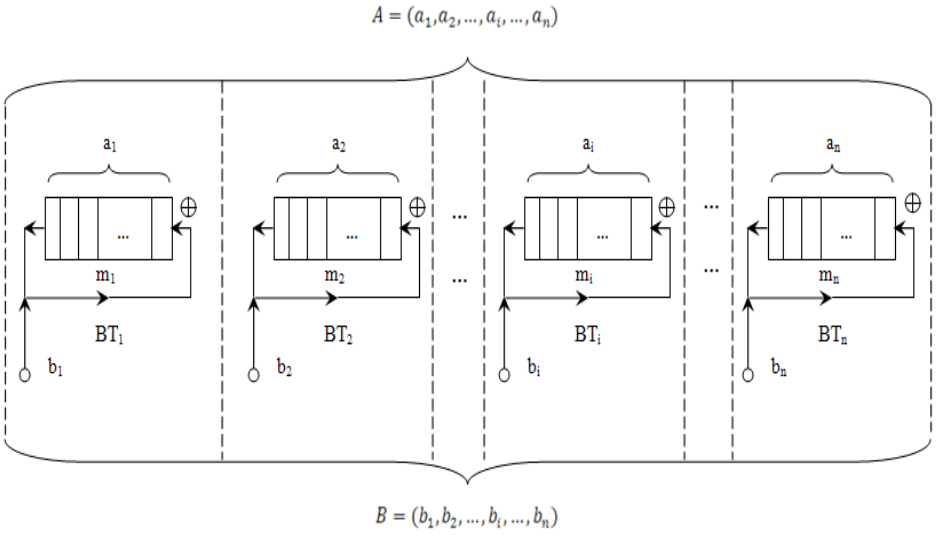


Рис. 5.6. Схема операционного устройства в МСС

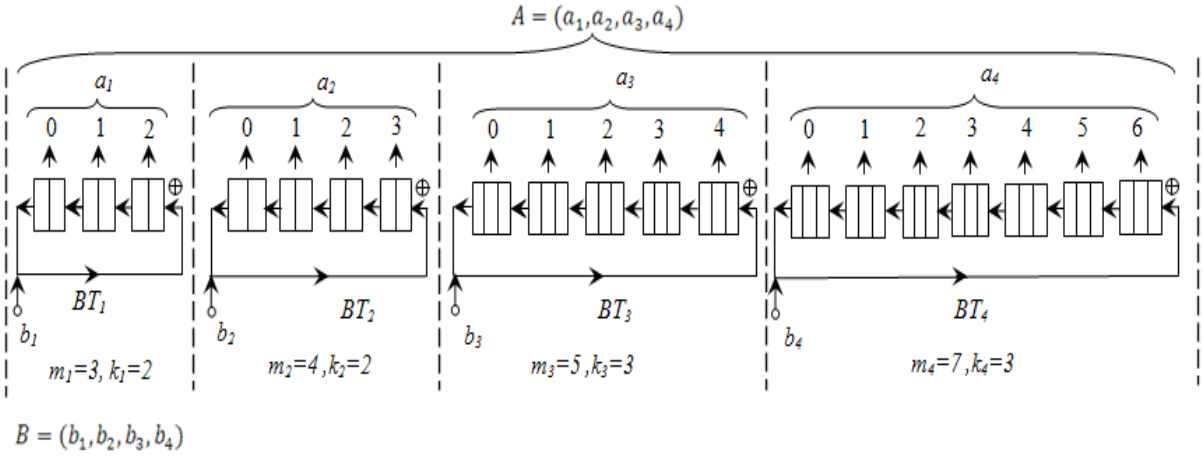


Рис. 5.7. Упрощенная схема операционного устройства в МСС для однобайтового $(l=1)$ процессора.

Исходя из [119,127-128,131] время сложения двух остатков $(a_i + b_i) \bmod m_i$ в МСС определяется математическим выражением

$$T^{(+)}_{\substack{\text{мсс} \\ m_i}} = K_{1i} \cdot K_{2i} \cdot t_{\text{сдв}}, \qquad (5.9)$$

где K_{1i} – значение второго b_i слагаемого в сумме $(a_i + b_i) \bmod m_i$ (количество разрядов КРС, на которое в положительном направлении (против часовой стрелки) сдвигается исходное содержимое КРС), т.е. $K_{1i} = \overline{0, m_i - 1}$;

K_{2i} – количество двоичных разрядов в одном разряде КРС по модулю m_i, т.е. $K_{2i} = \left[\log(m_i - 1)\right] + 1$;

$K_{1i} \cdot K_{2i}$ – количество сдвигаемых в положительном направлении двоичных разрядов КРС;

$t_{\text{сдв}} = 3 \cdot \tau_{\text{В}}$ – время “сдвига” одного двоичного разряда;

$\tau_{\text{В}}$ – время срабатывания одного логического вентиля (элементов И, ИЛИ).

Таким образом, для произвольного модуля m_i МСС время сложения двух остатков a_i и b_i равно

$$T^{(+)}_{\substack{\text{мсс} \\ m_i}} = 3 \cdot K_{1i} \cdot \left\{\left[\log_2(m_i - 1)\right] + 1\right\} \cdot \tau_{\text{В}}. \qquad (5.10)$$

В этом случае максимально возможное значение $T^{(+)}_{\substack{\text{мсс}\\ m_i}}$ для произвольного модуля m_i МСС равно

$$T^{(+)}_{\substack{\text{мсс}\\ m_i\\ max}} = 3\cdot(m_i - 1)\cdot\left\{\left[\log_2(m_i - 1)\right] + 1\right\}\cdot\tau_B, \qquad (5.11)$$

а для МСС максимальное время сложения двух чисел $A = (a_1, a_2, \cdots, a_n)$ и $B = (b_1, b_2, \cdots, b_n)$ равно

$$T^{(+)}_{\substack{\text{мсс}\\ m_n\\ max}} = 3\cdot(m_n - 1)\cdot\left\{\left[\log_2(m_n - 1)\right] + 1\right\}\cdot\tau_B. \qquad (5.12)$$

В общем случае время сложения двух чисел $A = (a_1, a_2, \cdots, a_n)$ и $B = (b_1, b_2, \cdots, b_n)$ в МСС определится временем $T^{(+)}_{\substack{\text{мсс}\\ m_i}}$ реализации модульной операции $(a_i + b_i) \bmod m_i$ в BT_i, для которого выполняется условие $K_{1i}\cdot K_{2i} = \max$ из всех $BT_j (j = \overline{1,n};\ i \neq j)$.

Приведем примеры конкретного выполнения операции сложения двух чисел в МСС для однобайтового $(l = 1)$ процессора (см. рис 5.7). Для $l = 1$ основания МСС могут быть следующими: $m_1 = 3,\ m_2 = 4,\ m_3 = 5$ и $m_4 = 7$.

Пример 5.1. Пусть второй операнд равен $B = (10,10,100,001)$. Тогда для $BT_1(m_1 = 3)$ имеем: $b_1 = 10,\ K_{11} = 2,\ K_{21} = \left[\log(m_i - 1)\right] + 1 = 2,$ и $K_{11}\cdot K_{21} = 2\cdot 2 = 4$. Для $BT_2(m_2 = 4)$ имеем: $b_2 = 10,\ K_{12} = 2,\ K_{22} = 2,$ и $K_{12}\cdot K_{22} = 2\cdot 2 = 4.$

Для $BT_3(m_3 = 4)$ – $b_3 = 100,\ K_{13} = 4,\ K_{23} = 3,$ и $K_{13}\cdot K_{23} = 4\cdot 3 = 12.$ Для $BT_4(m_4 = 7)$ – $b_4 = 001,\ K_{14} = 1,\ K_{24} = 3,$ и $K_{14}\cdot K_{24} = 1\cdot 3 = 3.$ Как видно, наибольшее количество сдвигаемых двоичных разрядов производится в третьем BT_3, а именно 12.

Таким образом, время сложения двух чисел *A* и *B* в МСС на основе принципа кольцевого сдвига определяется количественным значением второго слагаемого *B*, и равно $T^{(+)}_{\substack{\text{мсс}\\ m_3}} = K_{13}\cdot K_{23}\cdot 3\cdot\tau_B = 12\cdot 3\cdot\tau_B = 36\cdot\tau_B.$

Пример 5.2. Пусть $B = (10,11,001,001)$. Тогда имеем:

– для $BT_1(m_1=3)$, $b_1=2(10)$, $K_{11}=2$, $K_{21}=2$ и $K_{11}\cdot K_{21}=2\cdot 2=4$;

– для $BT_2(m_2=4)$, $b_2=3(11)$, $K_{12}=3$, $K_{22}=2$ и $K_{12}\cdot K_{22}=3\cdot 2=6$;

– для $BT_3(m_3=5)$, $b_3=1(001)$, $K_{13}=1$, $K_{23}=3$ и $K_{13}\cdot K_{23}=1\cdot 3=3$;

– для $BT_4(m_4=7)$, $b_4=1(001)$, $K_{14}=1$, $K_{24}=3$ и $K_{14}\cdot K_{24}=1\cdot 3=3$.

Таким образом, время сложения чисел *A* и *B* определяется временем реализации операции $(a_2+b_2)\bmod m_2$ во втором вычислительном тракте BT_2 и равно $T^{(+)}_{\substack{\text{мсс}\\ m_2}}=K_{12}\cdot K_{22}\cdot 3\cdot\tau_B=3\cdot 2\cdot 3\cdot\tau_B=18\cdot\tau_B$.

Проведем сравнительный анализ времени реализации операции сложения двух чисел A и B в ПСС и в МСС. Известно, что время $T^{(+)}_{\text{ПСС}}$ сложения чисел A и B в ПСС равно

$$T^{(+)}_{\text{ПСС}}=(2\cdot\rho-1)t_c=(16\cdot l-1)\cdot 3\cdot\tau_B, \qquad (5.13)$$

где: $\rho=8\cdot l$ – l-байтовое машинное слово (разрядная сетка системы обработки данных (СОД) для $l=\overline{1,4,8}$);

$t_c=3\cdot\tau_B$ – время суммирования в $(i+1)$- м двоичном разряде позиционного сумматора значений $a_{i+1}+b_{i+1}+c_i$, т.е определяется время нахождения значений C_{i+1} и S_{i+1}.

Учитывая, что существует метод уменьшения в два раза максимального времени реализации операции модульного сложения в МСС, для ПКС получаем

$$T^{(+)}_{\substack{\text{мсс}\\ \max}}=T^{(+)}_{\substack{\text{мсс}\\ m_n}}/2. \qquad (5.14)$$

Введем коэффициент α, как отношение времени реализации операции сложения в ПСС к соответствующему времени в МСС, т.е.

$$\alpha=T^{(+)}_{\text{ПСС}}/T^{(+)}_{\substack{\text{мсс}\\ \max}}=\frac{(16\cdot l-1)\cdot 3\cdot\tau_B\cdot 2}{(m_n-1)\cdot\{[\log_2(m_n-1)]+1\}\cdot 3\cdot\tau_B}=\frac{2\cdot(16\cdot l-1)}{(m_n-1)\cdot\{[\log_2(m_n-1)]+1\}}.$$

Первый операнд a_i указывает на номер разряда p_i КСР, который определяет результат модульной операции $(a_i+\beta_i)\bmod m_i$, а второй операнд β_i - определяет

необходимое количество сдвигов содержимого разрядов КСР. Очевидно, что при применении ПКС существенно повышается достоверность определения арифметической операции модульного сложения за счет устранения ошибок, возникших как в процессе, так и за счет переносов в связи с отсутствием таковых (как и при табличном принципе) вообще.

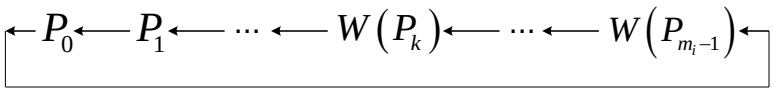


Рис. 5.8. Структурная схема кольцевого регистра сдвига для произвольного модуля m_i МСС

Если основание МСС m_i – простое число, то z/m_i – поле. Данное обстоятельство, как указывалось выше, и обуславливает возможность реализации арифметической операции сложения в МСС без межразрядных переносов путем использования принципа кольцевого сдвига посредством применения КСР (см. рис.5.9).

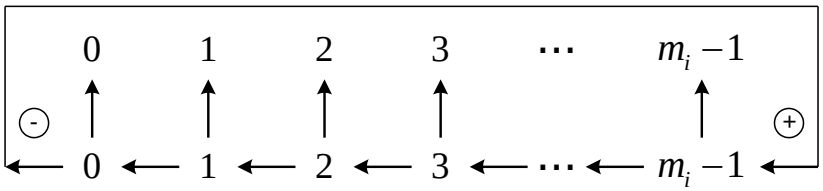


Рис. 5.9. Исходная информационная структура содержимого КРС для метода прямого сдвига

Пусть $m_i=5$ $\left(S=\langle\{0,1,2,3,4\},\langle+\rangle\right)$. Тогда таблица значений модульной суммы $(a_i+\beta_i)\bmod m_i$ для кольца класса вычетов $z/(S)$ представляется в виде числовых данных, например, первой строки (столбца) таблицы 5.4, рис. 5.10, где знаком $(+)$ обозначено положительное (против часовой стрелки) направление сдвига содержимого разрядов КРС.

В зависимости от формы представления содержимого разрядов КРС рассмотрим два метода реализации арифметических операций в МСС, основанные на использовании ПКС. Первый метод – метод двоичного позиционно-остаточного

кодирования. Данный метод реализации арифметических операций основывается на представлении содержимого КРС в двоичном коде. Второй метод – метод унитарного позиционного кодирования. Данный метод реализации арифметических операций основывается на представлении содержимого КРС в унитарном коде [127, 133].

5.4 Усовершенствованный метод реализации модульных арифметических операций, основанный на ПКС

Для рассматриваемых ниже методов двоичного кодирования данных, реализуемых арифметические модульные операции, характерно то, что содержимое разрядов КРС представляется позиционным двоичным кодом (см. рис. 5.10 для модуля МСС равного пяти $m_i=5$ $\left(S=\left\langle\{0,1,2,3,4\},\langle+\rangle\right\rangle\right)$. При этом первый операнд a_i – указывает номер разряда КСР, содержимое которого определяет результат данной операции, а второй операнд β_i указывает число сдвигов содержимого разрядов КСР.

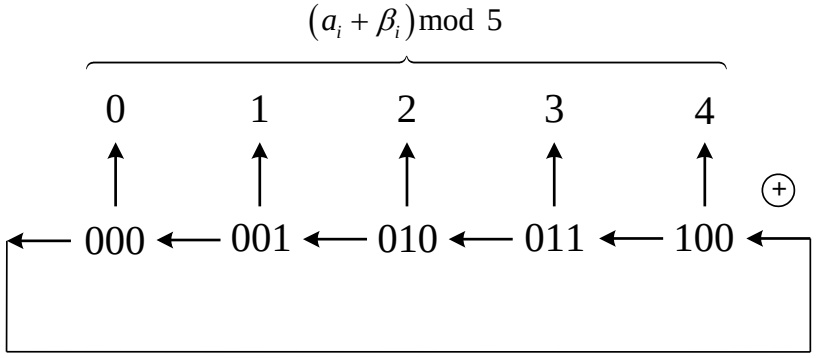


Рис. 5.10 Исходная информационная структура КРС для метода прямого сдвига ($m_i=5$)

Метод прямого сдвига. Введем и воспользуемся понятием оператора кольцевого сдвига (ОКС) – это оператор, определяющий величину (выраженную в количестве z одновременно сдвигаемых разрядов КСР) и направление сдвига разрядов КСР, и обозначается как $k^{(z)}$, где

$$z=\begin{cases}+z, & \text{при положительном направлениии сдвига содержимого разрядов КСР;}\\ -z, & \text{при отрицательном (по часовой стрелке) направлениии сдвига содержимого разрядов КСР;}\end{cases}$$

(z – показатель оператора кольцевого сдвига (ПОКС)).

Для операции модульного сложения ОКС представляется в виде $k^{(+\beta_i)}$, при этом время сдвига t_c (составляющее в основном время t выполнения операции) содержимого разрядов КСР определяется выражением:

$$t_c = k \cdot \tau \cdot z \qquad (5.15)$$

(в дальнейшем правомерно считать, что $t=t_c$),

где $k=\left[\log_2\left(m_n-1\right)\right]+1$ (m_n – максимальный по величине модуль МСС); τ – время сдвига одного двоичного разряда (время срабатывания одного триггера).

На основе ПКС, используя нижеприведенное тождество

$$\left(a_i-\beta_i\right)=\left[a_i+\left(m_i-b_i\right)\right]\bmod m_i,$$

можно реализовать и операцию модульного вычитания $\left(a_i-\beta_i\right)\bmod m_i$ (рис. 5.11).

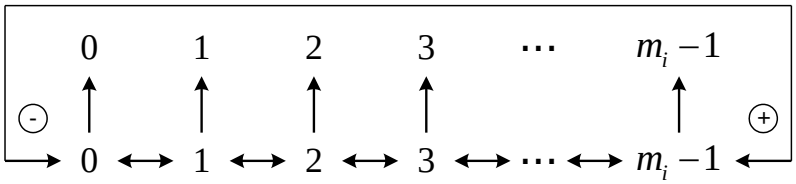


Рис. 5.11. Исходная информационная структура содержимого КРС для метода обратного сдвига

В этом случае ОКС имеет вид $k^{\left(+\left(m_i-\beta_i\right)\right)}$. Как видно, преимущество МСС по сравнению с методами, основанными на применении двоичных сумматоров, состоит в отсутствии межразрядных переносов, что существенно повышает достоверность реализации модульных операций. Однако, время выполнения модульных операций сравнительно велико, что снижает эффективность применения МСС.

Данное обстоятельство и обуславливает необходимость разработки алгоритмов повышения быстродействия выполнения данных арифметических операций.

Рассмотрим пример конкретного выполнения операции модульного сложения $(a_i + \beta_i) \bmod m_i$ посредством ПКС (табл. 5.4) для $m_i = 5$. Пусть $a_i = 001;\ \beta_i = 100$. Для этого случая исходное содержимое разрядов КСР представлено на рис. 5.12.

Таблица 5.5

Таблица значений $(a_i - \beta_i) \bmod 5$

β_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

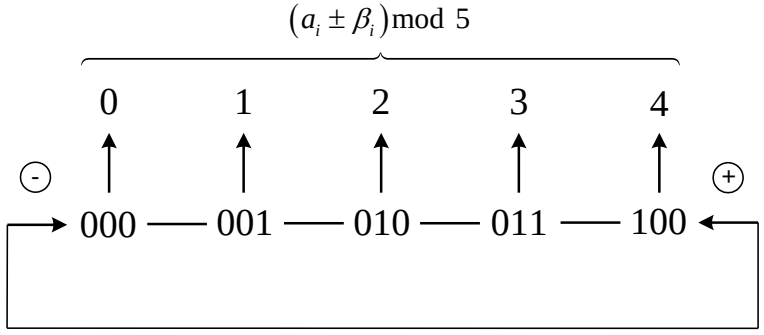


Рис. 5.12. Исходная информационная структура КРС для метода обратного сдвига $(m_i = 5)$

Первый операнд a_i определяет местоположение разряда КСР, содержимое которого будет определять результат операции (для $a_i = 001$ – первый разряд), а второй операнд β_i определяет необходимое количество сдвигов содержимого КСР, т.е. для $\beta_i = 100$ ПОКС имеет вид $z = +4$, а ОКС представляется в виде $k^{(+4)}$. Для данных значений входных операндов после четырех сдвигов в положитель-

ном направлении во втором разряде КСР будет находиться значение 000, что соответствует правильному результату операции $(1+4)\text{mod } 5 = 0$.

Алгоритм повышения быстродействия реализуется при использовании следующих соотношений: $a_i + \beta_i = \beta_i + a_i$, $a_i + (m_n - \beta_i) = (m_n - \beta_i) + a_i$.

В этом случае для операции модульного сложения $(a_i + \beta_i)\text{mod } m_n$ ПОКС представляется в виде

$$z = \begin{cases} +a_i, \text{ если } a_i \le \beta_i; \\ +\beta_i, \text{ если } a_i > \beta_i, \end{cases}$$

т.е., при $a_i \le \beta_i$, операнд a_i определяет количество z сдвигов содержимого КСР, а операнд β_i – номер разряда КСР, определяющий результат операции; при $a_i > \beta_i$ операнд β_i определяет количество z сдвигов содержимого КСР, а операнд a_i – номер разряда КСР, определяющий результат операции.

Для операции модульного вычитания $(a_i - \beta_i)\text{mod } m_i$ ПОКС представляется в виде:

$$z = \begin{cases} +a_i, \text{ если } a_i \le (m_i - \beta_i), \\ +(m_i - \beta_i), \text{ если } a_i > (m_i - \beta_i), \end{cases}$$

т.е. при $a_i \le (m_i - \beta_i)$ операнд a_i определяет количество z сдвигов содержимого разрядов КСР; при $a_i > (m_i - \beta_i)$ операнд $(m_i - \beta_i)$ определяет количество z сдвигов содержимого разрядов КСР, а операнд a_i – размер разряда КСР, определяющий результат операции. Данный алгоритм реализации модульных операций позволяет существенно уменьшить время t выполнения операции модульного сложения и вычитания (таблицы 5.4, 5.5 и рисунки 5.9 – 5.12).

Метод обратного сдвига**.** Один из алгоритмов повышения быстродействия выполнения операции модульного сложения (вычитания) является алгоритм, основанный на свойстве следующего тождества:

$$(a_i + \beta_i) = \left[a_i - (m_i - b_i)\right]\text{mod } m_i, \qquad (5.16)$$

т.е. сдвиг содержимого КСР можно осуществить как в положительную, так и в отрицательную сторону (для $m_i = 5$, рис. 5.13, где операции модульного сложения для ПОКС представляются в виде:

$$z = \begin{cases} +\beta_i, \text{ если } 0 \le \beta \le (m_i - 1)/2; \\ -(m_i - \beta_i), \text{ если } (m_i + 1)/2 \le \beta_i \le m_i - 1, \end{cases}$$

(в дальнейшем, без ущерба для общности рассуждений, будем считать, что m_i нечетное число), а для операции модульного вычитания ПОКС представляется в виде:

$$z = \begin{cases} +\beta_i, \text{ если } 0 \le \beta \le (m_i - 1)/2; \\ +(m_i - \beta_i), \text{ если } (m_i + 1)/2 \le \beta_i \le m_i - 1. \end{cases}$$

Применение данного алгоритма позволяет (в зависимости от величины модуля m_i) до 90% сократить значение величины z, что значительно уменьшает время t выполнения модульных операций.

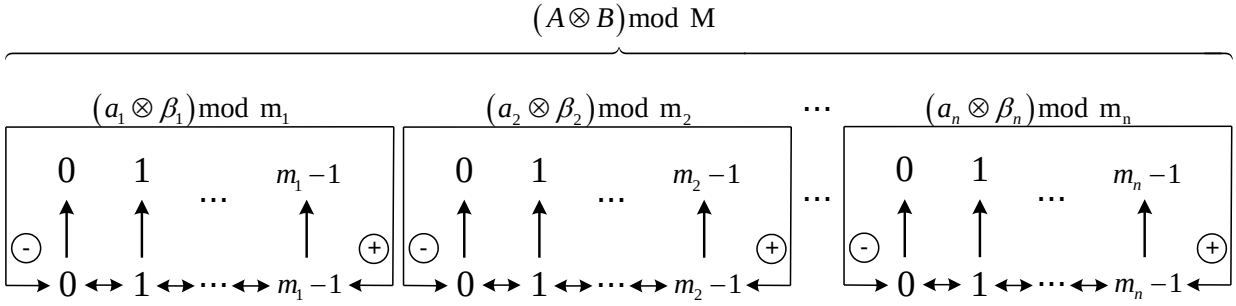


Рис. 5.13. Функциональная схема операционного устройства в МСС

Метод среднего значения. Рассмотрим алгоритм реализации МКС, позволяющий вдвое сократить максимальное значение ПОКС (максимальное число сдвигов содержимого разрядов КСР). Очевидно, что $z_{max} = m_i - 1$. Рассмотрим равенство (5.17)

$$a_i + \beta_i = a_i' + \beta_i' = (a_i + m_i/2) + (\beta_i - m_i/2). \qquad (5.17)$$

В этом случае содержимое разрядов КСР соответствует $\lceil (m_i - 1)/2 \rceil$- ой строке (столбцу) матрицы табл. 5.5, рис. 5.14 и 5.15. Сдвиг содержимого разрядов

КСР будет производиться относительно величины $(m_i - 1)/2$, т.е. величина максимального количества сдвига содержимого разрядов КСР будет равна $(m_i - 1)/2$. Таким образом, максимальное значение ПОКС будет равно $z_{max} = (m_i - 1)/2$. Рассмотренные алгоритмы выполнения операции модульного сложения (вычитания) позволяют существенно повысить быстродействие выполнения модульных операций по сравнению с тем, что определяется выражением (5.15).

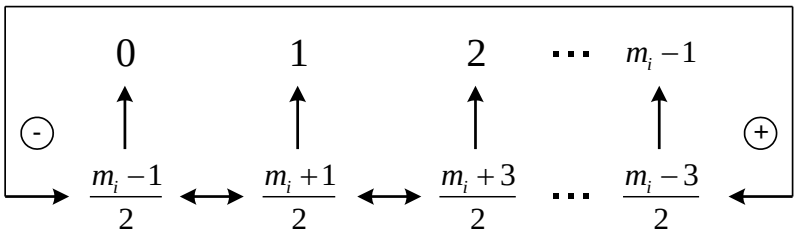


Рис. 5.14. Исходная информационная структура содержимого КРС для метода среднего значения (для произвольного модуля m_i МСС)

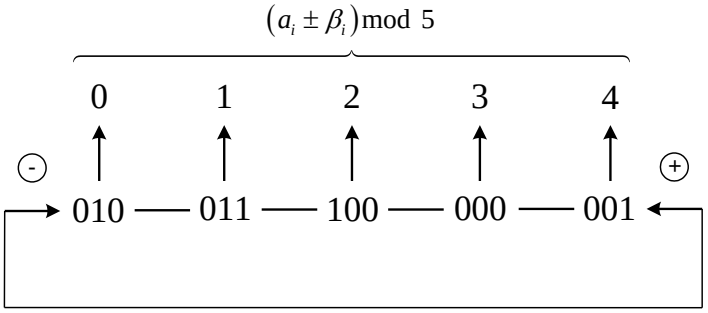


Рис. 5.15. Исходная информационная структура содержимого КРС для метода среднего значения $(m_i = 5)$

Современные системы обработки данных (СОД) при решении задач значительную часть своего полезного времени затрачивают на реализацию операции умножения. Операционное устройство СОД примерно половину времени своей работы "посвящают" реализации операции умножения и деления. Существует достаточно много методов, позволяющих "обойти" операцию деления (например, умножение первого операнда на обратную мультипликативную величину делителя), однако, замена операции умножения совокупностью однотипных операций сложения посредством КРС значительно снижает пользовательскую производительность обработки информации СОД. Поэтому при создании операционного

устройства (ОУ) в МСС важно синтезировать устройство для умножения, используя принцип кольцевого сдвига [119].

Функциональные схемы операционных устройств в МСС, синтезированные на основе предложенных методов, представлены на рис. 5.16 и 5.17.

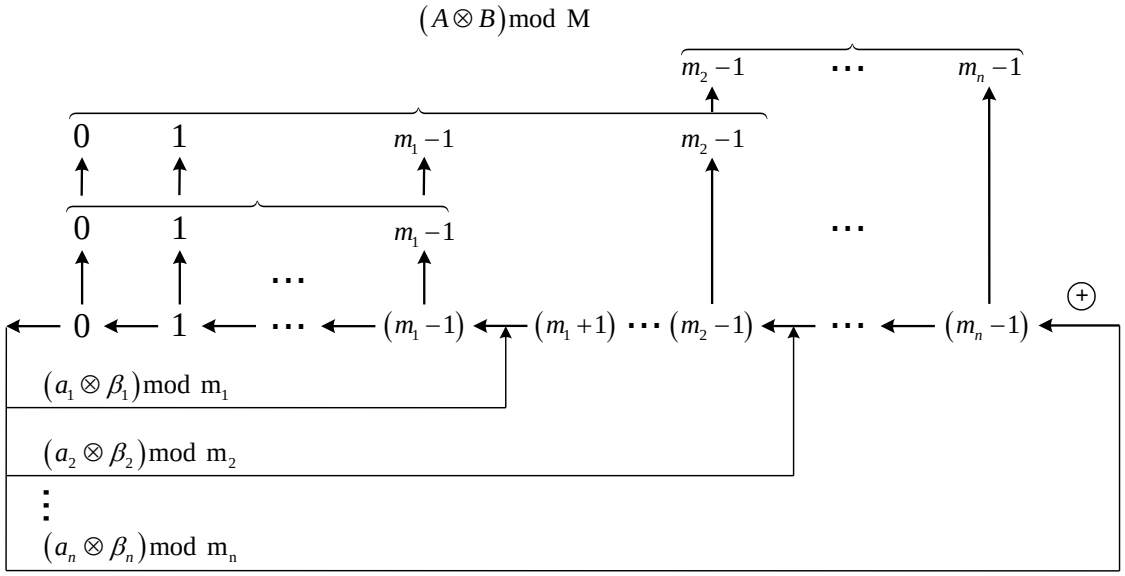


Рис. 5.16. Схема операционного устройства СОКИ в МСС

Метод остаточного сдвига**.** Рассмотрим метод, позволяющий определить результат $a_i\beta_i(\bmod m_i)$ операции модульного умножения посредством одного КРС. Для этого рассмотрим следующие два тождества:

$$\left\{a_i\beta_i(\bmod m_i)+\left[(m_i-a_i)\beta_i\right]\bmod m_i\right\}\bmod m_i\equiv 0(\bmod m_i); \qquad (5.18)$$

$$\left[(m_i-a_i)\beta_i\right]\bmod m_i\equiv m_i-a_i\beta_i(\bmod m_i). \qquad (5.19)$$

Тождества (5.18) и (5.19) отражают общий алгоритм реализации операции модульного сложения для определенных операндов, так, в частности, тождество (5.19) позволяет реализовать алгоритм модульного сложения $\left[a_i^{(1)}+\beta_i^{(1)}\right]\bmod m_i$ для операндов $a_i^{(1)}=0$, $\beta_i^{(1)}=\left[(m_i-a_i)\beta_i\right]\bmod m_i$. Из тождества (5.19) следует тождество

$$a_i\beta_i(\bmod m_i)\equiv m_i-\left[(m_i-a_i)\beta_i\right]\bmod m_i \qquad (5.20)$$

Из тождества (5.20) получим следующий алгоритм определения результата операции $a_i\beta_i(\bmod m_i)$:

– фиксируется нулевой разряд исходного состояния (нулевая строка таблицы 5.6) КРС;

– содержимое КРС сдвигается в положительном направлении на $\left[(m_i - a_i)\beta_i\right] \bmod m_i$ разрядов;

– содержимое нулевого разряда КРС инвертируется по модулю m_i, т.е. $m_i - \left[(m_i - a_i)\beta_i\right] \bmod m_i$.

Таблица 5.6

Таблица значений $(a_i\beta_i) \bmod 5$

β_i	a_i				
	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Сущность метода остаточного сдвига заключается в использовании алгоритмов выполнения операции модульного сложения при использовании тождеств (5.18) - (5.20). Несомненными достоинствами рассмотренного метода являются: однородность структуры реализации модульных операций сложения, вычитания и умножения; приемлемое время (сравнимое со временем реализации операции модульного сложения) выполнения операции модульного умножения; алгоритмическая простота реализации данного метода. К существенному недостатку метода остаточного сдвига следует отнести сложность технической реализации алгоритма определения результата операции модульного умножения, так как необходимость определения величины сдвига КРС, т.е. величины $\left[(m_i - a_i)\beta_i\right] \bmod m_i$ требует дополнительно существенного количества оборудования. Исходя из вышеиз-

ложенного материала, структурные схемы вычислений в МСС могут быть представлены в виде рис. 5.17 и 5.18.

Метод множеств контуров. Рассмотрим вариант реализации операции модульного умножения - вариант множества контуров (ВМК). В этом случае используется один КСР, посредством которого и определяется результат модульного сложения (вычитания) $(a_i \pm \beta_i) \bmod m_i$, а ОКС для операции модульного умножения представляется в виде $k_{ij}^{(z_i)}$, где i – номер контура, в котором производится сдвиг содержимого разрядов КСР ($i = \overline{1,n}$); n – количество контуров, по которым производится сдвиги содержимого разрядов КСР ($n = m_i - 1$); j – номер устанавливаемой строки матрицы значений $a\beta(\bmod m_i)$ (индекс i для операндов a, β опускается), $j = \overline{1,n}$; z_i – ПОКС, обозначающий количество сдвигов содержимого разрядов КСР в данном i-ом контуре ($z_i = \overline{0, m_i - 2}$). Сущность ВМК состоит в том, что по значению второго β операнда устанавливается β-ая строка таблицы 5.6 значений $a\beta(\bmod m_i)$ путем сдвига содержимого разрядов КСР по отдельным контурам (отдельным модулям m_i, причем, $m_i = i + 1$, так как минимальный (первый) модуль равен двум, т.е. $m_1 = 2$). Так как нулевая строка таблицы значений $a\beta(\bmod m_i)$ не устанавливается ($j \neq 0$), то $j = \overline{2,n}$. Вместе с тем, первый разряд КСР устанавливается одновременно со вторым и, таким образом, $i = \overline{2,n}$. Нулевой разряд КСР участия в реализации ВМК не принимает, так как операция умножения на нуль $(a = 0,\ \beta = 0)$ проще организуется по отдельному алгоритму, например, путем вывода входных нулевых шин операндов a, β непосредственно на нулевой выход устройства. Установление значения содержимого разрядов КСР проводится последовательно, начиная с $(m-1)$- го (старшего) разряда и до второго включительно, т.е. справа налево (рис. 5.17, 5.18).

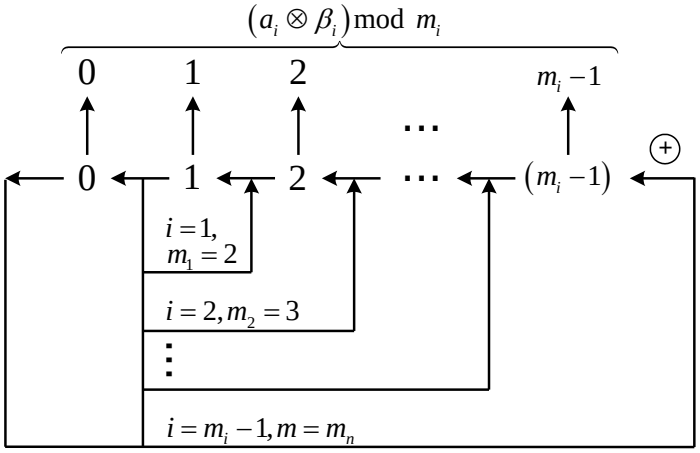


Рис. 5.17. Алгоритм реализации обобщенной арифметической операции для произвольного модуля m_i МСС

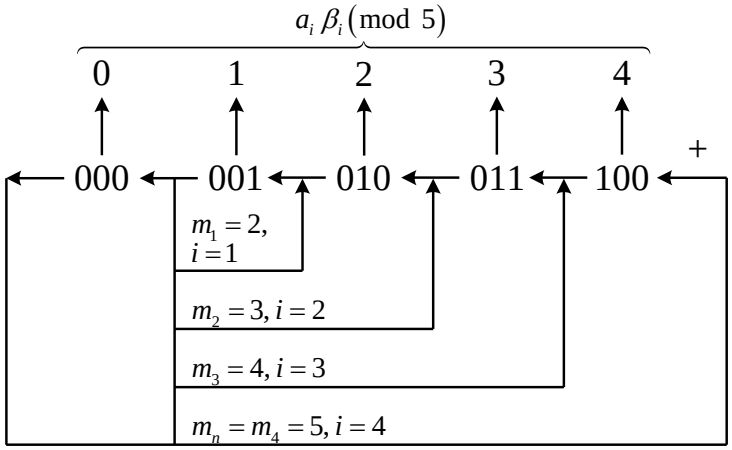


Рисунок 5.18. Алгоритм реализации операции модульного умножения для $m_i = 5$

Введем понятие обобщенного оператора кольцевого сдвига (ООКС), представленного в виде матрицы $\left\{k_{ij}\right\} = \left\{k_{ij}^{(z_{ij})}\right\}$, где показатель обобщенного оператора кольцевого сдвига (ПООКС) z_{ij} означает количество сдвигов содержимого разрядов КСР в i-ом контуре при установлении j-ой строки матрицы значений модульного произведения $a\beta(\bmod m_i)$. Таким образом, ООКС $\left\{k_{ij}\right\}$ будет состоять из набора $(m_n - 2) - x$ ОКС и может быть разложен либо по строкам k_j $\left(j = \overline{2,n}\right)$, либо по контурам k_i $\left(i = \overline{2,n}\right)$ в виде

$$\left\{k_{ij}\right\} = k_j = \left(k_{2j}^{(z_{2j})}\ k_{3j}^{(z_{3j})}\ \ldots\ k_{nj}^{(z_{nj})}\right), \tag{5.21}$$

$$\left\{k_{ij}\right\} = k_i = \left(k_{i2}^{(z_{i2})}\ k_{i3}^{(z_{i3})}\ \ldots\ k_{in}^{(z_{in})}\right). \tag{5.22}$$

Исходя из записи ООКС $\left\{k_{ij}\right\}$ в виде (5.21), можно определить по строкам временную матрицу $\left\{T_j\right\}$ в виде:

$$\left\{T_j\right\} = \begin{vmatrix} z_{22}\ z_{32}\ \ldots\ z_{n2} \\ \vdots \\ z_{2n}\ z_{3n}\ \ldots\ z_{nn} \end{vmatrix}.$$

Время t_j установления j-ой строки матрицы (время реализации операции) значений $a\beta\left(\mathrm{mod}\ m_i\right)$ равно сумме ПОКС для j-ой строки матрицы (5.24), умноженной на величину $k \cdot \tau$ (см. (5.15))

$$t_j = \sum_{i=2}^{n} z_{ij} k\tau. \tag{5.23}$$

Очевидно, что $t \approx t_j$. Время t реализации модульной операции умножения можно также определить, исходя из выражения (5.22). Действительно, в этом случае временная матрица $\left\{T_i\right\}$ по контурам будет совпадать с транспонированной матрицей

$$\left\{T_i\right\} = \left\{T_j\right\}^T = \begin{vmatrix} z_{22}\ z_{32}\ \ldots\ z_{n2} \\ \vdots \\ z_{2n}\ z_{3n}\ \ldots\ z_{nn} \end{vmatrix}, \tag{5.24}$$

а время установления j-ой строки матрицы значений табл. 5.7 равно сумме ПООКС для j-го столбца матрицы (5.24), умноженной на величину $k \cdot \tau$. Очевидно, что в общем случае время t реализации модульной операции $a\beta\left(\mathrm{mod}\ m_i\right)$ (как для операции модульного сложения и вычитания) зависит от величины операнда β (от номера j устанавливаемой строки), т.е.

$$t_{j\min} \le t \le t_{j\max}. \tag{5.25}$$

Исходя из выражения (5.25), целесообразно оперировать также средним $t_{ср}$ и максимальным t_{max} временем реализации модульных операций

$$t_{max}^{(x)} = \sum_{i=2}^{n} t_{ij\,max}\,, \tag{5.26}$$

$$t_{ср}^{(x)} = \sum_{j=2}^{n} t_j \big/ (n-1). \tag{5.27}$$

В соответствии с выражением (5.23) представим формулы (5.26), (5.27) в виде

$$t_{max}^{(x)} = k\tau(m_i - 1)m_i/2, \tag{5.28}$$

$$t_{ср}^{(x)} = k\tau\sum_{i=2}^{n}(m_i - 1)/2, \tag{5.29}$$

а для операции сложения (вычитания) формула (5.15) представится в виде

$$t_{max}^{(+)} = k\tau(m_i - 1); \tag{5.30}$$

$$t_{ср}^{(+)} = k\tau\sum_{i=2}^{n}(m_i - 1)/n, \tag{5.31}$$

Отметим, что в каждом из контуров можно применить вышеописанные алгоритмы сокращения времени установления нужной строки таблицы данной модульной операции. В этом случае результат операции модульного умножения будет определяться за меньшее время, чем в случае использования выражений (5.23), (5.28) и (5.29).

В качестве примера проведем сравнительный анализ времени реализации арифметических операций в ПСС и в МСС для одно -$(l=1)$ и четырехбайтового $(l=4)$ машинного слова. Для $l=1(\rho=8)$ МСС может представляться набором следующих оснований: $m_1=3,\ m_2=4,\ m_4=5,\ m_4=7$, а для $l=4(\rho=32)$ имеем набор оснований:

$$m_1=2,\ m_2=3,\ m_3=5,\ m_4=7,\ m_5=11,\ m_6=13,\ m_7=17,\ m_8=19,\ m_9=23,\ m_{10}=29.$$

Отметим, что время реализации арифметических операций в МСС, по принципу кольцевого сдвига, определяется временем реализации данной модульной операции для максимального по величине модуля m_n МСС, т.е. для $l=1$ – это модуль $m_n = m_4 = 7$, а для $l=4$ – $m_n = m_{10} = 29$. В соответствии с вышеприведенными формулами рассчитаем максимальное и среднее время для реализации арифметических операций в МСС без применения разработанных в разделе алгоритмов их ускорения (табл. 5.17).

Рассмотрим пример расчета времени выполнения операции модульного умножения при $m_n = 5$. В соответствии с выражением (5.21), ООКС для $m_n = 5$, можно представить в виде

$$\left\{k_{ij}\right\} = \left(k_{2j}^{(z_{2j})}\ k_{3j}^{(z_{3j})}\ k_{4j}^{(z_{4j})}\right). \qquad (5.32)$$

В общем виде ООКС разложим по строкам и контурам в следующем виде.

По строкам

$$j=2,\ k_2 = \left\{k_{22}^{(z_{22})}\ k_{32}^{(z_{32})}\ k_{42}^{(z_{42})}\right\},$$

$$j=3,\ k_3 = \left\{k_{23}^{(z_{23})}\ k_{33}^{(z_{33})}\ k_{43}^{(z_{43})}\right\},$$

$$j=4,\ k_4 = \left\{k_{24}^{(z_{24})}\ k_{34}^{(z_{34})}\ k_{44}^{(z_{44})}\right\}.$$

По контурам

$$i=2,\ k_2 = \left\{k_{22}^{(z_{22})}\ k_{23}^{(z_{23})}\ k_{24}^{(z_{24})}\right\},$$

$$i=3,\ k_3 = \left\{k_{32}^{(z_{32})}\ k_{33}^{(z_{33})}\ k_{34}^{(z_{34})}\right\},$$

$$i=4,\ k_4 = \left\{k_{42}^{(z_{42})}\ k_{43}^{(z_{43})}\ k_{44}^{(z_{44})}\right\}.$$

На основании соотношения (5.32) ООКС для, соответственно, второй $(j=2)$, третьей $(j=3)$ и четвертой $(j=4)$ строк будет иметь следующий вид:

$$k_2 = \left\{k_{22}^{(0)}\ k_{32}^{(2)}\ k_{42}^{(3)}\right\},$$

$$k_3 = \left\{k_{23}^{(1)}\ k_{33}^{(2)}\ k_{43}^{(2)}\right\},$$

$$k_4 = \left\{k_{24}^{(1)}\ k_{34}^{(1)}\ k_{44}^{(1)}\right\}.$$

Общий алгоритм образования ООКС для $m_n = 5$ представлен в таблице 5.7 (см. рис. 5.18).

Таблица 5.7

Алгоритм реализации модульной операции умножения в МСС

Номер строки матрицы $j=\beta=\overline{2,4}$	Номер контура $i=\overline{2,4}$	ПОКС z_{ij}	Содержимое строки матрицы: Исходное содержимое КСР					ОКС $(z_i)\,k_{ij}$	ООКС $\{k_{ij}\}$
			0	1	2	3	4		
j=2	i=4	$z_{42}=3$	0	2	3	4	1	$k_{42}^{(3)}$	$k_2=\{k_{22}^{(0)}k_{32}^{(2)}k_{42}^{(3)}\}$
			0	3	4	1	2		
			0	4	1	2	3		
	i=3	$z_{32}=2$	0	1	2	4	3	$k_{32}^{(2)}$	
			0	2	4	1	3		
	i=2	$z_{22}=0$	0	2	4	1	3	$k_{22}^{(0)}$	
j=3	i=4	$z_{43}=2$	0	2	3	4	1	$k_{43}^{(2)}$	$k_3=\{k_{23}^{(1)}k_{33}^{(2)}k_{43}^{(2)}\}$
			0	3	4	1	2		
	i=3	$z_{33}=2$	0	4	1	3	2	$k_{33}^{(2)}$	
			0	1	3	4	2		
	i=2	$z_{23}=1$	0	3	1	4	2	$k_{23}^{(1)}$	
j=4	i=3	$z_{44}=1$	0	2	3	4	1	$k_{44}^{(1)}$	$k_4=\{k_{24}^{(1)}k_{34}^{(1)}k_{44}^{(1)}\}$
	i=3	$z_{34}=1$	0	3	4	2	1	$k_{34}^{(3)}$	
	i=2	$z_{24}=1$	0	4	3	2	1	$k_{24}^{(1)}$	

Определим время t_j установления j- ой строки табл. 5.7 в соответствие с выражением (5.26): $t_2=15\tau$, $t_3=13\tau$, $t_4=9\tau$ $\left(k=\left[\log_2(m_i-1)+1\right]=3\right)$. Отметим, что в соответствие с выражением (5.28) максимальное время установления j-ой строки

равно: $t_{max}^{(x)}=30\tau\left(t_{ср}^{(x)}=13,5\tau\right)$. Данное обстоятельство подтверждает эффективность использования ПКС.

5.5 Методы реализации модульных операций, основанные на табличном принципе

В ПСС выполнение арифметической операции предполагает последовательную обработку разрядов операндов по правилам, определяемым содержанием данной операции, и не может быть закончено до тех пор, пока не будут последовательно определены значения всех промежуточных результатов с учетом всех связей между разрядами. Таким образом, ПСС, в которых представляется и обрабатывается информация в современных вычислительных машинах, обладают существенным недостатком – наличием межразрядных связей, которые накладывают свой отпечаток на методы реализации арифметических операций, усложняют аппаратуру и ограничивают быстродействие. Поэтому представляется естественным поиск возможностей применения такой арифметики, в которой бы поразрядные связи отсутствовали. В этом плане обращает на себя внимание система счисления в остаточных классах. Модульная система счисления (МСС) обладает ценным свойством независимости друг от друга остатков по принятой системе оснований. Эта независимость открывает широкие возможности в построении не только новой машинной арифметики, но и принципиально новой схемной реализации СОД, которая в свою очередь заметно расширяет применение машинной арифметики. Система счисления в большей степени влияет на структуру операционного устройства СОД [134-136]. Поиск путей одновременного повышения производительности обработки информации и надёжности функционирования СОД реального времени привел к необходимости разработки табличного метода реализации модульных операций, основанного на использовании ТП.

В общем случае табличное ОУ СОД для реализации арифметических операций (которые реализуется в унитарном коде) представляет собой двухвхо-

довое ПЗУ. Для каждого из входов количество входных шин для l-байтовой (8l двоичных разряда) СОД равно 2^{8l}. При этом общее количество логических схем совпадения “И” в узлах ПЗУ (которое в основном и определяет общее количество оборудования табличного ОУ СОД) равно $N_{1\ ПСС} = 2^{8l} \times 2^{8l} = 2^{16l}$. Исходя из формулы, очевидно, что табличная реализация целочисленных модульных арифметических операций в ПСС целесообразна только для значения l=1. Действительно, в этом случае $N_1 = 2^{16} = 65536$, что является приемлемым количеством оборудования для современного развития элементной базы. Однако, как отмечалось выше, тенденция развития средств обработки цифровой информации направлена на увеличение длины разрядной сетки СОД. Уже сейчас предлагается к практическому использованию СОД для l=2. В этом случае $N_{4ПСС}=2^{32}\times2^{32}=2^{64}$ и $N_{8ПСС}=2^{64}\times2^{64}=2^{128}$. Если учесть, например, что 2^{32}=4294967296, 2^{64}=18446744073709551616, а $2^{128}\approx3{,}4\times10^{38}$, то очевидно, что табличный метод реализации арифметических операций в ПСС практически не применим.

Положительные результаты могут быть получены, если рассмотреть СОД в МСС. Действительно, в общем случае, при реализации алгоритмов модульной обработки информации для табличного ОУ СОД, необходимо $N_{lСОК} = \sum_{i=1}^{n} m_i^2$ схем совпадения. Тогда для СОД в СОК с l=4 и l=8 соответственно имеем $N_{4СОК}$=2397 и $N_{8СОК}$=13275, что вполне приемлемо при реализации арифметических операций сложения, вычитания и умножения в МСС, используя современную элементную микроэлектронную базу (СБИС, ПЛМ или ПЛИС).

Вышеизложенное обстоятельство подтверждает важность, целесообразность и эффективность проведения практических исследований и разработки табличного метода реализации модульных операций в МСС [136,138,139].

Достоинства метода табличной реализации модульных операций состоят в следующем:

- высокая надежность, (операции реализуются в виде компактных ПЗУ; и. таким образом, весь тракт ОУ СОД строится по блочному принципу, что улучшает

ремонтопригодность СОД (уменьшается время восстановления $T_в$));

- простота табличных схем и дешифраторов, имеющих количество выходов, соответствующих значению оснований МСС;

- высокое быстродействие (результат операции может быть получен в момент поступления входных операндов, т.е. в один такт; время выполнения арифметических операций в МСС сравнимо с тактовой частотой вычислителя, что принципиально невозможно для позиционных вычислительных машин при существующей элементной базе).

Поиск путей упрощения структуры СОД обусловил необходимость построения алгоритмов реализации модульных операций, позволяющих повысить эффективность применения табличной арифметики.

Пусть задана пара операндов $A=(a_1,...,a_n)$ и $B=(b_1,...,b_n)$ в МСС с попарно взаимно простыми основаниями $m_1,\ldots,m_n$. Необходимо реализовать в табличном варианте обобщенную модульную операцию $(A \otimes B) \bmod M$. В соответствии с правилами выполнения арифметических операций каждой паре остатков a_i и b_i ставится в соответствие величина $(a_i \otimes b_i) \bmod m_i$. Таким образом, весь машинный тракт вычислительной операции $(A \otimes B) \bmod M$ можно представить в виде n независимых однотипных ПЗУ.

В дальнейшем рассмотрим эффективные методы сжатия табличных структур на основе использования планарной симметрии.

Рассмотрим процедуру реализации операции модульного умножения. Составим таблицу из числовых значений $a_i b_i (\bmod m_i)$. Эта таблица симметрична относительно диагоналей, вертикали и горизонтали, проходящих между числами $\frac{(m_i - 1)}{2}$ и $\frac{(m_i + 1)}{2}$. Симметричность относительно вертикали и горизонтали определяется из условия кратности суммы симметричных чисел:

$$a_i b_i + a_i (m_i - b_i) \equiv 0 (\bmod m_i),$$

$$a_i b_i + b_i (m_i - a_i) \equiv 0 (\bmod m_i).$$

Чтобы восстановить таблицу модульного умножения $a_i b_i (\mathrm{mod}\, m_i)$, достаточно иметь числовую информацию только ее восьмой части. Отсюда возникает возможность сократить таблицу (количество схем совпадения ПЗУ) модульного умножения. Отметим, что уменьшение таблицы в восемь раз приводит к необходимости производить предварительный анализ величин входных операндов a_i и b_i. Это обуславливает необходимость увеличения времени реализации операции. Вследствие этого, для реализации операции $a_i b_i (\mathrm{mod}\, m_i)$ представляется наиболее эффективным применение методов специального кодирования, позволяющих в четыре раза уменьшить таблицу модульного умножения. Для решения поставленной задачи возможны различные представления специальных кодов. Рассмотрим вариант реализации операции модульного умножения посредством кода табличного умножения (КТУ).

Пусть даны входные операнды a_i и b_i. Значения a_i (b_i), лежащие в диапазоне $\left[0, \frac{m_i - 1}{2}\right)$, могут быть закодированы произвольным образом, а значения a_i (b_i), лежащие в диапазоне $\left[\frac{m_1 + 1}{2}, m_i - 1\right)$, кодируются, как $m_i - a_i(m_i - b_i)$. Для отличия диапазонов вводится индекс γ_a (γ_b), определенный следующим образом [120]:

$$\gamma_a, \gamma_b = \begin{cases} 0, \text{если } 0 \le a_i (b_i) \le \dfrac{m_i - 1}{2}, \\ 1, \text{если } \dfrac{m_i + 1}{2} \le a_i (b_i) \le m_i - 1. \end{cases}$$

Метод определения результата операции модульного умножения, посредством код табличного умножения, следующий [120,132,137]: если заданы два операнда в КТУ $a_i = (\gamma_a, a_i')$, $b_i = (\gamma_b, b_i)$, то для, того чтобы получить произведение этих чисел по модулю m_i, достаточно получить произведение $a_i' b_i' (\mathrm{mod}\, m_i)$ и инвертировать его обобщенный индекс γ_i в случае, если γ_a отлично от γ_b, т.е. $a_i b_i (\mathrm{mod}\, m_i) = (\gamma_i, a_i' b_i (\mathrm{mod}\, m_i))$,

$$\text{где } \gamma_i = \begin{cases} \overline{\gamma}_i, \text{если } \gamma_a \neq \gamma_b, \\ \gamma, \text{если } \gamma_a = \gamma_b. \end{cases}$$

До настоящего времени вопросы эффективной реализации посредством КТУ, арифметических операций сложения и вычитания не освещены. Основная трудность заключается в том, что довольно сложно синтезировать алгоритмы модульных операций в связи с тем, что таблицы выполнения модульных операций различны по своей цифровой структуре.

Однако совершенно иные результаты можно получить, введя понятие специального кода табличного представления операндов (СКТПО) и исследуя возможности реализации одной модульной операции посредством таблицы, реализующих ей обратную операцию [120].

При исследовании цифровых свойств таблиц модульных операций сложения и вычитания доказано соотношение

$$\left[\left(\gamma_a, a_i'\right) + \left(\gamma_\beta, b_i'\right)\right] + \left\{\left[m_i - \left(\gamma_a, a_i'\right)\right] - \left(\gamma_\beta, b_i'\right)\right\} = 0 \left(\operatorname{mod} m_i\right), \qquad (5.33)$$

где $a_i = \left(\gamma_a, a_i'\right)$, $b_i = \left(\gamma_b, b_i'\right)$ – остатки, представленные в СКТПО.

Запишем выражение (5.33) в виде

$$\left(\gamma_a, a_i'\right) + \left(\gamma_b, b_i'\right) = m_i - \left\{\left[m_i - \left(\gamma_a, a_i'\right)\right] - \left(\gamma_b, b_i'\right)\right\}. \qquad (5.34)$$

Из выражения (5.34) следует, что для получения результата операции модульного сложения, посредством СКТПО, достаточно знать результат модульного вычитания, т.е. возникает возможность эффективно (с точки зрения уменьшения оборудования ПЗУ) использовать СКТПО для реализации модульных операций сложения и вычитания.

Разработаем метод выполнения операции модульного сложения посредством таблиц, реализующих операцию модульного вычитания (рис. 5.19), в соответствии с выражением (5.34).

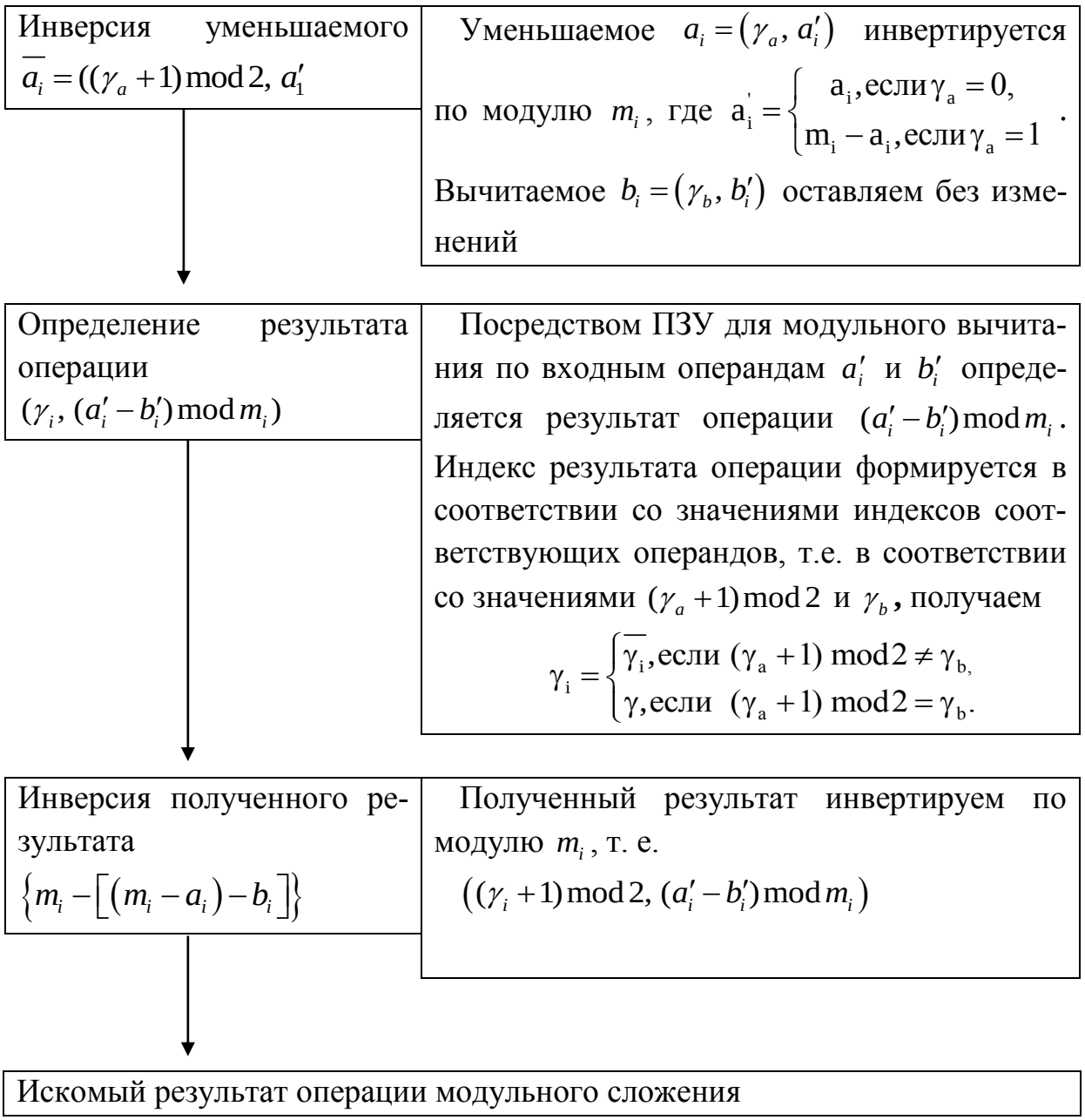


Рис. 5.19. Метод выполнения операции модульного сложения посредством таблиц, реализующих операцию модульного вычитания

Полученный метод схематично можно представить в виде

$$(a_i - b_i) \to [(m_i - a_i) - b_i] \to \{m_i [(m_i - a_i) - b_i]\} \to (a_i + b_i).$$

Таким образом, несмотря на различие цифровой структуры таблиц модульных операций сложения, вычитания и умножения создан новый табличный метод для реализации арифметических операций в МСС, посредством СКТПО. С помо-

щью этого метода можно построить конструктивно простое и высоконадежное ОУ СОД. Код табличного умножения приобрел, новые качественные свойства и стал СКТПО для реализации арифметических операций в МСС.

Рассмотрим вариант упрощения табличного метода.

Из выражения (5.33) следует

$$(\gamma_a, a_i') - (\gamma_b, b_i') = \left\{(\gamma_a, a_i') + \left[m_i(\gamma_b, b_i')\right]\right\}, \qquad (5.35)$$

т.е. можно определить результат операции модульного вычитания посредством ПЗУ, реализующего операцию модульного сложения (рис. 5.20).

Рис. 5.20. Метод выполнения операции модульного вычитания посредством таблиц, реализующих операцию модульного сложения

Схематично этот метод может быть представлен в виде

$$(a_i + b_i) \rightarrow \left[a_i + (m_i - b_i)\right] \rightarrow (a_i - b_i).$$

Второй метод (рис. 5.20) позволяет за меньшее время и с меньшими аппаратурными затратами, по сравнению с первым методом (рис.5.19), реализовать заданную в СОК арифметическую операцию вычитания. Несмотря на различие в

цифровой структуре таблиц модульных операций $(a_i \otimes b_i) \bmod m_i$, разработанные методы позволяют сократить на (60-70)% количество оборудования ОУ СОД. Это достигается за счет использования всего по 0,25 части каждой из таблиц ПЗУ, что раньше предполагалось возможным только для операции модульного умножения.

Рассмотрим примеры конкретной реализации арифметических операций в СОК для m_i=5. В этом случае, для табличного метода таблицы реализации модульных операций представлены в табл. 5.8 – 5.16.

Таблица 5.8

Специальный код табличного представления операндов

a_i	СКТПО		a_i	СКТПО	
	γ_a	a_i'		γ_a	a_i'
1	0	1	3	1	2
2	0	2	4	1	1

Таблица 5.9

Таблица модульного умножения

a_i / b_i	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Таблица 5.10

Таблица модульного сложени**я**

a_i / b_i	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Таблица 5.11

Таблица модульного вычитания

a_i / b_i	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

Таблица 5.12

Коммутатор модульного умножения

a_i / b_i		1	2
		4	3
1	4	1	2
2	3	2	4

Таблица 5.13

Первый коммутатор модульного вычитания

b_i \ a_i		1	2
		4	3
1	4	0	1
2	3	4	0

Таблица 5.14

Второй коммутатор модульного вычитания

β_i \ a_i		2	1
		3	4
1	4	2	3
2	3	1	2

Таблица 5.15

Первый коммутатор модульного сложения

b_i \ a_i		1	2
		4	3
1	4	2	3
2	3	3	4

Таблица 5.16

Второй коммутатор модульного сложения

b_i \ a_i		2	1
		3	4
1	4	4	0
2	3	0	1

Таким образом, несмотря на различие цифровой структуры таблиц модульных операций сложения, вычитания и умножения, на основе использования СКТПО, создан новый табличный метод обработки информации. На его основе разработан оригинальный универсальный табличный алгоритм для реализации арифметических операций в МСС.

Таким образом, при выполнении посредством разработанного в диссертации табличного метода всех трех арифметических операций удалось сократить 75% оборудования коммутаторов, посредством которых реализуются данные операции. Это в свою очередь (как показали расчеты) в зависимости от длины машинного слова (величины разрядной сетки), позволило сократить на (50-60)% оборудования табличного операционного устройства в МСС. Отметим, что с увеличением длины разрядной сетки обрабатываемых данных, что характерно для современной тенденции реализации операций, выполняемых при формировании и обработке сигналов, эффективность применения предложенного табличного метода обработки информации существенно возрастает.

В таблице 5.17 представлены некоторые расчетные данные времени реализации модульных операций в МСС.

Из таблицы 5.17 видно, что применение метода кольцевого сдвига и метода табличной реализации, даже без применения алгоритмов повышения быстродействия выполнения модульных операций, позволяет уменьшить время реализации модульных арифметического операций в МСС. Отметим, что с увеличением величины] разрядной сетки СОД, что характерно для современных методов формирования и обработки сигналов, эффективность применения ТП в МСС возрастает. В таблице введены следующие обозначения. Операции, выполняемые с применением: табличного принципа - (I); (II) – на основе малоразрядных двоичных сумматоров в МСС; посредством принципа кольцевого сдвига (метод прямого сдвига – III; усовершенствованный метод –IV).

Таблица 5.17

Расчетные данные времени реализации модульных операций в МСС

l, m_n, k	t, $[\tau]$												
	ПСС		МСС										
			Сложение (вычитание)						Умножение				
	сложение (вычитание)	умножение	I	II	III	IV	V	VI	I	II	III	IV	V	VI
$l=1$, $(\rho=8)$, $m_n=7$, $k=3$.	15	128	2	5	21	12	6	3	2	18	63	23	30	6
$l=2$, $(\rho=16)$, $m_n=13$, $k=4$.	31	512	2	7	52	31	16	4	2	32	234	60	132	9
$l=3$, $(\rho=24)$, $m_n=19$, $k=5$.	47	1152	2	9	95	34	17	5	2	50	513	132	306	13
$l=4$, $(\rho=32)$, $m_n=29$, $k=5$.	63	2048	2	9	145	60	30	5	2	50	2030	298	756	30
$l=8$, $(\rho=64)$, $m_n=53$, $k=6$.	127	8192	2	11	318	155	45	6	2	72	6500	660	1200	64

Суть предложенного в диссертации табличного метода обработки информации заключается в реализации, на основе использования специального кода табличного представления операндов, совокупности модульных операций сложения, вычитания и умножения, действий и приемов, направленных на повышение быст-

родействия реализации операций, используемых при формировании и обработке сигналов, а именно (рис. 5.21):

Представление данных в МСС	Информация представляется и обрабатывается в МСС, за счет формирования остатков $\{a_i\}$, i=1, n, чисел от деления их на выбранную систему оснований $\{m_i\}$, путем формирования и использования СКТПО.
Оптимизация оснований (модулей) **{m_i}** МСС	Производительность повышается за счёт исключения из структурной схемы избыточного оборудования таблиц реализации модульных операций.
Формирование специального кода табличного представления входных операндов для l =1, 2, 3,4,8	Производительность повышается за счёт уменьшения количества логических элементов таблиц.
Формирование поразрядных табличных структур	На основе значений полных таблиц реализации арифметических операции, используя СКТПО, составляется n поразрядных таблиц.
Табличная (матричная) обработка информации	Производительность повышается за счет распараллеливания вычислений на уровне микроопераций.
Расчет, анализ и сравнительная оценка производительности обработки данных в МСС	Проводится расчет и сравнительный анализ производительности в МСС. С увеличением величины разрядной сетки эффективность применения данного метода возрастает.
Повышение производительности обработки данных	

Рис. 5.21. Метод поразрядной табличной реализации арифметических операций

- представление и обработка данных осуществляется на основании использования непозиционных кодовых структур в МСС;
- реализация арифметических операций, используемых при формировании и обработке сигналов, производится на основе табличного принципа реализации модульных операций.

Выводы к разделу 5

В пятом разделе диссертации решена **восьмая** задача исследования.

1. С целью повышения быстродействия процедур формирования и обработки сигналов в телекоммуникационных системах в разделе рассмотрены принципы технической реализации модульных операций в модулярной системе счисления. В данном разделе представлено три принципа технической реализации модульных операций в МСС: сумматорный, принцип кольцевого сдвига и табличный принцип.

2. На основе принципа кольцевого сдвига в разделе усовершенствован метод двоичного кодирования остатков. Основное преимущество усовершенствованого метода, по сравнению с ПСС, состоит в возможности достижения более высокого быстродействия обработки данных, чем при сумматорном методе.

3. На основе табличного принципа в разделе разработаны три метода табличной реализации модульных операций: метод сложения, метод вычитания и метод поразрядной табличной реализации арифметических операций с использованием специального кода табличного представления операндов.

4. Результаты расчета и сравнительного анализа времени реализации модульных операций в МСС, на основе использования табличного принципа показали следующее: при реализации операции модульного сложения (вычитания) с использованием табличного метода, в зависимости от величины l-байтового ($l = \overline{1,4,8}$) машинного слова, в 7,5 – 63,5 раза эффективнее, а для операции модульного умножения, в 64 - 4096 раз эффективнее по времени выполнения арифметических модульных операций, чем при использовании сумматорного метода в ПСС.

5. На основе разработанных и усовершенствованных в диссертации методов быстрой реализации модульных операций в разделе представлены алгоритмы для их реализации, в соответствии с которыми синтезирован класс средств обработки данных по формированию и обработке сигналов в телекоммуникационных системах, на которые получено 9 патентов Украины, что подтверждает мировую новизну и практическую значимость полученных в диссертации научных результатов работы.

Отметим, что с увеличением объема обрабатываемых данных, что характерно для современной тенденции развития телекоммуникационных систем, эффективность МСС в целях повышения быстродействия выполнения модульных операций, по сравнению с ПСС, существенно возрастает.

РАЗДЕЛ 6
ТЕОРЕТИЧЕСКИЕ И ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ УСОВЕРШЕНСТВОВАННОГО МЕТОДА ИНФОРМАЦИОННОГО ОБМЕНА В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Исследования показали, что требуемые показатели имитозащищенности, информационной скрытности и помехозащищенности радиоканала телекоммуникационной системы могут быть обеспечены за счет применения динамического режима функционирования радиоканала со сложными сигналами. Под динамическим режимом функционирования радиоканала будем понимать радиоканал, в котором формы излучаемых сигналов или их параметры изменяются с течением времени [107]. При динамическом режиме функционирования радиоканала соответствие бит источника сообщения - состояние радиоканала (например, разрешенные для излучения сигналы) изменяется с течением каждого временного интервала длительностью T по закону, определить который станция противодействия может с вероятностью, не превышающей допустимого значения.

В данном разделе будут рассмотрены возможности совместного обеспечения имитозащищенности и информационной скрытности при динамическом режиме функционирования радиоканала с использованием дискретных сигналов с заданными корреляционными, ансамблевыми, структурными свойствами.

6.1 Усовершенствованный метод информационного обмена на основе динамического использования сложных сигналов и классов сигналов с улучшенными свойствами

Определим условия смены соответствия m бит сообщения - 2^m сложных сигналов, при выполнении которых определение нарушителем правила смены соответствия возможно с вероятностью, не превышающей допустимой. Очевидно, что смена соответствия должна осуществляться с применением управляющей функции. Примером такой функции может быть управляющая последовательность

(УП) символов. И, если УП задается неким процессом, закон формирования выходной последовательности которого, является непредсказуемым, то в этом случае можно говорить о скрытности функционирования системы передачи информации на уровне источника сложных сигналов. Определим условия построения телекоммуникационной системы, использующей динамические принципы передачи, при которых обеспечивается абсолютная скрытность системы на уровне источника сигналов. При этом под абсолютной скрытностью будем понимать невозможность злоумышленника определить закон, по которому производится смена соответствия: бит сообщения – сложный сигнал.

На рисунке 1 представлена структурная схема передающей части системы, реализующей динамический режим функционирования радиоканала. Схема состоит из источника информации (ИИ), динамического модулятора (ДМ), устройства формирования управляющей последовательности (УФУП).

Пусть имеется некоторый источник информации, создающий в фиксированный момент времени одно из M возможных сообщений.

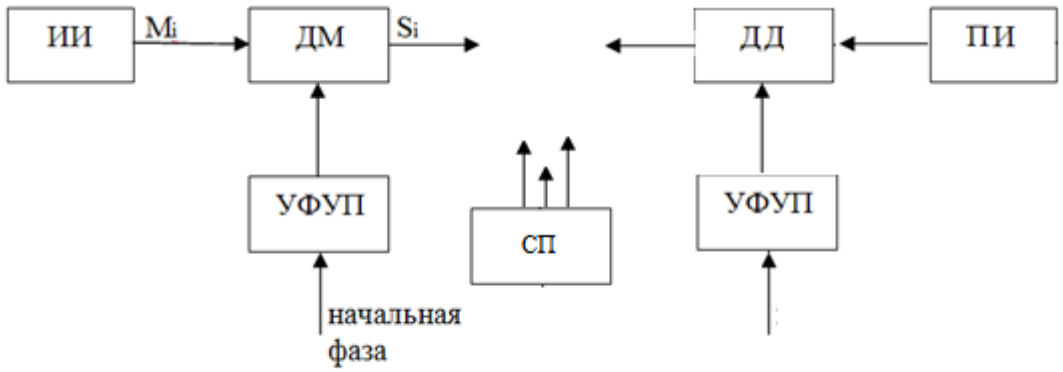


Рис. 6.1 Схема реализации динамического режима функционирования радиоканала

Каждое из M конкурирующих сообщений передается посредством сигнала: $S=\{S_i(t):i=1,2,\ldots M\}$. На число сигналов (или мощность множества S), не накладывается никаких ограничений и, если это необходимо, множество S может быть бесконечным. Модулятор обеспечивает формирование сложных сигналов, а демо-

дулятор приемной части системы (устройство обработки сложных сигналов) - их поиск, обнаружение и различение. Символы сообщения от источника информации, представленные в виде m бит, поступают в динамический модулятор, в котором в соответствии с символами управляющей последовательности (УП) устройства формирования управляющей последовательности (УФУП), осуществляется выбор 2^m из S сложных сигналов и таким образом устанавливается соответствие: m бит - 2^m сложных сигналов.

При появлении на входе динамического модулятора m бит сообщения в канал связи излучается сложный сигнал S_i, выбранный в зависимости от значения управляющей последовательности. По истечении времени T соответствие m бит - 2^m сложных сигналов изменяется по определенному закону (правилу).

Станция противодействия, осуществляющая наблюдение за каналом связи, может реализовывать различные стратегии воздействия на телекоммуникационную систему: перехват переданных сигналов и их анализ; попытки распознавания сигналов и определения закона их излучения; формирование и постановка помех с целью навязывания ложных сообщений и др.

В демодуляторе на станции приема производится различение одного из 2^m разрешенных информационных сигналов. После демодуляции на выходе демодулятора формируются m бит сообщения, которые поступают получателю сообщений.

Естественным представляется постановка ряда вопросов, на которые необходимо дать ответы при решении задачи синтеза метода динамической смены соответствия: m бит сообщения - 2^m сложных сигналов:

- насколько устойчива система против раскрытия закона установления соответствия m бит сообщения - 2^m сложных сигналов, если нарушитель не ограничен во времени и обладает всеми необходимыми средствами для анализа перехваченных сигналов;

- имеет ли для станции противодействия правило установления соответствия m бит сообщения - 2^m сигналов единственное решение, и если нет, - сколько приемлемых решений возможно;

- какой объем данных (число элементов физического переносчика информации, - сигнала) необходимо перехватить станции противодействия, для того, чтобы решение стало единственно верным;

- существуют ли системы, в которых невозможно принять единственное правильное решение независимо от того, каков объем перехваченного в канале наблюдения.

Исследования показали [93-94,107], что при реализации в телекоммуникационной системе динамического режима функционирования, когда, в общем случае, соответствие m- бит - 2^m сложных сигналов изменяется с течением времени, появляется возможность комплексного обеспечения требуемых показателей помехо- и имитозащищенности, а также информационной скрытности функционирования системы.

Информационная скрытность передаваемых в системе сообщений может быть реализована на дискретном уровне (на физическом уровне), на уровне источника сигналов, или дискретном уровне (на физическом уровне) и уровне источника сигналов одновременно. При выполнении определенных условий, которые будут сформулированы в настоящем разделе, информационная безопасность системы, осуществляемая на уровне источника сообщений, может быть обеспечена с показателями не ниже, чем на дискретном уровне. При этом, на уровне источника сигналов обеспечивает более высокие показатели по имитозащищенности.

В настоящем разделе сформулирована и решена задача обеспечения информационной безопасности (имитостойкости и информационной скрытности) телекоммуникационной системы на уровне источника сложных сигналов. Также приводятся в виде утверждений и следствий теоретические основы динамического режима функционирования радиоканала телекоммуникационной системы. При этом показано, что сформулированные и доказанные утверждения, являющиеся

теоретическим обобщением теории криптографической защиты данных, дают необходимые и достаточные условия теоретической информационной скрытности телекоммуникационной системы.

В данном разделе будут приведены результаты расчетов основных из рассматриваемых в работе показателей эффективности функционирования телекоммуникационной системы, в которой реализован динамический режим функционирования, а в качестве систем сложных сигналов используются нелинейные системы сигналов, методы синтеза которых получены в ходе диссертационных исследований.

Утверждение 6.1 Пусть каждым из m бит источника сообщений в интервале времени t ставится в фиксированное соответствие 2^m сложных сигналов, выбираемых из пространства сигналов {W} размерности K ≥2, тогда необходимым и достаточным условием обеспечения теоретической недешифруемости (теоретической информационной скрытности) на уровне источника сложных сигналов являются условия:

$$P(W_j/M_i) = P(W_j) \qquad (6.1)$$

$$P(W_j/W_{j-1}, W_{j-2}, \ldots\ldots W_k \ldots\ldots W_1) = P(W_j), \qquad (6.2)$$

где: - $P(W_j/M_i)$ – условная вероятность передачи W_j сигнала, при условии, что выбрано M_i сообщение; $P(W_j)$ – априорная вероятность передачи W_j сигнала.

Условия (6.1) и (6.2) означают, что вероятность выбора для передачи W_j сигнала не должна зависеть ни от передаваемых m- бит сообщения, ни от ранее переданных сигналов.

Необходимое условие (6.1) следует из формулы Байеса. Действительно, только в случае, когда станция противодействия при приеме сигналов W_j ($j = \overline{1,k}$), не может уточнить имеющиеся у него априорные вероятности на основе вычисления апостериорных вероятностей

$$P(M_i/W_j) = P(M_i)P(W_j/M_i)/P(W_j), \qquad (6.3)$$

криптоанализ с его стороны оказывается безрезультатным. Условие (6.1) является также и достаточным в виду того, что оно выполняется либо при $P(M_i) = 0$, либо при $P(W_j/M_i) = P(W_j)$. Выполнение условия $P(M_i) = 0$ означает отсутствие

сообщений на выходе источника. При условии $P(W_j/M_i) = P(W_j)$, криптоаналитик не получает при перехвате сигналов дополнительной информации о системе, и располагает только априорными сведениями о передаваемых сообщениях, поэтому количество информации, полученной им принятия сигналов, равно нулю, т.е.

$$I(M,W) = H(M) - Y(M/W) = H(M) - H(M) = 0, \quad (6.4)$$

что является достаточным условием обеспечения абсолютной информационной скрытности на уровне источника сложных сигналов. При выполнении условия (6.4) однозначное установление соответствия бит сообщения – сложный сигнал, может быть выполнено только с применением метода статистического опробывания всех возможных вариантов соответствия, т.е. методом перебора.

Для доказательства необходимого условия второй части утверждения 6.1 (выражение 6.2) будем полагать, что при его выполнении вероятность появления W_j сигнала не зависит от вероятности появления всех j-1 сигналов. Поэтому количество информации, содержащейся в сигнале W_j (после перехвата всех j-1 сигналов) равно

$$I(W_j, W_k) = H(W_j) - H(W_j/W_k) = H(W_j) - H(W_k), \quad (6.5)$$

где $k = \overline{1, j-1}$.

Из (6.2) так же следует равновероятность появления сигналов (равновероятность отображения: бит сообщения - W_i сигнал), поэтому

$$H(W_j) = H(W_k). \quad (6.6)$$

Условие (6.6) является также и достаточным, т.к. независимость и равновероятность появления сигналов означает и равновероятность появления управляющей последовательности, символы которой статистически независимы и асимптотически равновероятны.

Формулируемое ниже утверждение задает необходимые и достаточные условия обеспечения идеальной структурной скрытности сигналов на выходе источника.

Утверждение 6.2

Пусть словарь (ансамбль) {W} широкополосных сигналов обладает объемом N и числом символов L в каждом из словарей. Тогда, для обеспечения теоретической недешифруемости (абсолютной структурной скрытности) каждого из $W_i \in \{W\}$ сложных сигналов, необходимо и достаточно, чтобы

$$P\,(W_{\upsilon,k}) \;=\; P\left(W_{j,i}\right), \upsilon = \overline{1,L}, k = \overline{1,N} \qquad (6.7)$$

то есть, чтобы вероятность появления элемента $W_{j,i}$ сложного сигнала не зависела ни от элементов ранее переданных сигналов, ни от элементов $W_{j,\,i-1}$, $W_{j,i-2}$, …. $W_{j,\upsilon,\ldots\ldots}$ $W_{j,\,2}$ данного сигнала.

Необходимость условия (6.7) следует непосредственно из критерия теоретической недешифруемости – потенциальной структурной скрытности, т.е. только в случае, если

$$S = l/N = N/N = 1. \qquad (6.8)$$

Поэтому, по любому числу перехваченных символов сложного сигнала нельзя предсказать последующие N – l символов сигнала $W_{j,}$ так и всех сигналов W_υ ($\upsilon = \overline{1,N}$).

Условие (6.7) является и достаточным. Действительно, условная апостериорная энтропия относительно закона формирования W_j сигнала после перехвата не менее k символов в сигналах определяется из соотношения:

$$H\left(W_j / W_{v,k}\right) = \sum_{i=1}^{N} P\left(W_{j,i} / W_{v,k}\right) \log_2 P\left(W_{j,i} / W_{v,k}\right). \qquad (6.9)$$

Среднее значение условной апостериорной энтропии (закона формирования сигналов) есть:

$$H\left(W / W_j\right) = \sum_{j=1}^{v}\sum_{i=1}^{k} P\left(W_i\right) P\left(W_{j,i} / W_{v,k}\right) \log_2 P\left(W_{j,i} / W_{v,k}\right), \qquad (6.10)$$

и, с учетом (6.7), совпадает с априорной неопределенностью $H(\{W_j\})$ о источнике сигналов. Поэтому количество информации, получаемой станцией противодействия после проведения криптоанализа, определяется из выражения:

$$I\left[H\left[\{W\} / \{W_\upsilon\}\right] = H\left[\{W\}\right] - H\left[\{W\} / \{W_\upsilon\}\right] = H\left[\{W\}\right] - H\left[\{W\}\right] = 0. \qquad (6.11)$$

Из утверждений 6.1 - 6.2 вытекает ряд важных следствий, накладывающих ограничения на источник сигналов {W}.

Следствие 1. Закон формирования каждого из сигналов должен быть псевдослучайным, причем даже при перехвате N-1 из N символов не должно существовать единственного решения относительно его закона формирования, кроме статистического перебора всех возможных вариантов.

Следствие 2. Теоретически недешифруемым, с точки зрения закона формирования сигналов, является источник сигналов со случайным формированием всех сигналов, т.к. только в этом случае у станции противодействия отсутствует возможность получения регулярного решения о законе формирования сигналов.

Смена форм сложных сигналов позволяет улучшить показатели защищенности телекоммуникационной системы, в частности, защищенности от навязывания сигналов синхронизации, установления подлинности и полномочий, цифровой подписи и информационных сигналов. Как было показано в разделе 1, вероятность навязывания зависит от размерности (объема) используемых сложных сигналов и определяется из соотношения $P_{нав.} = \frac{1}{M}$.

При использовании в качестве физических переносчиков информации линейных рекуррентных последовательностей максимального периода с числом символов $L= 10^3$, объем системы M= 30. В случае применения нелинейных рекуррентных последовательностей с числом символов $L = 10^3$, M= 300. При применении в качестве сложных сигналов производных ортогональных нелинейных последовательностей при $L = 10^3$, $M= 10^6$. Вероятности навязывания одного изоморфизма сложного сигнала, т.е. сигнала, отличающегося «тонкой» структурой, и не являющегося циклически сдвигом сигнала, с одной попытки, соответственно равны $P_{нав} = 3{,}3\ 10^{-2}$; $P_{нав} = 3.3\ 10^{-3}$; $P_{нав} = 10^{-6}$.

При реализации динамического режима со сменой соответствий m бит сообщения - 2^m сигналов, если закон смены соответствий не может быть предсказан с вероятностью, не превышающей допустимую, обеспечивается также и информационная скрытность. При этом показатели информационной безопасности (ин-

формационной скрытности) зависят только от периода и статистических свойств генерируемой шифратором (устройством управления) гаммы управляющей (ГУ).

Принципы формирования и требования к свойствам ГУ рассмотрены в разделе 4. Значения показателей информационной безопасности (имитостойкости и информационной скрытности) телекоммуникационной системы, достигаемые при реализации динамического режима передачи информации и использовании сложных сигналов с необходимыми свойствами, будут рассмотрены в разделах 6.2 - 6.4.

6.2 Методология вероятностной оценки защищенности информации от навязывания ложных сообщений в телекоммуникационных системах

К основным механизмам обеспечения подлинности, целостности, аутентичности сообщений относят алгоритмы шифрования даннях, электронные цифровые подписи, коды аутентификации сообщений (MAC коды) и др. В данном разделе приведенна математическая постановка и решение задачи оценки показателей имитостойкости телекоммуникационной системы на основе применения кодов аутентификации сообщений (MAC кодов), а также для случая, когда в целях защищенности системы от ввода ложных сообщений применяются системы сложных сигналов с заданными корреляционными, ансамблевыми и структурными свойствами.

MAC код [65] - это функция отображения h: $K \times D \to R$, где $K = \{0,1\}^n$ – пространство ключей, $D = \{0,1\}^*$ – пространство сообщений, а $R = \{0,1\}^n$ – пространство MAC значений для $k,\ n \geq 1$. Для заданных значений ключа $k \in K$ и сообщения $X \in D$, функция производит MAC значения $Y \in R$.

Приведем определение и сформулируем предложения по обеспечению стойкости кодов аутентификации сообщений к различным атакам со стороны станции противодействия. Покажем возможность применения приведенных результатов

для обеспечения истинности и целостности сообщений на уровне источника сложных нелинейных дискретных сигналов.

Рассмотрим случай, когда злоумышленник может подделать сообщение для MAC h кода, если, не зная случайного ключа, он способен создать новое сообщение X и MAC значение Y такое, что $h(K, X) = Y$.

Введем определение: MAC код $h: K \times M \to R$ є $(t; \varepsilon; q)$ –- секретным, если, при случайно взятом ключе K, злоумышленник не может подделать новое сообщение за время t с вероятностью выше ε, даже если он (по своему выбору) имеет возможность получить q значений MAC кодов других сообщений.

В зависимости от информации, доступной злоумышленнику, различают следующие типы атак на коды аутентификации сообщений [56,89-90].

1. Атака с известным текстом. Злоумышленник имеет возможность исследовать некоторые открытые тексты и соответствующие им значения кода аутентификации сообщений.

2. Атака с выбранным текстом. Нарушитель имеет возможность выбирать наборы текстов и впоследствии получать значения кодов аутентификации сообщений, соответствующих выбранным текстам.

3. Атака с адаптивным выбором текста. Это наиболее общая атака, когда злоумышленник выбирает текст и немедленно получает соответствующие значения кода аутентификации сообщения.

4. Угадывания кода аутентификации сообщения (Guessing of the MAC). Это прямая атака на алгоритм MAC кода и заключается в выборе произвольного нового сообщения и, впоследствии, угадывания значение кода аутентификации сообщения. Она может быть выполнена следующими способами:

- угадывание ключа, с последующим вычисления значения MAC кода, с вероятностью успеха 2^{-n}, n- обозначает размер (в битах) значения MAC кода.

- угадывание ключа, с последующим вычисления значения MAC кода, с вероятностью успеха 2^{-k}, k – длина (в битах) секретного ключа.

Данный тип атаки не поддается проверке и, следовательно, нарушитель априорно не знает, верно ли он угадал значение MAC кода. Успех атаки (достижения ожидаемого результата) зависит от количества предпринимаемых попыток совершения атак.

Исчерпывающий поиск ключа (Exhaustive Key Search). Атака требует примерно k/n известных пар текст-MAC для фиксированного ключа. Пытаясь определить ключ, криптоаналитик перебирае один за другим все возможные ключи. Ожидаемое число испытаний, которое приведет к взлому MAC алгоритма, равно k/n . В отличие от предыдущей атаки, эту атаку можно осуществлять вне сеанса связи (off-line).

Подделка, основанная на внутренней коллизии (Internal Collision Based Forgery). Последствие этой атаки заключается в том, что если выявить внутреннюю коллизию (совпадение промежуточных результатов при вычислении значений MAC кодов), ее можно использовать для подделки MAC кода для отдельно выбранного текста.

Выполним оценку стойкости MAC кодов при имитации и подмене.

Анализ показывает, что с целью подмены сообщений, нарушитель должен сформировать сообщение x' и соответствующий сообщению аутентификатор $y' = f(x')$. Это может быть выполнено двумя способами: путем имитации и путем подмены .

В случае имитации нарушитель формирует аутентификатор $y = f(x)$, основываясь на априорных вероятностях распределений MAC значений и ключевых данных. Вероятность имитации будет определяться максимальной вероятностью того, что сформированный аутентификатор $y = f(x)$ является истинным:

$$\mathrm{P_{им}} = \mathrm{P}\left(\mathrm{y} = \mathrm{f}\left(\mathrm{x}\right) - \text{истинно}\right), \left(\mathrm{x}, \mathrm{y}\right) \in \mathrm{A} \times \mathrm{B},\ \mathrm{f} \in \mathrm{H}. \qquad (6.12)$$

При равно вероятном выборе ключа, что эквивалентно выбору $f \in H$, необходимо учитывать распределение MAC значений y для конкретного сообщения по ключевому пространству. Для вероятности имитации, обозначим ее как вероятность имитации по ключу $\mathrm{P_{имКл}}$, справедливо следующее выражение:

$$P_{\text{имКл}} = \frac{\left|\{f \in H : y = f(x)\}\right|}{|H|}, (x, y) \in A \times B \quad , \tag{6.13}$$

где $|\{f \in H : y = f(x)\}|$ - количество хеш-функций f, которые порождают для сообщения x значения MAC кода y.

Очевидно, что

$$P_{\text{имКл}} \geq \frac{1}{|H|} \tag{6.14}$$

Кроме того, все записи в столбцах массива MAC кодов встречаются одинаковое количество раз и, поэтому, имеем: $P_{\text{имКл}} \geq \frac{1}{|B|}$.

Поэтому верхняя граница вероятности имитации MAC кода по ключу определяется максимальным значением $P_{\text{им}Кл}$ на всем пространстве сообщений, а значение вероятности $P_{\text{им}Кл}$ определяется следующим соотношением:

$$P_{\text{имКл}_{x \in A}} \leq \max \frac{\left|\{f \in H : y = f(x)\}\right|}{|H|}, (x, y) \in A \times B. \tag{6.15}$$

Если не учитывать распределение MAC значений y для данного сообщения по ключевому пространству, тогда вероятность имитации обозначим как вероятность имитации по MAC значению $P_{\text{имMAC}}$. Имитация посредством навязывания MAC значения определяется тем, что из множества предполагаемых MAC кодов выбирается одно. Вероятность успеха будет определяться выражением:

$$P_{\text{имMAC}} = \frac{1}{\left|\{y \in B : y = f(x)\}\right|}, (x, y) \in A \times B. f \in H, \tag{6.16}$$

где $|\{y \in B : y = f(x)\}|$ – мощность множества возможных MAC значений для сообщения x.

Если MAC значения для сообщения x принимают полное множество значений $|B|$, получим

$$P_{\text{имМАС}} = \frac{1}{|B|}\ .$$

В общем случае справедлива такая нижняя граница:

$$P_{\text{имМАС}} \geq \frac{1}{|B|}. \qquad (6.17)$$

Если для сообщения известно статистическое распределение МАС значений, то оценка вероятности имитации по МАС значению сводится к оценке вероятности имитации по ключу. Верхняя граница для вероятности имитации по МАС значению будет определяться максимальным значением по всему пространству сообщений:

$$P_{\text{имМАС}} \leq \max \frac{1}{\left|\{y \in B : y = f(x)\}\right|}, y \in B.f \in H \cdot \qquad (6.18)$$

Атака подмены основана на том, что нарушитель наблюдает (x, y) и меняет его на (x', y'), где $x \neq x'$. Вероятность подмены определяться условной вероятностью:

$$P_{\text{под}} = P(f(x') = y' - \text{истинно} \,|\, f(x) = y), \quad (x,y), (x',y') \in A \times B, x \neq x', f \in H. \qquad (6.19)$$

Выражение для вероятности подмены с использованием формулы полной вероятности и статистики наблюдений будет выглядеть как:

$$P_{\text{под}} = \frac{\left|\{f \in H : y = f(x), y' = f(x')\}\right|}{\left|\{f \in H : y = f(x)\}\right|}, (x,y), (x', y') \in A \times B, x \neq x', f \in H. \qquad (6.20)$$

Верхняя граница вероятности навязывания путем подмены сообщений и МАС определяется максимальной вероятностью успеха для всех пар сообщений, но при условии ровно вероятного выбора ключа.

Анализ показывает, что возможны два случая, когда подмена сообщения x на x', если $x \neq x'$ осуществляется с тем же аутентификатором $y = y'$, (замена первого рода) и с разными $y \neq y'$ (подмена второго рода).

Вероятность замены при условии равенства $y = y'$ определяется вероятностью коллизии MAC кода и оценивается выражением:

$$P_{под1} \le P_{кол} = \max \frac{\left|\left\{f \in H : y = f(x), y' = f(x')\right\}\right|}{\left|\left\{f \in H : y = f(x)\right\}\right|}, (x,y),(x',y') \in A \times B, x \ne x', f \in H. \qquad (6.21)$$

Для вероятности замены второго рода имеем:

$$P_{под2} \le \max \frac{\left|\left\{f \in H : y = f(x), y' = f(x')\right\}\right|}{\left|\left\{f \in H : y = f(x)\right\}\right|}, (x,y),(x',y') \in A \times B, x \ne x', y \ne y', f \in H. \qquad (6.22)$$

Таким образом, для точного вычисления имитационной и коллизионной стойкости MAC кодов по приведенным формулам необходимо использовать статистику совместных распределений MAC кодов по ключам для истинных и поддельных сообщений. Для MAC кодов определение такой статистики выглядит проблематичным из-за очень большго размера массива возможных MAC. Нижние границы для вероятностей имитации и подмены не учитывают статистические свойства массивов аутентификаторов, и основываются на модели псевдослучайности функции f(x) и определяют минимальные требования к размеру ключевого пространства и пространства MAC значений.

Верхние границы для вероятностей имитации и подмены связанны с комбинаторными свойствами MAC массивов и оценивают значения коллизий в пространстве A x B для наихудшего случая выбора ключей и сообщений.

Рассмотрим коллизионные характеристики MAC кодов.

Под стойкостью к коллизиям понимают вычислительную сложность нахождения двух сообщений M_i и M_j таких, что [56]:

$$H(M_i) = H(M_j), \qquad (6.23)$$

где H есть соответствующим преобразования. В [56] приводятся оценки вероятности создания коллизий, причем считается, что для реализации коллизии необходимо выполнить не менее $\sqrt{n}$ экспериментов из общего количества возможных значений n.

Математическая постановка задачи вероятностной оценки коллизий формулируется следующим образом.

Пусть имеется некоторая функция преобразования H сообщения M

$$h = H(M), \tag{6.24}$$

где M - это сообщение произвольной длины l_M, причем h может принимать значения $n = 2^m$ независимо от длины l_M. Необходимо определить число случайных сообщений k, которые необходимо подать на вход преобразователя H, чтобы с вероятностью $P_з$ состоялось хотя бы одно совпадение вида (6.23), то есть произошла коллизия.

Оценка числа испытаний появления коллизий. Проведенный анализ показал, что при решении данной задачи имеет место выборка из k значений целочисленной случайной величины с равновероятным законом распределения, принимающей значения от 1 до $n = 2^m$, а $k \le n$. В этих условиях необходимо найти вероятность $P(n,k)$ того, что среди значений H(M) выборки, по крайней мере, две совпадают, то есть: $H(M_i) = H(M_j)$.

Для решения сформулированной задачи найдем вероятность того, что в группе из k событий не произойдет коллизия, то есть соотношение (6.23) не выполнится ни разу. Обозначим эту вероятность как $R(n,k)$. Понятно, что $P(n,k)$ и $R(n,k)$ составляют полную группу событий, то есть: $P(n,k) + R(n,k) = 1$, и

$$P(n,k) = 1 - R(n,k). \tag{6.25}$$

Далее найдем общее количество N различных способов, которыми можно получить k значений без повторений. Для первого элемента мы имеем n значений без повторений, для второго n-1, для третьего – n-2 и т.д., для k - го – (n-k+1). Поэтому общее число способов, при которых нет совпадений может быть рассчитано как :

$$N = n \cdot (n-1)(n-2)\ldots(n-k+1) = \frac{n!}{(n-k)!} \tag{6.26}$$

Поскольку при каждом из событий с одинаковой вероятностью может происходить каждое из событий, то общее число событий можно оценить как

$$N_{\sum} = n^k. \tag{6.27}$$

Вероятность отсутствия совпадений можно оценить отношением числа вариантов без совпадений (6.26) к общему числу вариантов (6.27), то есть:

$$R(n,k) = \frac{\frac{n!}{(n-k)!}}{n^k} = \frac{n!}{(n-k)!n^k}. \tag{6.28}$$

Используя выражение (4.38), получим:

$$P(n,k) = 1 - \frac{n!}{(n-k)!n^k}. \tag{6.29}$$

Выражение (4.42) может быть использовано для оценки искомой вероятности, однако желательно получить общее решение уравнения (6.29), например, для значения k . С этой целью представим $P(n,k)$ в виде:

$$P(n,k) = 1 - \frac{n(n-1)\ldots(n-k+1)}{n^k} = 1 - \left[\frac{n-1}{n}\,\frac{n-2}{n}\ldots\frac{n-k+1}{n}\right] =$$

$$= 1 - [\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)\ldots\left(1-\frac{k-1}{n}\right)]. \tag{6.30}$$

Далее воспользуемся тем, что для всех $1 > x \geq 0$ [56] справедливым является:

$$(1-x) \leq e^{-x}. \tag{6.31}$$

При малых значений x (например, $x \leq 0{,}1$) можно считать, что:

$$(1-x) \approx e^{-x}. \tag{6.32}$$

Учитывая это, преобразуем выражение (6.30), подставив в него значения (4.45). В результате получим:

$$P(\bar{n},k) = 1 - \left(e^{-\frac{1}{n}}e^{-\frac{2}{n}}\ldots e^{-\frac{k-1}{n}}\right) = 1 - e^{-\left(\frac{1}{n}+\frac{2}{n}+\ldots+\frac{k-1}{n}\right)} = 1 - e^{-\frac{k(k-1)}{2n}} \tag{6.33}$$

Обозначим $P(n,k) = P_з$, то есть значением вероятности, с которой должна возникнуть коллизия. В результате имеем:

$$P_з = 1 - e^{-k(k-1)/2n}$$

или

$$1 - P_з = e^{-k(k-1)/2n}. \qquad (6.34)$$

Выполнив логарифмирования (6.34), получим:

$$\ln(1 - P_з) = -k(k-1)/2n. \qquad (6.35)$$

Преобразуя (6.38), имеем:

$$\frac{k(k-1)}{2n} = -\ln(1 - P_з),$$

или

$$\mathrm{k}(\mathrm{k}-1) = -2\mathrm{n}\ln(1 - \mathrm{P}_з).$$

В конечном виде получаем:

$$\mathrm{k}^2 - \mathrm{k} + 2\mathrm{n}\ln(1 - \mathrm{P}_3) = 0.. \qquad (6.36)$$

Таким образом, получено уравнение, в котором связаны три величины - число событий k, общее число событий n и вероятность P(n,k), с которой должна возникать коллизия. Зная соответствующее значение $\mathrm{P}_з$ и n, можно получить точное решение по нахождению k.

Пусть $\mathrm{P}_з = 0{,}5$, тогда с использованием (6.36) получим:

$$\mathrm{k}^2 - \mathrm{k} + 2\mathrm{n}\ln 0.5 = \mathrm{k}^2 - \mathrm{k} - 2\mathrm{n}\ln 2 = 0. \qquad (6.37)$$

Если $\mathrm{n} = 2^{\mathrm{m}}$, то уравнение (6.37) будет иметь вид:

$$\mathrm{k}^2 - \mathrm{k} - 2^{m+1}\ln 2 = 0. \qquad (6.38)$$

Дадим оценку значения k, учитывая то, что $\mathrm{k}^2 \gg \mathrm{k}$. С учетом (6.36), получим:

$$\mathrm{k}^2 = -2\mathrm{n}\ln(1 - \mathrm{P}_з). \qquad (6.39)$$

При $\mathrm{P}_з = 0{,}5$ имеем:

$$\mathrm{k}^2 = -2\mathrm{n}\ln(1 - 0{,}5) = 2\mathrm{n}\ln 2.$$

И

$$\mathrm{k} = \sqrt{2\mathrm{n}\ln 2} \approx 1{,}41\sqrt{\mathrm{n}}. \qquad (6.40)$$

Для произвольного значения $P_з$, из уравнения (6.39), получим:

$$k = \sqrt{2\ln\left(\frac{1}{1-P_з}\right)\cdot n} = 1,41\sqrt{\ln\left(\frac{1}{1-P_з}\right)\cdot n}. \qquad (6.41)$$

Соотношение (6.41) позволяет оценить число преобразований (экспериментов) $H(M)$, которые необходимо осуществить для возникновения коллизии с вероятностью $P_з$. Сравнивая полученные для k значения, ((6.40) - (6.41)) с оценкой, которая приводится в [56]:

$$k = \sqrt{n} \qquad (6.42)$$

можно оценить степень близости оценки и возможность ее применения.

Рассмотрим пример оценки стойкости КАС. Пусть в качестве H используется хеш- функция SHA-1, в которой $n = 2^{160}$, и пусть: $P'_з = 0,5$ и $P''_з = 0,99$. Воспользовавшись выражением (6.41), получаем:

$$k_{0.5} = 1,41\sqrt{n} = 1,41\sqrt{2^{160}} = 1,41\cdot 2^{80} \approx 1,7\cdot 10^{24};$$

$$k = 1,41\sqrt{\ln\left(\frac{1}{1-0.99}\right)\cdot 2^{160}} = 2^{80} \approx 3\cdot 10^{24}.$$

В случае (4.55) получаем:

$$k_{0.5} = \sqrt{n} = \sqrt{2^{160}} = 2^{80} \approx 1,2\cdot 10^{24}.$$

Уравнение (6.41) позволяет точно решить задачу определения количества экспериментов k, которые необходимо выполнить для создания коллизии с вероятностью $P_з$ на множестве n. Достаточно хорошим приближением оценки является соотношение (6.42).

Приведенные в разделе результаты позволяют получить как зависимость числа событий k от значениий вероятности, с которой может возникнуть коллизия $P_з$, и общего числа событий n, так и зависимость $P_з$ от k и n.

6.3 Оценка показателей эффективности телекоммуникационных систем на основе применения нелинейных дискретных сигналов и динамического режима передачи информации

В ряде практических приложений телекоммуникационных систем одной из нерешенных является задача обеспечения имитостойкости данных как в канале передачи данных, так и в канале цикловой синхронизации.

Рассмотрим принципы обеспечения имитостойкости телекоммуникационных систем на основе применения различных систем (в том числе, нелинейных) дискретных сигналов и динамического режима передачи информации.

В существующих системах реализуется принцип фиксированного соответствия бит сообщения – сложный сигнал в течение продолжительного интервала времени и в качестве физических перенеосчиков данных используются классы сложных сигналов, синтезированные на основе линейных законов построения. Поэтому в соответствие с выражениями (1.21), (1.29), (1.31; 1.37) в радиоканалах некоторых специальных приложений телекоммуникационных систем не могут быть обеспечены необходимые значения показателей помехозащищенности, имитостойкости и скрытности функционирования.

Обработка широкополосных сигналов в приемных устройствах системы множественного доступа возможна при согласованном введении и использовании специальных данных об используемых формах сложных сигналов, несущих частотах, времени передачи и других параметров. Такая информация содержится в протоколе или алгоритме множественного доступа. Для выполнения указанных функций система должны содержать устройство ввода, хранения и выработки специальных данных.

После обнаружения приемным устройством синхромаркера с необходимыми значениями вероятности ложной тревоги ($P_{лт.}$), пропуска сигнала ($P_{пр.}$), определяется момент времени, начиная с которого в радиоканале реализуется динамический режим работы. Отметим, что необходимые значения указанных вероятностей, а также значение показателя структурной скрытности системы (S_c) могут

быть обеспечены за счет выбора сигналов с улучшенными корреляционными, ансамблевыми, структурными свойствами, заданной базой B сигналов, использования радиоканала с заданными значениями вероятности ошибки $P_{ош,}$ а также квазиоптимальной обработкой сигналов приемным устройством.

Будем полагать, что в радиоканале динамическими (изменяющимися) являются такие параметры как кодовая форма сигнала, выбираемая из определенного ансамбля сигналов или различных ансамблей, а также несущая частота. Таким образом, смена соответствия m бит сообщения - 2^m сложных сигналов осуществляется из пространства N состояний системы:

$$M = M_f M_{кф} , \qquad (6.43)$$

где:

M_f – общее число несущих частот;

$M_{кф}$ – общее число кодовых форм сложных сигналов.

Будем также считать, что соответствие m бит сообщения - 2^m сложных сигналов изменяется с течением времени по закону (правилу) предсказание которого возможно с достаточно малой вероятностью.

Если динамический режим реализован с применением метода «с возвращением», при котором на каждом интервале mT времени передачи m бит информации разрешенными для излучения на частотах M_f являются все $M_{кф}$ сложных сигналов и выбираются они в соответствии со значениями символов управляющей последовательности (гаммы), то вероятность навязывания (с учетом (4.30)) сложного сигнала определяется с использованием выражения:

$$P_{\frac{нав^к}{сигн.}} = k \frac{M_{f^р} M_{кф^р}}{M_f M_{кф}} \qquad (6.44)$$

где: $M_j^р$,$M_{кф}^р$ - соответственно число частот и кодовых форм сигналов, разрешенных для излучения в соответствии со знаками (символами) управляющей последовательности;

M_f $M_{кф.}$ – общее число частот и кодовых форм сигналов;

k – число попыток, которые предпринимает станция противодействия с целю навязывания ложных сообщений.

В таблице 6.1 приведены значения $P_{нав.}$ на сигнал (авто- или изоморфизм), достигаемые при использовании в качестве синхромаркера: линейной рекуррентной последовательности максимального периода (ЛРПМ); нелинейного характеристического дискретного сигнала (ХДС). При расчетах было принято, что $M_j^p = M_{кф}^p = 1$. В таблице указаны близкие по значениям длительности сигналов, для которых могут быть построены соответствующие системы сигналов (ЛРПМ, ХДС).

Таблица 6.1

Значения вероятностей навязывания для различных систем сигналов длительностью L

Система сигналов	31 (32)	63 (66)	127 (130)	255 (256)	1023 (1032)	2047 (2098)
ЛРПМ	$5{,}4\cdot10^{-3}$	$5{,}5\cdot10^{-3}$	$9\cdot10^{-4}$	$2{,}5\cdot10^{-4}$	$1{,}6\cdot10^{-5}$	$1{,}7\cdot10^{-6}$
ХДС	$2{,}6\cdot10^{-3}$	$1{,}5\cdot10^{-3}$	$4{,}3\cdot10^{-4}$	$6\cdot10^{-5}$	$5{,}7\cdot10^{-6}$	$3{,}1\cdot10^{-7}$

Анализ данных таблицы 6.1 показывает, что при использовании в качестве синхромаркера ХДС, обеспечивается меньшая вероятность навязывания по сравнению со случаем применения ЛРПМ, а также более высокая структурная скрытность и, следовательно, - помехозащищенность телекоммуникационной системы. При этом, необходимо иметь в виду, что ХДС, так же как и ЛРПМ относятся к оптимальным, с точки зрения, периодической функции автокорреляции сигналам и, следовательно, помехоустойчивость приема ХДС не ниже, чем при обработке ЛРПМ. В таблице 6.2 приведены значения вероятности навязывания на изоморфизм для случаев, когда в качестве синхромаркера используются ЛРПМ, ХДС и характеристические производные ортогональне сигналы (ХПОС). Расчеты проводились для следующих значений параметров динамического режима передачи

информации: $M_f = 10^3$, $M_f{}^p = 4$, $M_{кф.}{}^p = 16$. В таблице значения вероятностей навязывания приведены для ряда близких по величине длительностей сигнала.

Из данных табл. 6.2 следует, что в динамическом радиоканале могут быть обеспечены достаточно малые вероятности навязывания даже единичного элемента синхросигнала. В тоже же время, если в качестве синхросигнала используется одна и та же форма сигнала, то навязывание может быть выполнено с вероятностью практически равной единицы.

Таблица 6.2

Значения вероятностей навязывания для различных систем сигналов длительностью N

Система сигналов	63 (66)	255 (256)	1023 (1032)	2047 (2098)
ЛРПМ	10^{-2}	$4\cdot10^{-3}$	10^{-3}	$3{,}6\cdot10^{-4}$
ХДС	$3\cdot10^{-3}$	$5\cdot10^{-4}$	$2\cdot10^{-4}$	$6\cdot10^{-5}$
ХПОС	$4\cdot10^{-6}$	$6\cdot10^{-8}$	$8\cdot10^{-10}$	$6\cdot10^{-10}$

Исследования качественных показателей телекоммуникационной системы, в частности, имитостойкости при реализации динамического режима функционирования радиоканала были выполнены для ряда частных случаев:

а) разрешенными для излучения в интервале mT являются 2^m сигналов, причем, соответствие m бит сообщения - 2^m сигналам, может быть как фиксированным, так и меняться по закону управляющей последовательности;

б) выполняется условие, аналогичное а), с тем лишь отличием, что каждый из 2^m сигналов может излучаться на M_f частотах;

в) разрешенными для излучения в интервале времени mT являются $M_f{}^p$ частот, и используется $M_{кф.} = 2^m$ сигналов.

Будем полагать, что смена соответствия m бит сообщения - 2^m сигналам, выбор несущих частот M_f производится по псевдослучайному закону, вероятность

предсказания которого в интервале времени T не превышает допустимой величины $P_{доп}$.

В случае а), если $M_f = M_f{}^p = 1$ и $M_{кф.}{}^p = 2^m$, как следует из (6.13), радиоканал не обладает имитозащищенностью, даже при реализации динамического режима функционирования радиоканала. Необходимая имитостойкость для данного случая может быть обеспечена только за счет смены несущих частот M_f, т.е. необходимо, чтобы M_f было больше единицы. В таблице 6.3 приведены значения $P_{нав.}$ на сигнал, вычисленные с использованием (6.13), для случая, когда $M_{кф.}{}^p = 2^m$.

Таблица 6.3

Значения вероятностей навязывания $P_{нав./с}$ в зависимости от количества используемых несущих частот M_f

Количество несущих частот (M_f)	128	256	1024	4096
Вероятностей навязывания на сигнал ($P_{нав./с}$)	$8 \cdot 10^{-3}$	$4 \cdot 10^{-3}$	10^{-3}	$2 \cdot 10^{-4}$

Анализ данных таблицы 6.3 показывает, что как при фиксированном, так и при смене по псевдослучайному закону соответствия m бит сообщения - 2^m сигналам (в случаях а) и б)), вероятность навязывания $P_{нав./с}$ не зависит от основания алфавита m, а при фиксированном M_f и от числа разрешенных для излучения частот $M_f{}^p$. Поэтому, такие радиоканалы обладают неудовлетворительной имитостойкостью даже при реализации в них динамического режима.

Рассмотрим случай в). В таблицах 6.4 – 6.6 приведены значения вероятностей навязывания $P_{нав./с}$ на сигнал при использовании в качестве синхропоследовательностей ЛРПМ, ХДС и характеристических ПОС. При этом, в качестве параметров динамического режима примем: $M_f = 1024$, $M_f{}^p = 1$, $M_{кф.}{}^p = 16$.

Таблица 6.4

Значения вероятностей навязывания на сигнал при использовании ЛРПМ при смене форм сигналов и несущих частот

$P_{нав./с}$	63	127	255	1023	4095
$P_{нав./с\ при}\ M_f = 1$	$4 \cdot 10^{-2}$	$7 \cdot 10^{-3}$	$3{,}8 \cdot 10^{-3}$	$2{,}6 \cdot 10^{-5}$	$2{,}6 \cdot 10^{-7}$
$P_{нав./с\ при}\ M_f = 1024$	$4 \cdot 10^{-5}$	$7 \cdot 10^{-6}$	$3{,}8 \cdot 10^{-6}$	$2{,}6 \cdot 10^{-7}$	$2{,}6 \cdot 10^{-8}$

Таблица 6.5

Значения вероятностей навязывания на сигнал при использовании ХДС при смене форм сигналов и несущих частот

$P_{нав./с}$	66	172	255	1032	4000	10000
$P_{нав./с}$ при $M_f = 1$	$1{,}5 \cdot 10^{-2}$	$2{,}1 \cdot 10^{-3}$	$9{,}6 \cdot 10^{-4}$	$8{,}8 \cdot 10^{-5}$	$4{,}8 \cdot 10^{-6}$	$7{,}8 \cdot 10^{-7}$
$P_{нав./с}$ при $M_f = 1024$	$2{,}4 \cdot 10^{-6}$	$2 \cdot 10^{-6}$	$9{,}6 \cdot 10^{-6}$	$8{,}86 \cdot 10^{-8}$	$4{,}8 \cdot 10^{-9}$	$7{,}8 \cdot 10^{-10}$

Таблица 6.6

Значения вероятностей навязывания на сигнал при использовании характеристических ПОС при смене форм сигналов и несущих частот

$P_{нав./с}$	64	100	256	512	1024	4000
$P_{нав./с}$ при $M_f = 1$	$1{,}7 \cdot 10^{-5}$	$8 \cdot 10^{-6}$	$5{,}6 \cdot 10^{-8}$	$4 \cdot 10^{-6}$	$1{,}8 \cdot 10^{-10}$	$8 \cdot 10^{-11}$
$P_{нав./с}$ при $M_f = 1024$	$1{,}7 \cdot 10^{-9}$	$7{,}8 \cdot 10^{-9}$	$5{,}6 \cdot 10^{-11}$	$4 \cdot 10^{-9}$	$1{,}8 \cdot 10^{-13}$	$7{,}8 \cdot 10^{-14}$

Анализ данных таблиц 6.4 – 6.6 показывает, что при реализации в радиоканале динамического режима и использовании характеристических ПОС уже при периоде сигнала L = 512 и большем периоде обеспечиваются высокие показатели с точки зрения вероятности навязывания $P_{нав./с}$. При обще количестве несущих частот $M_f = 1024$, высокие показатели по исследуемому показателю обеспечивается уже при периоде характеристического ПОС с периодом L= 256. Поэтому, в ряде приложений телекоммуникационных систем, например, при построении радиока-

налов специального назначения, предпочтительным является использование в качестве информационных характеристических производных ортогональных сигналов. Подчеркнем, что приведенные в табл. 6.4 – 6.6 результаты, получены при $M_{кф.}^{р} = 16$. Если же в системе не реализуется многоосновное кодирование, то $P_{нав./с}$ может быть уменьшена почти на порядок.

Проведем оценку имитостойкости радиоканала телекоммуникационной системы при решении задачи различения сигналов при использовании динамического режима и предлагаемых в работе дискретных сигналов. В разделе 3 приведены разработанные в ходе исследований методы синтеза криптографических нелинейных сигналов. В разделе 4 описаны результаты исследований корреляционных, ансамблевых и структурных свойств данного класса сигналов. В таблице 6.7 в соответствии с выражением (1.37) приведены значения вероятностей навязывания при использовании в ТКС в качестве физического переносчика данных криптографических нелинейных сигналов (КС) в сравнении с другими классами сигналов (М-последовательности, последовательности с 3-х уровневой периодической функцией взаимной корреляции (ПФВКТ). Также в таблице указаны граничные значения (границы «плотной упаковки») максимальных боковых лепестков ПФВК и число пар исследуемых последовательностей, которые соответствуют (с точки зрения ПФВК) указанным граничным значениям.

Анализ таблицы 6.7 показывает, что значения вероятностей навязывания в случае применения криптографических нелинейных сигналов значительно меньше (при периоде последовательности L= 1023 - на четыре порядка меньше, чем при применении М-последовательностей и на порядок меньше, чем в случае применения последовательностей с 3-х уровневой ПФВК). Повышение имитостойкости телекоммуникационной системы достигается благодаря тому, что КС обладают улучшенными по сравнению с линейными классами сигналов, в частности, М-последовательностями, ансамблевыми свойствами. При этом, необходимо отметить, что использование КС обеспечивает помехоустойчивость приема сигналов не ниже, чем при применении указанных выше сигналов, основанных на линейных законах формирования.

В данном разделе были приведены оценки имитостойкости телекоммуникационной системы, как способности противостоять навязыванию ложной информации, приходящейся на символ сообщения. Выполним оценку защищенности от навязывания ложных сообщений в телекоммуникационной системе.

Таблица 6.7

Значения вероятностей навязывания для различных систем сложных сигналов

Класс сигналов	Период последовательности (L)	Значение границы «плотной упаковки»	Число пар последовательностей	Значение вероятности навязывания
М-последовательности	31	9	3	$3 \cdot 10^{-1}$
ПФВКТ	31	9	495	$2 \cdot 10^{-3}$
КС	31	9	1465137	$7 \cdot 10^{-7}$
М-последовательности	127	27	36	$2 \cdot 10^{-2}$
ПФВКТ	127	17	11610	$8 \cdot 10^{-5}$
КС	127	27	9006648	$1 \cdot 10^{-7}$
М-последовательности	255	36	28	$3 \cdot 10^{-2}$
КС	255	36	17599	$5 \cdot 10^{-5}$
М-последовательности	511	63	276	$3 \cdot 10^{-3}$
ПФВКТ	511	33	147500	$6 \cdot 10^{-6}$
КС	511	63	2666671	$3,7 \cdot 10^{-7}$
М-последовательности	1023	100	435	$2 \cdot 10^{-3}$
ПФВКТ	1023	65	338000	$3 \cdot 10^{-6}$
КС	1023	100	5293538	$2 \cdot 10^{-7}$

При этом будем полагать, что в качестве манипулирующих (расширяющих спектр) используются различные системы сложных дискретных последовательностей. Также будем полагать, что в системе реализован динамический режим работы, предполагающий, в том числе, смену соответствия m бит сообщения - 2^m сложных сигналам. Смена соответствия осуществляется через установленные временные интервалы и с применением управляющей последовательности, отвечающей требованиям случайности (данные требования описаны в разделе 6.1). Для обеспечения необходимой помехоустойчивости приема сигналов будем использовать системы сигналов, которые обладают хорошими корреляционными свойствами [82-83,85]. Результаты исследования корреляционных свойств различных систем сигналов проведены в разделе 4 настоящей работы.

Вероятность навязывания ложного сообщения определяется возможностью станции противодействия определить закон установления соответствия: бит сообщения - сложный сигнал, или, другими словами, определить структуру управляющей последовательности, устанавливающей указанное соответствие, и определяется из соотношения:

$$P_{\text{нав./сообщение}} = (2^{-k})^n, \qquad (6.45)$$

где: 2^{-k-} число возможных состояний источника управляющей последовательности;

n – длина, выраженная в битах, сообщения.

Отметим, что число возможных состояний источника управляющей последовательности (2^{-k}) определяется ансамблем или числом пар дискретных последовательностей, с помощью которых манипулируют фазу высокочастотной несущей для образования фазоманипулированного широкополосного дискретного сигнала.

В таблице 6.8 приведены значения $P_{\text{нав./сообщение}}$ для различных систем дискретных сигналов, полученных на основе М – последовательностей, последовательностей с трехуровневой периодической функцией взаимной корреляции (ПФВК) и нелинейных криптографических последовательностей (НКП). В качестве размерности сообщения выбрано значение n = 32. В качестве периода N последовательностей были выбраны: 31, 63, 127, 1023.

Необходимо подчеркнуть, что в расчетах $P_{нав./сообщение}$ для случая применения в системе нелинейных криптографических последовательностей, были отобраны последовательности, корреляционные характеристики которых, близки к оптимальным граничным значениям («плотной упаковки») с точки зрения ПФВК. Такие граничные значения достигнуты в классе последовательностей с трехуровневой ПФВК и составляют $R_{бок.\ max} \leq 1{,}5\sqrt{N}$.

Таблица 6.8

Значения вероятности навязывания на сообщение для различных систем дискретных сигналов

Период последовательности (N)	Значения $P_{нав./сообщение}$ для систем сигналов:		
	М последовательности	Последовательностей с трехуровневой ПФВК	Нелинейные криптографические последовательности
31	2^{-96}	2^{-288}	2^{-672}
63	2^{-96}	2^{-320}	2^{-768}
127	2^{-160}	2^{-448}	2^{-640}
1023	2^{-192}	2^{-608}	2^{-736}

Как видно из данных таблицы, значения $P_{нав./сообщение}$ для нелинейных криптографических последовательностей значительно меньшие, чем в случае использования наиболее широко применяемых на практике линейных классов сигналов (М последовательностей и последовательностей с трехуровневой ПФВК).

В случае, когда в системе не установлены жесткие требования к значению $P_{нав./сообщение}$, но при этом необходимо обеспечить повышенные требования к помехоустойчивости приема сигналов, и реализовать (как и в рассматриваемом случае, при применении систем НКП) высокие требования с точки зрения структурной скрытности используемых сложных сигналов, то в качестве граничных значений могут быть выбраны значения максимальных боковых пиков ПФВК точно соответствующим границе «плотной упаковки». Например, объем системы НКП,

например, при N = 1024, со значения максимальных боковых пиков ПФВК $R_{бок.max} \leq 90$, объем системы составляет M = 5062 сигналов, в отличие от данных таблицы 6.8 , где указано, что при граничном значении $R_{бок.max} \leq 100$ (или - $3\sqrt{N}$), объем системы сигналов составляет M = 5293532 пар сигналов. Для рассматриваемого примера , т.е. при граничном значении $R_{бок.max} \leq 90$, $P_{нав./сообщение}$ есть:

$$P_{нав./сообщение} = (2^{-15})^{32} = 2^{-480}.$$

Заметим, что при использовании в качестве манипулирующих последовательностей М – последовательностей (объем системы сигналов составляет M = 60 сигналов), вероятность $P_{нав./сообщение}$ равна:

$$P_{нав./сообщение} = (2^{-6})^{32} = 2^{-192}.$$

Таким образом, выигрыш с точки зрения имитостойкости при использовании в качестве манипулирующих последовательностей нелинейных криптографических последовательностей, для указанного периода сигналов, практически на два порядка выше, чем при использовании М – последовательностей.

Приведенные выше оценки позволяют утверждать, что в телекоммуникационной системе, в которой в качестве метода информационного обмена реализуется динамический режим и применяются нелинейные криптографические сигналы, обеспечиваются высокие показатели защищенности системы от несанкционированной модификации данных и навязывания ложной информации.

По сути, такая система обеспечения имитостойкости представляет собой криптографическую систему, поскольку содержит все атрибуты такой системы: алгоритм защиты от навязывания ложного сообщения и скрытия смыслового содержания сообщения на основе реализации динамического режима функционирования радиоканала телекоммуникационной системы и использования криптографических дискретных сигналов в качестве переносчиков информации; алгоритм принятия решения об истинности полученной информации; ключевая система, реализующая генерацию управляющей последовательности для смены соответствия: бит сообщения – сложный сигнал, а также криптографических дискретных сигналов, с использованием которых осуществляют манипуляцию фазы высоко-

частотной несущей, образуя, таким образом, фазоманипулированные широкополосные сигналы (ФМШПС).

6.4 Практические приложения динамического режима передачи данных в телекоммуникационных системах на основе использования сложных нелинейных дискретных сигналов

6.4.1 Применение нелинейных дискретных сигналов в телекоммуникационных системах с кодовым разделением в качестве манипулирующих последовательностей

Типичным для телекоммуникационных систем является подход, заключающийся в использовании множества сигналов, обладающего, по меньшей мере, одним из следующих свойств:

- каждый из сигналов данного множества легко отличим от своей сдвинутой по времени копии;

- каждый из сигналов данного множества легко отличим от любого другого (в том числе, сдвинутого во времени) сигнала этого множества.

Первое свойство важно для радиолокационных систем, систем синхронизации, а также для широкополосных систем связи, второе – для многопользовательских систем с кодовым разделением абонентов. Наиболее часто используемым критерием различимости является минимум эвклидового расстояния [15,67]. Критерий состоит в том, что два сигнала являются легко различимыми тогда и только тогда, когда среднеквадратичное расстояние между ними велико. Необходимость совместного рассмотрения сигналов $Y(t)$ и $X(t)$ возникает при использовании манипуляции, например, в тех случаях, когда сигнал $X(t)$ модулируется двоичной последовательностью или когда им самим модулируется некоторая несущая. Таким образом, в качестве меры различимости сигналов используют величину [27]:

$$T^{-1}\int_0^T [Y(t) \pm X(t)]^2 = -T^{-1}\{\int_0^T \left[Y^2(t) + X^2(t) \right] dt \pm 2\int_0^T X(t)Y(t)dt\}, \qquad (6.46)$$

где T - период сигналов $X(t)$ и $Y(t)$.

Первый интеграл в правой части (6.46) есть сумма энергий сигналов $X(t)$ и $Y(t), 0 \le t \le T$. Следовательно, при фиксированных энергиях сигнал $Y(t)$ сильно отличается как от сигнала $X(t)$ так и от сигнала $-X(t)$ только в том случае, когда параметр

$$R = \int_0^T X(t)Y(t)dt \ , \text{ мал.} \qquad (6.47)$$

Параметр R при решении задач поиска, обнаружения, оценки параметров, (в этом случае используется согласованная фильтрация или корреляционный прием), представляет собой отклик согласованного с сигналом $Y(t)$ фильтра на входной сигнал $X(t)$. Например, если в многопользовательской телекоммуникационной системе с кодовым разделением сигналы $X(t)$ и $Y(t)$ выделены двум различным станциям (абонентам), то параметр ρ является мерой уровня взаимных помех, создаваемых каждым из сигналов приему другого.

Минимизация уровня боковых лепестков автокорреляционной функции имеет наивысший приоритет при конструировании сигнала для таких приложений систем как измерение времени запаздывания, временное разрешение, синхронизация работы станций и др.

В ряде приложений имеют место взаимные временные задержки между сигналами пользователей, делая процедуру синхронизации сигнатур на входе приемника проблематичной. Примером такой ситуации может служить система мобильной сотовой связи (канал «вверх»), в которой вследствие движения потребителей внутри соты, происходит изменение расстояния между ними и базовой станцией, а значит, и времени поступления пользовательских сигналов на приемник базовой станции. При наличии взаимных задержек сигналов последние не могут оставаться ортогональными. Следствием этого является возникновение меж-

пользовательского мешающего воздействия (помехи множественного доступа), что, в свою очередь, приведет к ненулевому отклику приемника, настроенного на k -го пользователя, от сигналов других абонентов. Помехоустойчивость обработки (различения) данных будет определяться энергетическим отношением сигнал-помеха на выходе приемника и числом пользователей.

Равенство нулю всех боковых лепестков для апериодических амплитудно - фазоманипулированных сигналов невозможно [51]. При синтезе сигналов используют минимаксный критерий, который требует достижения минимально возможной величины максимального бокового лепестка АКФ апериодического кода. Формальная запись данного критерия имеет следующий вид

$$R_{a,max} = \max R_a(m) = \min. \qquad (6.48)$$

В соответствии с критерием (6.48) предпочтительными являются последовательности с наименьшим значением бокового лепестка.

При решении указанных ранее задач (измерение времени запаздывания или временное разрешение) должно быть реализовано требование получения «острой» АКФ сигнала и, связанного с этим, широкой полосы сигнала. Достоинство применения широкополосных систем состоит в том, что требуемое значение энергии сигнала, которое в свою очередь диктуется необходимым значение отношения сигнал-шум, достигается только длительностью, а не пиковой мощностью, которая чаще всего ограничена. В этом случае использование угловой модуляции позволяет расширить полосу сигнала, что обеспечивает временную компрессию (сжатие) сигнала согласованным фильтром. При этом длительность отклика фильтра (время корреляции $\tau = 1/W$) окажется во много (примерно в WT) раз меньше длительности T сигнала.

Поскольку кодовое разделение основано на различии сигналов, то построение многопользовательских телекоммуникационных систем и показатели эффективности указанных систем определяются выбором сигналов и их свойствами. Обычно число абонентов в современных телекоммуникационных системах достаточно велико, поэтому выбор сигналов для систем сводится к определению систем сигналов с заданными свойствами. Развитие многопользовательских систем

и, в частности систем с кодовым разделением абонентов (CDMA) и привело к исследованиям в области теории систем сигналов.

В стандарте UMTS 3-го поколения системы с кодовым разделением в качестве кода первичной синхронизации используется бинарная последовательность длины 256, обладающая апериодическими боковыми лепестками вплоть до ¼ , т.е. $R_{max} = 64$ (или -12 дБ) [15].

В качестве альтернативы указанным последовательностям могут быть предложены нелинейные классы сигналов, в частности, криптографические сигналы (КС) и нелинейные сигналы в конечных полях. В ходе диссертационных исследований были разработаны теоретические основы синтеза указанных систем сигналов (разделы 2-3 данной работы).

В целях реализации данного предложения были отобраны 2940 КС, значения максимальных боковых выбросов апериодической функции автокорреляции ($\rho a,max$) которых, не превышают величины 36. Если к системе предъявляются более высокие требования с точки зрения помехоустойчивости приема сигналов (вероятности правильного приема), то при решении задачи синхронизации, могут быть использованы 680 КС, величина $\rho_{a,max}$ для которых, не превышает значений 33 (это наилучшее граничное значения для максимальных боковых пиков двоичных сигналов с периодом 256 элементов). В этом случае, выигрыш по сравнению с использование последовательностей, применяемых в стандарте UMTS, составляет 3 дБ. Указанное позволяет повысить помехоустойчивость приема СП.

К числу привлекательных с точки зрения ФАК относятся нелинейные характеристические дискретные сигналов (ХДС) с числом позиций $N = 4x + 2$ и N=4x, x=1,2. Максимальные боковые выбросы ПФАК таких сигналов составляют соответственно {- 4, 0} и {+2, - 2}, т.е данный класс сигналов относится к оптимальным или минимаксным, с точки зрения ПФАК, сигналам. Были исследованы автокорреляционные свойства в апериодическом режиме данного класса сигналов. Были отобраны 470 сигналов, боковые лепестки АФАК которых, не превышают величины 20/256. В Приложении Д (таблица Д.1) приведены значения $R_{a,max}$ бо-

ковых лепестков апериодической функции автокорреляции таких сигналов, с указанием номера изоморфизма сигнала (сигнала, полученного с использованием соответствующего коэффициента децимации, и номер (такт) циклического сдвига изоморфизма). Необходимо заметить, что для периода ХДС с периодом 256 символов, существует 64 изоморфных сигналов, что существенно превышает объем линейных классов сигналов для указанного периода. Выигрыш при выборе ХДС в качестве СП по сравнению с сигналами, применяемыми в стандарте UMTS, составляет более 4 дБ.

6.4.2 Применение нелинейных дискретных последовательностей в телекоммуникационных системах в качестве производящих последовательностей

Среди систем фазоманипулированных сигналов многие образованы на базе систем Уолша [55]. Известно, что авто - и взаимно корреляционные функции последовательностей Уолша имеют большие боковые пики. Для улучшения корреляционных свойств сигналов формируют производные системы сигналов (ПСС) посредством перемножения последовательностей Уолша (исходных последовательностей) на сигнал, который обладает определенными свойствами (производящий сигнал), в частности, имеют малые боковые пики авто корреляционной функции. Было высказана гипотеза о возможности использования в качестве производящих – нелинейных криптографических последовательностей (КП) и нелинейных сигналов в конечных полях, теоретические основы синтеза которых, разработаны в ходе исследований.

В основу построения ПСС были положены следующие принципы.

1. Осуществляется отбор КП, обладающих необходимыми, с точки зрения требований по помехоустойчивости приема информации, значениями ПФАК.

2. Формируется набор кодов Уолша, в котором каждая строка соответствует отельному коду.

3. Каждая из строк кода Уолша суммируется по модулю 2 с одной из КП, при этом образуется ПСС.

4. Выполняются исследования корреляционных свойств ПСС. Для исследования взаимно корреляционных свойств ПСС, образуют матрицу, которая содержит все возможные пары ПСС, необходимые для реализации режима передачи данных в телекоммуникационных системах.

В таблице 6.9 приведены результаты исследований статистических характеристик различных классов сигналов (ПРИЛОЖЕНИЕ Е). Расчеты проводились для значений длин последовательностей (от 30 до 2052).

Таблица 6.9

Статистические характеристики корреляционных функций различных классов сигналов.

Тип сигналов	Характеристики	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\lvert R\rvert}}{\sqrt{N}}$	$\frac{D_{\lvert R\rvert}^{1/2}}{\sqrt{N}}$	$\frac{D_{(R)}^{1/2}}{\sqrt{N}}$
ХДС	АФАК	1,6 - 2,4	0,3 - 3,4	1,4 - 7,7	1,9 - 10,8
	ПФАК	0,02 - 0,5	0,02 - 0,3	0,03 - 0,3	0,06 - 05
	АФВК	1,3 - 3,3	0,5 - 0,7	2,4 - 18,2	3,6 - 27
	ПФВК	0,8 - 3,3	0,7 - 0,8	5,8 - 45,3	5,9 - 45,3
ПСС	АФАК	0,8 - 2,4	0,4 - 0,5	0,9 - 1	1 - 1,1
	ПФАК	0,7 - 2,5	0,2 - 0,7	0,2 - 0,5	0,3 - 0,9
	АФВК	1 - 2,5	0,2 - 0,7	0,2 - 0,5	0,3 - 0,7
	ПФВК	1,4 - 2,8	0,2 - 0,7	0,4 - 0,5	0,6 - 0,9
КП	АФАК	0,7 - 2,5	0,4 - 0,5	0,9 - 1	0,9 - 1,2
	ПФАК	0,9 - 2,5	0,3 - 0,7	0,2 - 0,5	0,3 - 0,9
	АФВК	1,2 - 2,7	0,4 - 0,7	0,3 - 0,5	0,5 - 0,7
	ПФВК	1,5 - 2,8	0,5 - 0,7	0,3 - 0,5	0,8 - 0,9
М - последовательности.	АФАК	0,7 - 1,25	0,32	0,26	0,41
	ПФАК	$1/\sqrt{N}$	$1\sqrt{N}$	0	0
	АФВК	1,4 – 5,0	0,54	0,48	0,73
	ПФВК	1,9 – 6,0	0,8	0,62	1

Анализ данных таблицы 6.9 показывает, что статистические характеристики ПСС близки к соответствующим характеристика, указанным в таблице, линейных и нелинейных классов сигналов. При этом значения максимальных боковых пи-

ков функций взаимной корреляции меньше, чем у широко используемых современных телекоммуникационных системах линейных М последовательностей.

Для ПСС, в которых в качестве производящих используются нелинейные криптографические сигналы с периодом 64 двоичных элементов, число пар сигналов, для которых значения максимальных боковых пиков взаимно корреляционной функции (ВКФ) не превышают 17 (это так называемая граница «плотной упаковки», достигаемая в классе лучших с точки зрения ВКФ последовательностей с трехуровневой ПФВК), составляет 604 пары, что составляет около 30% из общего числа возможных сочетаний пар сигналов. Для остальных пар сигналов значения максимальных боковых пиков ВКФ не превышают 25. Максимальное количество отобранных сигналов, для которых значения максимальных боковых пиков ВКФ не превышают граничного значения 25, составляет 96,8 % (1984 сигналов) от общего количества сочетаний пар ПСС.

Кроме того, ПСС обладают улучшенными (по сравнению с линейными классами сигналов) ансамблевыми и структурными свойствами.

В ходе исследований был разработан комплекс программных средств (ПРИЛОЖЕНИЕ Е), позволивший реализовывать указанные выше принципы создания ПСС и решать задачи, связанные с исследованием свойств указанных систем сигналов.

Стандарты 2-го и 3-го поколения (IS-95 и UMTS соответственно) представляют собой систему множественного доступа с кодовым разделением каналов (CDMA) и прямым расширением спектра, т.е. биты информации пользователя передаются в широкой полосе частот путем умножения исходного потока данных пользователя на псевдослучайные последовательности символов (чипы), являющимися кодами расширения CDMA. Причем, в качестве устройств формирования псевдослучайных последовательностей, используют n - разрядные (n – степень двоичного полинома) сдвиговые регистры с линейной цепью обратной связи. Известно, что кодовая устойчивость (структурная скрытность) таких последовательностей (чипов) – низка [55].

Альтернативой указанным последовательностям могут быть нелинейные классы сигналов, в частности, криптографические последовательности (КП). Построение таких последовательностей не может быть представлено в виде рекуррентного правила (алгоритма) и структурные свойства КП близки (как это было показано в разделе 4) к свойствам случайных последовательностей. В качестве еще одного довода в пользу КП свидетельствует то обстоятельство, что характеристики их авто - и взаимных функций корреляции не уступают характеристикам лучших с точки зрения корреляционных свойств дискретных последовательностей (М-последовательностей, множеств Голда и Касами, ансамблей Камалетдинова и др.)

Одним из достоинств ортогональных сигналов является простота технической реализации. При этом необходимо отметить, что применение в телекоммуникационных системах ПСС (на основе криптографических последовательностей и нелинейных сигналов в конечном поле) не усложняет реализации информационного обмена. Об этом свидетельствует характеристики разработанного пакета программных средств, реализующего такие системы

Метод CDMA заключается в том, что разделение осуществляется по форме сигналов, которые использует тот или иной абонент, причем каждый пользовательский сигнал занимает как всю доступную полосу F, так и временной интервал T . Указанное означает, что при таком способе множественного доступа все пользовательские сигналы широкополосны. Таким образом система с CDMA будет обладать всеми достоинствами широкополосной системы (технологии распределенного спектра): помехоустойчивость, низкая вероятность обнаружения и др. В разделе 1 было отмечено, что помехоустойчивость приема сложных сигналов в многопользовательских системах определяется энергетическим отношением сигнал/шум на входе решающего устройства приемника, а также степенью коррелированности (значением максимальных боковых выбросов функции взаимной корреляции, (выражения (1.39-1.42)), используемых при решении задач различения), сигналов. Для идеального гипотетического ансамбля ρ_{max} равен нулю, а для любо-

го реального ансамбля значение ρ_{max} может служить адекватной мерой его близости к идеальному. Для решения задач поиска, обнаружения важно иметь сигналы, для которых функция корреляции имеет нулевые лепестки вблизи центрального пика тела неопределенности. Были проведены исследования, целью которых был поиск нелинейных сигналов с нулевыми значениями максимальных боковых пиков ФВК и ФАК, в том числе, вблизи основного (максимального пика) функции корреляции. Разработанный в ходе исследований программный комплекс позволяет осуществлять поиск последовательностей, обладающих указанными свойствами для их применения в качестве синхропоследовательностей, а также последовательностей, с помощью которых осуществляют модуляцию информационных битов пользователей телекоммуникационной системы.

В таблице 6.10 приведены примеры различных корреляционных функций (ПФВК и ПФАК) для нелинейных дискретных сигналов (ХДС) с периодом 96 и 256 элементов, имеющие нулевые пики вблизи центрального пика.

Таблица 6.10

Примеры корреляционных функций для отдельных нелинейных сигналов, имеющих нулевые боковые лепестки

Период ХДС – 96 символов (ПФВК)	
1 85	[1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, -1, 1, -1, -1, -1] [-1, 1, -1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, 1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, -1, -1, 1, -1, -1, -1, -1, -1, -1, -1, -1, 1, -1, -1, 1, -1, -1, -1, 1, 1, 1, 1] [0, 0, 0, -4, -4, 4, -16, -24, 4, -16, 0, -4, 12, 24, 0, -4, 12, -4, -12, 4, -24, -16, -4, 12, 0, 0, -8, 0, -8, 0, 4, 4, 0, 16, 16, 0, -12, 16, 0, 4, 12, 0, 0, 4, -4, -4, 0, -12, -8, 0, 8, -12, 0, -4, 4, 4, 0, 0, -12, 4, 0, 16, 12, 0, -16, 16, 0, 4, -4, 0, 8, 0, 8, 0, 0, 12, 4, -16, 24, 4, 12, -4, -12, -4, 0, 24, -12, -4, 0, -16, -4, -24, 16, 4, 4, -4]

Продолжение Таблицы 6.10

<table>
<tr><td>13

49</td><td>[-1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, -1, 1, -1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, -1, 1, -1, -1, -1, 1, 1, -1, -1, 1, 1, 1, -1, 1, -1, 1, -1, -1, 1, 1, 1]
[1, -1, 1, 1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, -1, -1, -1, 1, -1, 1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1, -1, 1, 1, 1, -1, -1, 1, -1, -1, -1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1]
[0, 0, 0, 12, -4, 0, 4, 16, -16, -4, 0, -8, 16, 0, -4, -4, -4, 4, 4, 0, 0, -12, -4, 12, 0, 0, -12, -16, -16, -4, -24, -24, 16, 0, 4, 8, 24, 0, -4, -8, 0, 4, 4, 12, 4, 0, 12, -12, 0, 12, 12, 0, 4, -12, 4, -4, 0, 8, -4, 0, 24, -8, 4, 0, 16, 24, -24, 4, -16, 16, -12, 0, 0, -12, -4, 12, 0, 0, 4, -4, -4, 4, -4, 0, 16, 8, 0, 4, -16, -16, 4, 0, -4, -12, 0, 0]</td></tr>
<tr><td colspan="2">Период ХДС 256 символов (ПФАК)</td></tr>
<tr><td colspan="2">[256, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0]</td></tr>
<tr><td colspan="2">[256, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0]</td></tr>
</table>

Продолжение Таблицы 6.10

[256, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, -4, 0, 0, 0, -4, 0, -4, 0, 0, 0, 0, 0, -4, 0, -4, 0, -4, 0, -4, 0, 0, 0, 0, 0, 0, 0, -4, 0, -4, 0, 0, 0]

Таблица 6.11

Ансамбли криптографических сигналов, значения боковых выбросов корреляционных функций которых равны нулю вблизи центрального пика

Размерность сегмента КП	Граничные значения функции неопределенности	ПФАК				ПФВК				
		Число КП удовлетворящих границе	Наименьшее значение Rбmax	Количество КП с наименьшим Rбmax	Число КП содержащих один или более Rб = 0 вблизи центрального пика	Общее количество пар	Количество пар, удовлетворяющих границе	Количество пар, имеющее Rб = 0	Наименьшее значение Rбmax	Количество пар с наименьшим Rбmax
64	17	9545	8	14	2041	45553512	5451589	4534955	10	278
256	33	680	28	48	81	231200	0	11589	34	83
256	36	2940	28	48	302	4321800	17599	215694	30	48
1024	80	247	72	3	7	30504	0	735	86	3
1024	90	2209	72	3	123	2439840	26638	60966	82	90
2048	129	409	116	12	39	83640	0	1483	130	13

В классе ХДС размерностью 100 символов существует 210 пар сигналов, имеющие нулевые выбросы (от одного до трех нулей) и 16 сигналов, имеющих нулевые выбросы ПФАК вблизи центрального пика функции неопределенности. Так же был проведен поиск нелинейных криптографических последовательностей (КП), функции авто - и взаимной корреляции которых, имеют нулевые пики вблизи центрального пика). В таблице 6.11 приведены данные о количестве отдельных сигналов и пар сигналов, имеющих нулевые боковые лепестки функции неопределенности и взаимной функции неопределенности вблизи центрального пика для ряда значений периода КС.

Как следует из данных таблицы, для КС с периода 256 символов существует 302 сигнала, для которых боковые пики ПФАК имеют один и более нулевых выбросов функции корреляции вблизи центрального пика и более 215 тысяч пар сигналов, для которых боковые пики ПФВК имеют нулевые значения.

Выводы к разделу 6

В шестом разделе диссертации решена **седьмая** и **девятая** задачи исследования.

1. Комплексное обеспечение требуемых показателей помехо- и имитозащищенности, а также информационной скрытности, в радиоканалах телекоммуникационных систем, обладающих большой частотной избыточностью, может достигаться на основе реализации динамического режима функционирования, когда с течением времени соответствие m - бит - 2^m сложных сигналов изменяется по сложному закону, например, по закону псевдослучайной или случайной последовательности. Сформулированное утверждение (6.1) определяет необходимые и достаточные условия обеспечения теоретической недешифруемости (теоретической информационной скрытности) на уровне источника сложных сигналов. При их реализации вероятность выбора для передачи W_j сигнала не будет зависеть ни от передаваемых m- бит сообщения, ни от ранее переданных сигналов. Для обеспечения теоретической недешифруемости (абсолютной структурной скрытности) каждого из $W_i \in \{W\}$ сложных сигналов, необходимо и достаточно, чтобы выпол-

нялось условие (6.7), то есть, чтобы вероятность появления элемента $W_{j,i}$ сложного сигнала не зависела ни от элементов ранее переданных сигналов, ни от элементов $W_{j,\,i-1}$, $W_{j,i-2}$, …. $W_{j,\upsilon,\ldots\ldots..}$ $W_{j,\,2}$ данного сигнала.

2. Теоретически недешифруемым, с точки зрения закона формирования сигналов, является источник сигналов со случайным формированием всех сигналов, т.к. только в этом случае у станции противодействия отсутствует возможность получения регулярного решения о законе формирования сигналов. К указанному классу сигналов необходимо отнести нелинейные криптографические сигналы.

3. Получены аналитические выражения для определения показателей информационной безопасности ТКС, в частности: вероятности имитации и подмены сообщения станцией противодействия; вероятности возникновения коллизий кодов аутентификации сообщений; числа экспериментов (сообщений), которые необходимо подать на вход преобразователя (МАС - сообщения; устройства формирования сложного сигнала) для создания коллизии с заданной вероятностью для заданного множества сообщений. Имитационную и коллизионную стойкости МАС кодов предложено оценивать посредством использования статистики совместных распределений МАС кодов по ключам для истинных и поддельных сообщений. Для МАС кодов определение такой статистики выглядит проблематичным из-за очень большого размера массива возможных МАС. Нижние границы для вероятностей имитации и подмены не учитывают статистические свойства массивов аутентификаторов, и основываются на модели псевдослучайности функции f(x) и определяют минимальные требования к размеру ключевого пространства и пространства МАС значений. Верхние границы для вероятностей имитации и подмены связанны с комбинаторными свойствами МАС массивов и оценивают значения для наихудшего случая выбора ключей и сообщений.

4. Показано, что повышение помехозащищенности, имитостойкости и информационной скрытности ТКС может быть достигнуто на основе использования динамического метода передачи данных. При этом в качестве физического переносчика данных применяются системы нелинейных дискретных сигналов в конечных полях, системы нелинейных криптографических дискретных сигналов.

Показано, что в качестве порождающих последовательностей при синтезе производных систем сигналов целесообразно использовать криптографические системы сигналов и нелинейные сигналы в конечных полях, теоретические основы синтеза которых, получены при проведении диссертационных исследований и представлены в разделах 2 и 3. Помехоустойчивость приема сигналов при использовании нелинейных систем сигналов на 3-4 дБ выше, чем в случае применения линейных классов сигналов.

5. При использовании для передачи данных нелинейных классов сигналов, методы синтеза которых приведены в разделах 2-3 диссертации, обеспечивается (по сравнению с линейными классами сигналов) меньшая вероятность навязывания, а также более высокая структурная скрытность, и, следовательно, помехозащищенность. Так, при периоде сигнала с числом элементов 1023, вероятность навязывания на сигнал при использовании системы криптографических сигналов на 5 порядков меньше чем в случае использования линейных сигналов (М- последовательностей).

6. Предложенная система обеспечения имитостойкости, по сути представляет собой криптографическую систему, так как она содержит все составляющие криптографической системы: алгоритм защиты от навязывания ложного сообщения и скрытия смыслового содержания сообщения на основе реализации динамического режима; алгоритм принятия решения об истинности полученной информации; ключевую систему, реализующую генерацию управляющей последовательности для смены соответствия, а также источник криптографических дискретных сигналов.

ВЫВОДЫ

В диссертации проведено теоретическое обобщение и получено новое решение научно - прикладной проблемы повышения помехозащищенности и информационной безопасности телекоммуникационной системы (ТКС) на основе усовершенствования методологических основ построения ТКС путем разработки методов информационного обмена, а также методов синтеза новых классов нелинейных дискретных сложных сигналов с необходимыми ансамблевыми, корреляционными и структурными свойствами.

1. Функционирование целого ряда современных ТКС осуществляется в условиях внешних и внутренних воздействий, обусловленных, с одной стороны, действием естественных помех, помех от других радиотехнических систем, функционирующих на близких частотах или в общем участке диапазона частот, с другой стороны, - преднамеренных помех, создаваемых в целях радиоэлектронного подавления действующих систем, станциями противодействия. Эффективность функционирования ТКС определяется их способностью выполнять стоящие перед ними задачи, в заданных условиях. К основным показателям эффективности функционирования ТКС относят: пропускную способность, помехозащищенность (помехоустойчивость, скрытность) и информационную безопасность (имитостойкость, информационная скрытность), живучесть, достоверность, производительность и др. В процессе исследований выполнен анализ проблем информационной безопасности, скрытности и помехозащищенности существующих ТКС, получена совокупность частных показателей эффективности, интегральный безусловный критерий защищенной телекоммуникационной системы.

Анализ методов информационного обмена в ТКС показывает, что в течение длительного времени в информационном канале, т.е. на физическом уровне, соответствие: бит сообщения - сигнал с течением времени остается фиксированным, а в качестве физических переносчиков данных применяются сигналы, основанные на линейных правилах построения, и обладающие низкой структурной скрытностью, ограниченными ансамблевыми свойствами. В указанных условиях, в процессе ин-

формационного противодействия, возможными стратегиями станции противодействия являются: определение содержания сообщений при использовании легальными абонентами алгоритмов криптографической защиты данных; фальсификация сообщений; нарушение целостности данных; постановка различных типов помех и другое. Такое воздействие нарушителя на систему может привести к существенному ухудшению показателей эффективности ТКС (помехозащищенности, информационной безопасности, имитостойкости, вероятносто-временных показателей передачи сообщений, живучести и др.)

2. Проведенные исследования и сравнительный анализ известных методов повышения показателей информационной безопасности и помехозащищенности показали, что одним из перспективных направлений комплексного обеспечения требуемых значений указанных показателей является реализация в радиоканалах ТКС динамического режима функционирования, когда с течением времени соответствие: m - бит - 2^m сложных сигналов изменяется по сложному закону, например, по закону псевдослучайной или случайной последовательности, а в качестве сложных сигналов применяются сигналы, основанные на нелинейных принципах построения.

3. Наиболее важными научными результатами, полученными в диссертации, являются следующие.

Впервые получен метод синтеза нелинейных криптографических дискретных сложных сигналов (КС), который использует случайные (псевдослучайные) процессы и позволяет создавать сигналы с необходимыми ансамблевыми, структурными и корреляционными свойствами, что дает вовможность улучшить показатели помехозащищенности и информационной безопасности ТКС в условиях внешних и внутренних воздействий.

Улучшение указанных показателей эффективности достигается, в частности, за счет возможности формирования, с применением полученного метода, больших ансамблей дискретных последовательностей практически любого периода с необходимыми (для тех или иных приложений системы) значениями боковых лепестков функций авто – взаимной и стыковой функции корреляции в периодиче-

ском и апериодическом режимах работы, а так же статистическими характеристиками корреляционных функций (КФ), не уступающих аналогичным характеристикам лучших, с точки зрения КФ, линейных классов сигналов. Указанное дает возможность повысить помехоустойчивость приема сигналов до 4дБ. Нелинейные дискретные сигналы обладают улучшенными по сравнению с линейными классами сигналов ансамблевыми свойствами. Так, для периода последовательности N = 1023, объем системы, составленный из нелинейных криптографических сигналов более чем в 15 раз превышает объем системы сигналов с 3-х уровневой функцией взаимной корреляции, и более чем в 1200 раз объем системы, составленной из М – последовательностей. За счет улучшенных ансамблевых свойств КС и динамической смены соответствия бит сообщения – сложный сигнал, появляется возможность улучшить показатели информационной безопасности. Так, имитостойкость системы при применении КС с периодом сигнала 1023 элемента на пять порядков выше, чем при применении линейных классов сигналов (например, М – последовательностей). При этом необходимо подчеркнуть, что при улучшении показателей имитостойкости системы обеспечивается высокий уровень помехоустойчивости приема сигналов. Улучшенные по сравнению с линейными классами сигналов ансамблевые свойства КС позволяют повысить информационную скрытность системы. Кроме того, синтезируемые с использованием разработанного метода КС, как показали результаты проведенного тестирования, по своим статистическим свойствам, близки к свойствам случайных последовательностей, т.е. обладают (по критерию (3)) практически идеальной структурной скрытностью, поскольку удовлетворяют свойствам непредсказуемости следования символов, необратимости, случайности, равновероятности и независимости символов последовательности, что дает возможность увеличить структурную скрытность ТКС.

Впервые получена математическая модель структуры сложных нелинейных дискретных сигналов (НС) в конечных полях. Данная модель определяет зависимость характеров элементов мультипликативной группы поля Галуа и символов дискретных последовательностей, синтезированных с использованием характеров элементов мультипликативной группы поля, что позволяет определить значения

показателей помехозащищенности (структурной скрытности) дискретных сигналов. Показано, что для определения закона (правила) построения нелинейных дискретных сигналов в конечных полях необходимо знать не менее половины символов периода сигнала. Например, для периода сигнала 1023 элемента выигрыш с точки зрения структурной скрытности при использовании полученных в работе систем сигналов по сравнению с сигналами линейной формы (М-последовательностями) составляет 50 раз, а при периоде 8192 – более 300 раз.

Впервые получен метод реализации арифметических модульных операций сложения и вычитания, основанный на табличном принципе реализации арифметических операций с помощью использования специального кода табличного умножения, что позволяет повысить быстродействие выполнения модульных операций сложения и вычитания;

Впервые получен метод реализации арифметической модульной операции умножения, основанный на использовании табличного принципа путем использования процедуры поразрядного определения результата операции, что позволяет повысить быстродействие выполнения операций модульного умножения.

Усовершенствован метод реализации арифметических модульных операций сложения и вычитания, который, в отличие от известных, основан на использовании принципа кольцевого сдвига, с помощью представления остатков числа двоичным кодом, за счет использования свойств циклических перестановок содержимого кольцевого регистра, что позволяет повысить быстродействие выполнения модульных операций.

Результаты расчета и сравнительного анализа времени реализации арифметических модульных операций в модулярной системе счисления, на основе использовании табличного принципа показали следующее: при реализации операции модульного сложения (вычитания) с использованием табличного метода, в зависимости от величины l-байтового ($l=\overline{1-4,8}$) машинного слова, в 7,5 – 63,5 раза эффективнее, а для операции модульного умножения, в 64 - 4096 раз эффек-

тивнее по времени выполнения арифметических модульных операций, чем при использовании сумматорного метода в позиционной системе счисления.

Усовершенствован метод синтеза нелинейных дискретных сложных сигналов, в котором, в отличие от известных, используется зависимость между элементами и индексами элементов конечного поля, что позволяет повысить быстродействие синтеза сигналов. Так, выигрыш во времени синтеза сигнала, с применением полученного метода по сравнению с известным, для периода сигнала 256 элементов, составляет - 25,5 раз, а для периода 9972 элементов – 1039,6 раза.

Усовершенствован метод синтеза нелинейных криптографических дискретных сложных сигналов, в котором, в отличие от известных, используются механизмы направленного (ограниченного) перебора сигналов для отбора сигналов, соответствующих определенным требованиям, что позволяет повысить производительность синтеза системы сигналов с требуемыми свойствами. Выигрыш в производительности синтеза дискретных сигналов с периодом от 256 до 2000 элементов, с применением разработанного метода, составляет (для указанных периодов сигнало) 40 - 60 процентов по сравнению с методом синтеза, основанном на переборе всех возможных вариантов сигналов. При реализации предложенного метода возможны пропуски (потери) при нахождении сигналов с заданными свойствами, но как показали исследования, процент таких потерь – незначителен и, для указанных периодов, составляет не более 8 процентов.

Усовершенствован метод оценки свойств линейных дискретных сложных сигналов, в котором в отличие от известных, использованы алгебраические свойства элементов конечного поля, что позволяет увеличить быстродействие процесса исследования свойств сигналов, и, таким образом, повысить производительность синтеза системы сигналов. Так, для периода сигнала 10098 элементов (объем системы составляет 2880 сигналов), выигрыш в производительности синтеза системы сигналов с заданными свойствами при использовании разработанного метода по сравнению с известным методом составляет 720 раз.

Усовершенствован метод синтеза всей системы нелинейных дискретных сигналов, в котором, в отличие от известных, используется процедура считывания и

записи (по определенному правилу) символов сигнала для формирования всего множества сигналов, относящихся к этой системе сигналов, что позволяет повысить производительность синтеза сигналов. Применение такого метода позволяет получить выигрыш при формировании всей системы нелинейных дискретных сигналов характеристического типа (с использованием программной модели), по сравнению с известным, при периоде формируемого сигнала 1020 элементов, - в 16 раз, а при периоде 2380 - 26 раз. В целом при увеличении периода сигнала выигрыш возрастает.

Развиты теоретические основы функционального построения ТКС, в том числе, с динамическим кодированием, включающие строго обоснованные и доказанные необходимые и достаточные условия обеспечения необходимых показателей помехозащищенности, информационной и структурной скрытности системы на уровне источника сложных сигналов.

Разработан усовершенствованный метод информационного обмена данными, в котором, в отличие от известных, применяются принципы динамического радиоканал на основе осуществления изменения соответствия: бит сообщения - сложный сигнал, и в качестве сложных сигналов применяются нелинейные дискретные сигналы с необходимыми ансамблевыми, структурными и корреляционными свойствами, что позволяет улучшить показатели информационной безопасности и помехозащищенности. Так вероятность навязывания ложного сообщения (при длине сообщения 32 бита) при применении нелинейных криптографических сигналов с периодом 1023 элементов, составляет 2^{-736}.

4. На основе разработанных и усовершенствованных в диссертации методов синтеза систем нелинейных сигналов, быстрой реализации модульных операций в работе представлены алгоритмы для их реализации, в соответствии с которыми синтезирован класс аппаратных средств формирования и обработки сигналов, на которые получено 14 авторских свидетельств на изобретения и патентов Украины, что подтверждает новизну и практическую значимость полученных в диссертации научных результатов работы. Разработан комплекс программных средств, реализующий методы синтеза и исследования свойств новых классов сложных

нелинейных дискретных сигналов. Такой комплекс позволяет: генерировать нелинейные КС и нелинейные последовательности символов в конечных полях практически любой длительности; определять значения минимальных и максимальных боковых выбросов различных КФ; сравнивать полученные значения с известными, потенциально достижимыми, границами для соответствующих КФ; присваивать синтезированным последовательностям уникальные идентификаторы (специальные радио данные), необходимые для оптимальной обработки данных; определять статистические характеристики различных КФ синтезированных сигналов; исследовать ансамблевые характеристики синтезируемых нелинейных сигналов. Компоненты программной компьютерной реализации разработанных методов синтеза и исследования свойств синтезируемых систем сигналов представлены в приложениях к диссертационной работе. Программное и математическое обеспечение, полученное в ходе исследований методов синтеза и исследования свойств систем нелинейных сигналов, практически готово к возможному использованию в составе опытных образцов и элементов современных цифровых коммуникационных средств.

5. Обоснованность полученных результатов подтверждается комплексным учетом полного набора факторов, влияющих на показатели эффективности функционирования телекоммуникационной системы. Дополнительным подтверждением обоснованности является совпадение результатов, полученных аналитическими методами, с данными многочисленных имитационно-математических моделей, использующих характеристики реальных реализаций сигналов и помех и непротиворечивостью разработанных аналитических описаний и формулировок основным положениям теории защиты информации, теории информации, теории систем сигналов, теории потенциальной помехоустойчивости. Кроме того, достоверность подтверждается использованием некоторых из полученных результатов в практических технических разработках на предприятиях промышленности.

6. Научные и практические результаты диссертационной работы целесообразно использовать:

- при проведении научно-исследовательских и опытно-конструкторских работ по разработке методов и средств синтеза систем дискретных сигналов, используемых в ТКС;

- в перспективных радиоканалах ТКС в виде технических средств формирования, обработки и передачи информации физического уровня, в частности, для организации помехозащищенных информационных каналов распределенных телекоммуникационных сетей.;

- при изучении учебных дисциплин по теории телекоммуникационных и информационных сетей.

Соискатель

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Advanced Encryption Standard (AES) [Электронный ресурс] / FIPS PUB 197. 2001. – Режим доступа: www. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

2. Andrea, Rock. Pseudorandom Number Generators for Cryptographic Applications [Текст] / Andrea Rock // Diplomarbeit zur Erlangung des Magistergrades an der Naturwissenschaftlichen Fakultat der Paris-Lodron-Universitat Salzburg. – Salzburg. – 2005.

3. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.

4. Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.

5. Berg, O. Spread Spectrum in Mobile Communication [Текст] / O. Berg, T. Berg, S. Haavik, J. Hjelmstad, R.Skaug. – IEE, London, 1998.

6. Blahut R. E. Algebraic Codes for Data Transmission [Текст] / Blahut R. E. – Cambridge: Cambridge Uni versity Press, 2003.

7. Chernisn, V.I. Assessing security Risks Using the Apparatus of Fuzzy Logic Theori / V.I. Chernisn, K.I. Ivanov, A.A. Zamula [Текст]// Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління». – 2011 – № 987. Випуск 18. – С.145 – 151.

8. Deng, X. New binary sequences with good aperiodic autocorrelation obtained by evolutionary algorithm [Текст] / X. Deng, P. Fan. // IEEE Commun. Lett. – 1999. vol. 3. – P. 288–290.

9. Dixon R. C. Spread Spectrum Systems with Commercial Applications, John Wiley & Sons, 1994. – 297 с.

10. Federal Information Processing Standards Publication (FIPS PUB) 140–1. Security requirements for cryptographic modules. NIST, 1994.

11. Federal Information Processing Standards Publication (FIPS PUB) 140–2. Security requirements for cryptographic modules. NIST, 1999.

12. Freeman R. L. Radio System Design for Telecommunications [Текст] / R. L. Freeman. – John Wiley & Sons, 1997.

13. Gold, R. Optimal binary sequences for spread spectrum multiplexing [Текст] // IEEE Trans. Inform. Theory.– 1967. Vol. 13. – P. 619–621.

14. Golomb S.W Digital Communications with Space Applications[Текст] / S.W. Golomb Prentice. – Hall, Englewood Cliffs, NJ, 1964.

15. Ipatov, Valery P. Spread Spectrum and CDMA.Principles and Applications [Текст] / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. – John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. – 2005. – 385 p.

16. ISO/IEC 10116:2006 Information technology - Security techniques - Modes of operation for an n-bit block cipher.

17. J. Kelsey. Cryptanalytic attacks on pseudorandom number generators [Текст] / J. Kelsey, B. Schneier, D. Wagner // C. Hall FSE. – 1998.

18. Kamaletdinov, B. Zh. "Optimal sets of binary sequences"/ B. Zh. Kamaletdinov // Problems of Inform. Transmission.– 1996. Vol. 32. – P. 171–175.

19. Kamaletdinov, B. Zh. An optimal ensemble of binary sequences based on the union of the ensembles of Kasami and bent-function sequences [Текст] / B. Zh. Kamaletdinov // Problems of Inform. Transmission. – 1988. Vol. 24. – P. 167–169.

20. Karim M.R., and Sarraf, R. W-CDMA and cdma2000 for 3G Mobile Networks [Текст] / M.R. Karim, R. Sarraf. – McGraw-Hill. – New York, 2002.

21. Kasami T. Weight distribution formula for some class of cyclic codes [Текст] / T. Kasami. – Coordinated Science Lab., Univ. Illinois, Urbana, Tech. Rep. R-285, April 1966.

22. Kim, K.I. CDMA cellular engineering issues [Текст] / K.I. Kim // – IEEE Trans. Veh. Tech. – 1993. Vol. 42 – P. 345–350,

23. Land, A.H. An automatic method of solving discrete programming problems. [Текст] / A.H. Land, A.G. Doig // Econometrica / – 1960.– V. 28. – P/ 497–520.

24. Lee, W. C. Y. Mobile Communications Engineering [Текст] / W. C. Y. Lee // McGraw-Hill, New York. – 1997.

25. NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

26. NIST 800-90 b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.

27. Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences [Текст] / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. – Vol. Com 68 – P. 59–90.

28. Shannon C. Communication theory of secrecy system [Текст] / C. Shannon Bell System Techn.J., 28, №4. – 1949.

29. Shannon, C.E. A mathematical theory of communication / C.E. Shannon // Bell System Technical Journal. – 1948. – №27. – P. 379–423, 623–525.

30. Simon M.K. Spread Spectrum Communication Handbook [Текст] / M.K. Simon, J.K. Omura, R.A. Scholtz, B. K Levitt. – McGraw-Hill, New York, 1994.

31. Sklar B. Digital Communications [Текст] / B Sklar. – Prentice-Hall, Upper Saddle River, NJ, 2001. – 1082 с.

32. Walke B. UMTS: The Fundamentals [Текст] / B. Walke, P. Seidenberg, M.P. Althoff. – John Wiley & Sons, 2003.

33. Welch L. R. Lower bound on the maximum cross-correlation of signals [Текст] / L. R. Welch. – IEEE Trans. Inform. Theory, vol. 20, P. 397–399, 1974.

34. Ziemer R. E. Introduction to Digital Communication [Текст] / R. E. Ziemer, and R. L Peterson. – Prentice- Hall, Upper Saddle River, NJ, 2001.

35. Ziemer R.E. Introduction to Spread Spectrum Communications [Текст] / R. E. Ziemer, R. L.Peterson, D. E.Borth. – Prentice-Hall, Englewood Cliffs, NJ, 1995.

36. Zierler, N. Linear recurring sequences [Текст] / N. J. Zierler // Soc. Appl. Math. – 1959. Vol. 7 – P. 31–48.

37. А.А. Замула Інформаційна безпека в каналах телекомунікацій: монографія [Текст]. – Изд. «Регіон - информ», г. Харків, 2000. – 214 с.

38. А.с. 1326162 СССР. 4Н 03К 3/84 Устройство для формирования псевдослучайных сигналов. [Текст] / Горбенко И.Д., Замула А.А., Стасев Ю.В., Кулешов В.Л., Мясоедов А.П. (СССР). – №3970022; заявл. 28.10.85; опубл. 22.03.1987.

39. А.с. 1353310 СССР. 4Н 03К 3/84 Устройство для формирования псевдослучайных сигналов. [Текст] / Горбенко И.Д., Замула А.А., Стасев Ю.В., Кулешов В.Л., Давыдов Г.П., Аносов А.М. (СССР).– №4020323; заявл. 11.02.86; опубл. 15.07.1987.

40. А.с. 1360545 СССР. 4Н 03К 3/84 Устройство для формирования псевдослучайных сигналов / Горбенко И.Д., Замула А.А., Стасев Ю.В., Бессарабенко К.В., Борисов В.И. (СССР). – №4017635, заявл. 06.02.86; опубл. 15.08.1987.

41. А.с. 1441413 СССР. Н06F 15/20 Устройство для формирования элементов расширенных полей Галуа GF (Pn) и кодовых последовательностей на их основе [Текст] / Горбенко И.Д., Замула А.А., Глазин Д.Е, Бычковский И.А., Захаров А.Т. (СССР). – №4230384; заявл. 15.01.87; опубл. 01.08.1988.

42. А.с. 1455976 СССР. Н03К 3/84 Устройство для формирования псевдослучайных сигналов [Текст] / Горбенко И.Д., Замула А.А., Родионов С.В., Левин П.Ю., Гавриленко (СССР). – №4210710; заявл. 16.03.87; опубл. 01.10.1988.

43. Альберт А. А. Конечные поля [Текст] / А. А. Альберт. – В киберн. сб. М.: Мир, 1966. – 242 с.

44. Амиантов И.Н. Избранные вопросы статистической теории связи [Текст] / И.Н. Амиантов. – М.: Сов. Радио, 1971. – 416с

45. Барсов, В.И. Концепция создания системы обработки информации беспилотных летательных аппаратов на основе использования кодов модулярной арифметики [Текст]/ В.И. Барсов, А.А. Сиора, В.А. Краснобаев, А.А. Замула, // Прикладная радиоэлектроника. Научно-технический журнал. – 2008. – Том 7, № 3. – С. 304–307.

46. Барсов, В.И. Метод повышения производительности и отказоустойчивости нейрокомпьютеров обработки криптографической информации автоматизиро-

ванных систем управления специального назначения на основе модулярной арифметики [Текст] / В.И. Барсов., В.А.Краснобаев, А.А. Замула, Я.В. Илюшко // Прикладная радиоэлектроника, Х.: ХНУРЭ. – 2007. – №2. – С. 282 – 289.

47. Бобало Ю. Я. Прикладне застосування теорії хаотичних систем у телекомунікація [Текст]: монографія / Ю. Я. Бобало, С. Д. Галюк, М. М. Климаш, Р. Л. Політанський; Нац. ун-т "Львів. політехніка". – Львів: Коло, 2015. – 178 с.

48. Бондаренко, М.Ф. Методологические основы концепции и политики безопасности информационных технологий [Текст] / М.Ф.Бондаренко, И.Д. Горбенко, А.А. Замула // Радиотехника, Харьков, ХНУРЭ. – 2001. – Вып. 119. – С. 5–16.

49. Бондаренко, О.В. Эксплуатационные показатели качества работы транспортной телекоммуникационной первичной сети Украины [Текст] / О.В. Бондаренко, Б.Я. Костик, Д.М. Степанов, Е.В. Левенберг // Научно-технический журнал «Технология и конструирование в электронной аппаратуре». – 2013. – Вып. 6. – С. 37–40.

50. Бондаренко, О.В. Кількісні показники надійності волоконно-оптичних ліній зв’язку в різних кліматичних умовах [Текст] / О.В. Бондаренко, Б.Я. Костік, С.В. Кіфорук, Д.М. Степанова, І.А. Слободянюк // Наукові праці ОНАЗ ім. О.С. Попова: зб. – Одеса, 2014. – №2, Ч.1. – С. 36–43.

51. Варакин Л. Е. Системы связи с шумоподобными сигналами [Текст] / Л. Е Варакин.– М.: Радио и связь,1985. – 384 с.

52. Виноградов И.М. Основы теории чисел [Текст] / И.М. Виноградов. – М.: Наука, 1965. – 162 с.

53. Гантмахер В.Е. Шумоподобные сигналы. Анализ, синтез, обработка [Текст] / В.Е. Гантмахер Н.Е., Быстров, Д.В. Чеботарев. – СПб.: Наука и техника, 2005. – 400с.

54. Горбенко И.Д. Механізми захисту інформації в каналах телекомунікацій [Текст]: учбовий посібник. Частина 1, Частина 2 / І.Д. Горбенко, О.А.Замула, І. М Пресняков. – м. Харків, ХНУРЕ, 1998. – 214 с.

55. Горбенко І.Д. Теория дискретных сигналов [Текст]: учебное пособие / Ю.В.Стасев, А.А. Замула. – МО СССР, 1988. – 119с.

56. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування [Текст]: монографія / І.Д. Горбенко, Ю.І Горбенко. – Харків.: Видавництво «Форт», 2012. – 880 с.

57. Горбенко, И.Д. Ансамблевые и корреляционные свойства криптографических сигналов для приложений телекоммуникационных систем и сетей [Текст]/ А.А. Замула, Е.А. Семенко // Радиотехника: Всеукраинский межведомственный научно – техничческий сборник – 2015 г. – Вып. 181. – С. 110 – 117.

58. Горбенко, И.Д. Защита ресурсов информационной системы на основе сложных сигналов [Текст] / И.Д. Горбенко, А.А. Замула // 4 –й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития».Сборник научных трудов. Международная конференція «Телекоммуникационные системы и технологи». – Харьков, АНПРЭ. 2011. – С. 298 – 301.

59. Горбенко, И.Д. Метод построения многофазных характеристических дискретных сигналов [Текст] / И.Д. Горбенко, А.А. Замула, Р.И Киянчук // 4 –й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития».Сборник научных трудов. Международная конференція «Телекоммуникационные системы и технологи». – Харьков. АНПРЭ. – 2011. – С. 295 – 297.

60. Горбенко, И.Д. Методы построения и исследования свойств производных нелинейных рекуррентных последовательностей [Текст]/ И.Д. Горбенко, А.А. Замула, Р.И. Киянчук // Радиотехника: Всеукраинский межведомственный научно – техничческий сборник. – 2011. – Выпуск 166/ – С. 125 – 133.

61. Горбенко, И.Д. Синтез одного класса дискретных сигналов в полях Галуа [Текст] / И.Д. Горбенко, Е.П. Колованова, А.А. Замула, Т.А. Ярыгина // Прикладная радиоелектроника: науч.- техн. журнал – 2011. – Том 10, № 2/ – С. 240 – 244.

62. Горбенко, И.Д. Синтез систем сигналов с заданными корреляционными свойствами, законами формирования, структурными и ансамблевыми свойства-

ми [Текст]/ И.Д.Горбенко, А.А. Замула // Прикладная радиоелектроника. Научно-технический журнал. Харьков. – 2012. – Том 2. – С. 293–298.

63. Горбенко, И.Д. Синтез систем сложных сигналов с заданными свойствами корреляционных функций для приложений многопользовательских систем с кодовым разделением абонентов [Текст] / И.Д. Горбенко, А.А. Замула, Е.А. Семенко // Системи обробки інформації:– Х.: ХУПС. – 2014. – Вып. 9 (125).– С. 25 – 30.

64. Горбенко, И.Д. Ускоренный метод синтеза дискретных сигналов с необходимыми свойствами для приложений телекоммуникационных систем и сетей [Текст]/ Замула А.А., Семенко Е.А // Системи обробки інформації:– Х.: ХУПС. – 2015. – Вип. 3 (128).– С. 71 – 74.

65. Горбенко Ю.І. Побудова, аналіз, стандартизація та застосування криптографічних систем [Текст] / Ю.І. Горбенко. – Харків.: Видавництво «Форт», 2015. – 959 с.

66. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Текст]. – Введ. 01–07–1990. – М.: Изд-во стандартов, 1989. – 28 с.

67. Долгов В.І. Основи статистичної теорії прийому дискретних сигналів [Текст] / В.І. Долгов. – Харків. Вид-во «Форт», 2010. – 496 с.

68. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення [Текст]. – Введ. 01–07–2015. – К.: Мінекономрозвитку України, 2015.

69. Замула, А.А. Перспективы применения нелинейных дискретных сигналов в современных телекоммуникационных системах и сетях [Текст] / А.А. Замула., Е.А. Семенко // Системи обробки інформації:– Х.: ХУПС, 2015. – Вип. 5 (130).– С. 129 – 134.

70. Замула А.А. Связь, навигация, наблюдение в системе организации воздушного движения [Текст]: монография / В.И. Черныш, А.В. Ефремов. – Харьков: Издательство Лидер, 2014. – 208 с.

71. Замула О.А. Захист інформації в системах передачі даних [Текст]: учбовий посібник. О.А Замула., Г.З. Халимов. – Харків, 1999. – 162 с.

72. Замула О.А., Нормативно – правове забезпечення інформаційної безпеки. Комплексні системи захисту інформаці [Текст]: навч. посібник / О.А. Замула, Ю.І. Горбенко, А.І. Шумов – Харків: ХНУРЕ. 2010. –248 с.

73. Замула, А.А. Методы генерации псевдослучайных последовательностей и оценка их свойств [Текст]/ А.А. Замула, Д.А. Семченко // Прикладная радиоелектроника. – 2012. –Том 2. – С. 76– 79.

74. Замула, А.А. Ансамблевые свойства характеристических дискретних сигналов [Текст] / А.А. Замула // Науково-технічний журнал Системи обробки інформації. Харьков. – 2013.– Випуск 8 (115). – С. 213 – 216.

75. Замула, А.А. Визначення найбільш небезпечних загроз в методиці оцінки інформаційних ризиків [Текст] / А.А. Замула, В.И. Черныш. // Науково-технічний журнал "Інформаційні-керуючі системи на залізничному транспорті. – 2012 – №3. – С.76–80.

76. Замула, А.А. Генераторы псевдослучайных чисел, основанные на дискретном логарифме [Текст] / А.А. Замула, Д.А. Семченко // Научно-технический журнал Технологический аудит и резервы производства. Харьков. – 2013. – № 5 (13). – С. 28–31.

77. Замула, А.А. Защита информации в информационно-телекоммуникационной системе от внутреннего нарушителя [Текст] / А.А. Замула, А.П. Шумар //Радиотехника: Всеукраинский межведомственный научно – техничнеский сборник – 2011, Выпуск 165 – С. 213 – 217.

78. Замула, А.А. Использование технологи распределенного спектра при решении некоторых классических задач приема сигналов в корпоративних системах [Текст] / Замула А.А. // Міжнародна науково-практична конференція «Перспективи розвитку інформаційних та транспортно-митних технологій у митній справі, зовнішньо економічній діяльності та управлінні організаціями», м. Дніпропетровськ. – 2011. – С. 164–166.

79. Замула, А.А. Исследование уязвимости коммуникационной сети в процессе аудита информационной безопасности [Текст]/ А.А. Замула, К.И. Іванов // Науково-технічний журнал “Інформаційні-керуючі системи на залізничному транспорті. – 2012. – №2. – С. 56–59.

80. Замула, А.А. Количественная оценка уязвимостей информационно-телекоммуникационных систем [Текст]/ А.А. Замула, С.А. Сирота, Н.И. Косиковская // Радиотехника. Всеукраинский Научно-технический сборник. – 2012. – №171, вып. 4. – С. 171–177.

81. Замула, А.А. Критерии оценки генераторов псевдослучайных последовательностей для криптографических приложений /Замула А.А., Семченко Д.А. [Текст] //15 Юбилейная Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах» . – 2012. – С. 63 – 64.

82. Замула, А.А. Метод оптимизации выбора дискретних сигналов в целях обеспечения информационной безопасности в многопользовательских телекоммуникационных системах [Текст] / А.А. Замула // Інформаційна безпека України: Наукові доповіді та тези учасників науково-технічної конференції. м. Київ. – 2015. – С.104–105.

83. Замула, А.А. Метод построения многофазных характеристических дискретных сигналов [Текст]/ А.А. Замула // Всеукраинский Научно-технический сборник Радиотехника. – 2013. – Вып. 172. С. 47–51.

84. Замула, А.А. Метод построения множества изоморфизмов характеристических кодов [Текст] // Інформаційно – керуючі системи на залізничному транспорті: науч.- техн. Журнал. – 2011, № 5 (90) – С. 32 – 37.

85. Замула, А.А. Метод синтеза сигналов с заданными ограничениями на уровень боковых лепестков корреляционной функции[Текст] / А.А. Замула, Р.И. Киянчук, Т.Е. Ярыгина, Е.П. Колованова // Восточно – европейский журнал передових технологий: науч.- техн. журнал – 2011. – № 5/9 (53)/ – С. 30 – 34.

86. Замула, А.А. Метод формирования множества дискретных сигналов с заданными корреляционными свойствами [Текст] / А.А. Замула, Т.Е. Ярыгина // 4

–й Международный радиоэлектронный форум «Прикладная радиоэлектроника. Состояние и перспективы развития».Сборник научных трудов. Международная конференція «Телекоммуникационные системы и технологи». – Харьков. АНПРЭ. – 2011. – С. 307 – 310.

87. Замула, А.А. Методология анализа рисков и управления рисками [Текст] / А.А. Замула // Радиотехника. Харьков, ХНУРЭ – 2002. – Вып. 126. – С.56–71.

88. Замула, А.А. Методология анализа рисков информационной безопасности при проектировании информационных систем с использованием нечетких сетей [Текст] / А.А. Замула, Б.В. Волобуев., В.И. Черныш // Наука і техніка Повітряних Сил Збройних Сил України: наук.- техн. журнал. Харьков – 2011. – № 2/ – С. 94 – 98.

89. Замула, А.А. Методы аутентификации в безусловно-стойких криптосистемах [Текст]/ А.А. Замула, Г.Н. Гулак // Радиотехника. Харьков, ХНУРЭ. – 2001. – Вып. 119. – С. 69–77.

90. Замула, А.А. Методы обеспечения аутентификации с введеним избыточности [Текст] / А.А. Замула, И.Д. Горбенко // Радиотехника. Харьков, ХНУРЭ – 2001. – Вып. 119. – С. 77–81.

91. Замула, А.А. Методы построения генераторов псевдослучайных последовательностей на основе параллельных вычислений с использованием графических процессоров [Текст]/ А.А. Замула, Д.А. Семченко // Наука і техніка Повітряних сил Збройних сил України. – 2014. – № 1 (14). – С. 182–186.

92. Замула, А.А. Методы построения генераторов, основапнные на дискретном логарифме [Текст] /Замула А.А., Семченко Д.А. //16-я Международная научно-практическая конф. Киев. – 2013. – С. 33–34.

93. Замула, А.А. Методы противодействия преднамеренным помехам в телекоммуникационных системах и сетях [Текст] / А.А. Замула // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. Матеріали п’ятої міжнародної науково-технічної конференції. – Полтава: ПНТУ; Баку; ВА ЗС АР; Кіровоград; КЛА НАУ; Харків; ДП «ХНДІ ТМ» – 2015. – С. 64.

94. Замула, А.А. Методы управления средствами сетевой безопасности [Текст] / Замула А.А.// І-я международная конференция «Глобальные информационные системы. Проблемы и тенденции развития». – Харьков. ХНУРЭ. – 2006. – С. 316–317.

95. Замула, А.А. Модели оценки рисков информационной безопасности [Текст] / Замула А.А., Черныш В.И. // Современные проблемы радиотехники и телекоммуникаций «РТ – 2014». Материалы 10-й международной научно – технической конференции. (Севастополь, 12-17 мая 2014 г.). – С. 315.

96. Замула, А.А. Мощность метода кодирования характеристических дискретних сигналов [Текст]/ А.А. Замула // Системи обробки інформації. – Х. ХУПС, 2014р. – Вып. 2 (118).– С. 162 – 168.

97. Замула, А.А. Обнаружение атак систем анализа сетевого трафика [Текст] / А.А. Замула, Р.И. Алиференко // Международная научно-техническая конференция «Компьютерное моделирование в наукоемких технологиях» (КМНТ-2014). Харьков, ХНУ имени Каразина В.Н.– 2014 –. 2014. – С. 11–14.

98. Замула, А.А. Оценивание временной задержки сигнала с использованием технологии распределенного спектра [Текст]/ Ю.В. Землянко // Науково-технічний журнал “Інформаційні-керуючі системи на залізничному транспорті - 2012. – №4. – С.58–63.

99. Замула, А.А. Оценивание рисков информационной безопасности в современных информационных системах [Текст] / А.А. Замула, В.И. Черныш, К.И. Иванов // 14 Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2011. С. 31.

100. Замула, А.А. Оценка защищенности информационных систем от угроз [Текст]/ Землянко Ю.В., Коваль С.Г. // Системи управління, навігації та зв’язку. – 2013. – Випуск 3 (27). – С. 123 – 128.

101. Замула, А.А. Практические аспекты имплементации международных стандартов в систему организации воздушного движения Украины [Текст]/

А.А.Замула, В.И. Черныш // Информационное противодействие угрозам терроризма. Научно-технический журнал: Россия. – 2014. – №22. – С. 111–118.

102. Замула, А.А. Предложения по построению широкополосных систем передачи со сложными сигналами [Текст]/ А.А. Замула // Радиотехника №171. Всеукраинский Научно-технический сборник. – 2012. – Вып 4. – С. 177–185.

103. Замула, А.А. Программный комплекс генерации и исследования дискретных последовательностей для приложений информационной безопасности в телекоммуникационных системах [Текст] / А.А.Замула, Е.А. Семенко // Інформаційна безпека України: Наукові доповіді та тези учасників науково-технічної конференції. м. Київ. – 2015. – С.105–106.

104. Замула, А.А. Ранжирование угроз при помощи метода анализа иерархий [Текст] / Замула А.А., Черныш В.И. // 15 Юбилейная Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2012. – С. 64 – 65.

105. Замула, А.А. Системы обнаружения и предотвращения вторжений [Текст] / А.А. Замула, В.Л. Морозов // Радиотехника: Всеукраинский межведомственный научно – техничнеский сборник. – 2014. – Вып. 176. – С. 122 – 127.

106. Замула, А.А. Теория и практика оценивания информационных рисков с использованием математического аппарата нечеткой логики [Текст] / Замула А.А., Одарченко А. // XIII Международная научно-практическая конференция. «Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2010. – С. 47–48.

107. Замула, А.А. Условия реализации динамического режима функционирования в системе связи [Текст] / А.А.Замула, Е.А.Семенко, Д.А. Семченко // Збірник наукових праць Харківського університету Повітряних сил. – 2014. – № 3 (40). – С. 113 – 116.

108. Замула, О. Принципи створення комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах [Текст] / О Замула., О. Одарченко, О. Халіна // XIII Международная научно-практическая конференция.

«Безопасность информации в информационно-телекоммуникационных системах». Киев. – 2010. – С. 103–104.

109. Замула, О.А. Аналіз і обґрунтування критеріїв і показників ефективності криптографічних генераторів псевдовипадкових чисел [Текст]/ А.А. Замула, Д.О. Семченко, Ю.В. Землянко // Системи обробки інформації:– Х.: ХУПС. – 2014р. – Вып. 4 (120).– С. 131 – 136.

110. Замула, О.А. Концепція створення комплексних систем захисту інформації в сучасних інформаційно-телекомунікаційних системах [Текст] / О.А. Замула // Системний аналіз. Інформатика. Управління (САІУ-2010): Тези доповідей Всеукраїнської науково-практичної конференції (м. Запоріжжя, 04-05 березня 2010 року)/ Міністерство освіти і науки України, Класичний приватний університет, Запорізький національний технічний університет, Академія наук вищої школи України. – Запоріжжя: Вид-во КПУ. – 2010. – С. 72–73.

111. Замула, О.А. Оцінка ефективності телекомунікаційної системи з кодовим поділом абонентів, що використовує нелінійні дискретні сигнали [Текст] / А.А. Замула // Матеріали IV міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем». м. Львів. – 2015. – С. 81–83.

112. Замула, О.А. Теоретичні основи побудови криптографічних систем абсолютної стійкості [Текст] / Замула О.А. // Науково-технічний журнал Системи обробки інформації. – 2013. – Випуск 4 (111). – С. 101–106.

113. Землянко, Ю.В. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно – телекомунікаційних системах [Текст]/ Ю.В. Землянко, О.А. Замула, О.О. Ткач // Прикладная радиоелектроника: науч.- техн. Журнал. – 2010. – Том 9, № 3 – С. 460 – 469.

114. Зюко А.Г. Теория электрической связи [Текст] / А.Г. Зюко, Д.Д., Кловский, В.И. Коржик, М.В. Назаров. – М.: Радио и связь, 1999. – 432 с.

115. Климаш М. М. Сучасні перетворення в архітектурах розподілених систем [Текст]: монографія / М.М. Климаш, А.О. Лунтовський, В.І. Романчук. – Нац. ун-т "Львівська політехніка". – Львів: Коло, 2015. – 328 с.

116. Климаш, М.М. Узагальнений метод оптимізації структур телекомунікаційної мережі за критерієм ефективності розподілу її ресурсів [Текст] / М. М. Климаш, Б. А. Бугиль // Системи оброб. інформації. – 2013. Вип. 7. – С. 72–78.

117. Колмогоров А. Н. Теория информации и теория алгоритмов [Текст] / А. Н. Колмогоров – М.: Наука, 1987. – 304 с.

118. Колмогоров А. Н. Теория передачи информации [Текст] / Колмогоров А. Н. – М.: Изд–во АН СССР, 1956. – 264 с.

119. Краснобаев, В.А Метод обработки криптографической информации в модулярной системе счисления, основанный на принципе кольцевого сдвига [Текст]/ В.А. Краснобаев, С.О. Мартыненко, Ж.В. Дейнеко, А.А. Замула, А.А. Баклыков. // Прикладная радиоэлектроника. Научно-технический журнал. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2009. – Том 8. № 3. – С. 343–350.

120. Краснобаев, В.А. Алгоритмы сжатия табличных цифровых данных результатов выполнения арифметических операций в системе остаточных классов [Текст] / В.А. Краснобаев А.А. Замула, Я.В. Илюшко // Радиотехника. Всеукр. Межвед. науч.-техн. сб. – 2005. – Вып. 141. – С. 217–225.

121. Кучук, Г.А. Математична модель технічної структури інформаційно-телекомунікаційної мережі [Текст] / Г.А. Кучук, В.В. Косенко, О.П. Давікоза // Системи обробки інформаці. Харківський університет Повітряних Сил імені Івана Кожедуба. – 2013. №6 – С. 234–237.

122. Кучук, Г.А. Метод розподілу потоків даних в мультисервісній мережі з безпроводовою компонентою [Текст] / Г.А. Кучук, Н.Х. Раковська, С.О. Загайнов, О.С Савченко // Системи обробки інформаці. Харківський університет Повітряних Сил імені Івана Кожедуба. – 2014. №4 – С. 164–169.

123. Кучук, Г.А. Метод синтезу інформаційної структури зв’язного фрагменту корпоративної мультисервісної мережі [Текст] / Г.А. Кучук // Збірник наукових праць Харківського університету Повітряних сил. – 2013. №2 – С. 97–102

124. Кучук, Г.А. Моделирование агрегированного трафика беспроводной сети передачи данных на основе статистического мониторинга информационных потоков [Текст] / Г.А. Кучук // Авиационно-космическая техника и технология Національний аерокосмічний університет імені МЄ Жуковського. – 2013. №8 – С. 260–264.

125. Кучук, Г.А. Модель процесса эволюции топологической структуры компьютерной сети системы управления объектом критического применения [Текст] / Г.А. Кучук А.А. Коваленко, А.А. Янковский // Системи обробки інформаці. Харківський університет Повітряних Сил імені Івана Кожедуба. – 2014. №74 – С. 93–96.

126. Лидл Р. Конечные поля [Текст]: монография / Р. Лидл, Г. Нидеррайтер М.: Мир, 1988. – 808 с.

127. Мартиненко, С.О. Метод снижения вычислительной сложности реализации RSA криптопреобразований на основе использования принципа кольцевого сдвиги в модулярной системе счисления [Текст] / С.О. Мартиненко, В.А. Краснобаев, О.А. Замула // Прикладная радиоелектроника: науч.- техн. журнал – 2010. – Том 9, № 3. – С. 454 – 459.

128. Мартиненко, С.О. Метод технічної реалізації арифметичних операцій у модулярній системі числення на основі використання принципу кільцевого зсуву [Текст] / С.О.Мартиненко, В.А. Краснобаєв, С.О.Кошман, О.А Замула, М.С. Деренько // Вісник ХНТУСГ імені Петра Василенка. – 2009. – Вип. 87. – С. 71 – 73.

129. Нікітюк Л.А. Архітектура інформаційних мереж [Текст]:навчальний посібник [Текст] / Нікітюк Л.А. За ред. М.В. Захарченка. – Одесса: УДАС ім. О.С. Попова, 2000. – 60 с.

130. П.П. Воробієнко Телекомунікаційні та інформаційні мережі [Текст]: підручник / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К: САММІЕ – Книга, 2010. – 708с.

131. Пат. № 49054 Україна, Пристрій для виявлення помилок у модулярній системі числення [Текст] / І.Д. Горбенко, С.О. Мартиненко, О.А. Замула, В.А.

Краснобаєв, Ю.І. Горбенко, Ж.В. Дейнеко; власник Харківський національний університет радіоелектроніки. – опубл. 12.04.2010, Бюл. № 7.

132. Пат. № 49711 Україна, Спосіб виявлення помилок у системі обробки цифрової інформації, що функціонує у модулярній системі числення [Текст] / І.Д. Горбенко, С.О. Мартиненко, О.А. Замула, В.А. Краснобаєв, Ю.І. Горбенко; власник Харківський національний університет радіоелектроніки. – опубл. 11.05.2010, Бюл. № 9.

133. Пат. № 49712 Україна, Пристрій для додавання і віднімання чисел за модулем М в модулярної системи числення [Текст] / І.Д. Горбенко, С.О. Мартиненко, О.А. Замула, В.А. Краснобаєв, В.А. Бобух, Ю.І. Горбенко; власник Харківський національний університет радіоелектроніки, – опубл. 11.05.2010, Бюл. № 10.

134. Пат. № 60078 Україна, Табличний пристрій для множення чисел за модулем m у класі лишків [Текст] / І.Д. Горбенко, М.В. Дугін, О.А. Замула, В.А. Краснобаєв, Ю.І. Горбенко; власник Харківський національний університет радіоелектроніки. – опубл. 10.06.2011, Бюл. № 11.

135. Пат. № 61798 Україна Пристрій для піднесення чисел до квадрата за модулем m класу лишків [Текст] / І.Д. Горбенко, К.В. Загумена, О.А. Замула, В.А. Краснобаєв, Ю.І. Горбенко; власник Харківський національний університет радіоелектроніки. – опубл. 25.07.2011, Бюл. № 14.

136. Пат. № 62313 Україна, Табличний пристрій для множення двох чисел за модулем m класу лишків [Текст] / І.Д. Горбенко, К.В. Загумена, О.А. Замула, В.А. Краснобаєв, Ю.І. Горбенко; власник Харківський національний університет радіоелектроніки, – опубл. 25.07.2011, Бюл. № 16.

137. Пат. № 62490 Україна, Пристрій для порівняння чисел у класі лишків [Текст] / І.Д. Горбенко, К.В. Загумена, О.А. Замула, В.А. Краснобаєв, Ю.І. Горбенко; власник Харківський національний університет радіоелектроніки, – опубл. 25.08.2011, Бюл. № 16.

138. Пат. № 91894 Україна Пристрій для перетворення позиційного двійкового коду у лишки за двома довільними модулями [Текст] / І.Д. Горбенко, О.А. Замула

ла, В.А. Краснобаєв, Ю.І. Горбенко; власник Харківський національний університет радіоелектроніки, – опубл.25.07.2014, Бюл. № 14.

139. Пат. № 92155 Україна Пристрій для перетворення позиційного двійкового коду у лишок за довільним модулем [Текст] / І.Д. Горбенко, О.А. Замула, В.А. Краснобаєв, Ю.І. Горбенко; власник Харківський національний університет радіоелектроніки, – опубл. 11.08.2014, Бюл. № 15.

140. Пестряков, В. Б. Шумоподобные сигналы в системах передачи информации [Текст] / В. Б. Пестряков, В. П. Афанасьев, В. Л. Гурвич и др.; Под ред. В. Б. Пестрякова. – М.: Сов. радио, 1973. – 424 с.

141. Петрович Н.Т. Космическая радиосвязь [Текст] / Н.Е. Петрович, Е.Ф. Каменев, М.В. Каблукова. Под. ред. Н.Т. Петровича. – М.: Сов. радио, 1979. –280 с.

142. Помехозащищенность радиосистем со сложными сигналами. Г. И. Тузов, В. А. Сивов и др. Под ред. Г. И. Тузова. – М.: Радиосвязь, 1985. – 264 с.

143. Романовский И.В. Алгоритмы решения экстремальных задач [Текст] / И.В. Романовский. – Главная редакция физико-математической литературы издательства «Наука». – М., 1977. – 349 с.

144. Свердлик М. Б. Оптимальные дискретные сигналы / М. Б. Свердлик. – М: Радио и связь, 1975. – 200 с.

145. Свердлик М. Б. Оптимальные дискретные сигналы [Текст] / Свердлик М. Б. – М: Радио и связь, 1975. – 200 с.

146. Сидельников, В.М. О взаимной корреляции последовательностей [Текст] / В.М. Сидельников // Доклады АН СССР, 1971. – т.196, №3.– С. 531 – 534.

147. Сидельников, В.М. О взаимной корреляции последовательностей [Текст] / В.М. Сидельников // Доклады АН СССР. – 1971. т.196, №3. – С. 531 – 534.

148. Спилкер Дж. Цифровая спутниковая связь [Текст] / Дж. Спилкер.– М.: Связь, 1979. – 592 с.

149. Тихонов В. И. Оптимальный прием сигналов [Текст] / В. И. Тихонов. − М.: Радио и связь, 1983. − 320 с.

150. Холл М. Комбинаторика [Текст] / М. Холл. – М.: Мир, 1970. – 421 с.

ПРИЛОЖЕНИЕ А

Программные средства синтеза и исследования свойств нелинейных дискретных сигналов в конечныхм полях Галуа

В Функции main реализован алгоритм, который позволяет пользователю ввести простое число P и получить первые 3 нелинейные сигналы характеристического типа (ХДС). Далее для этих 3-х полученных сигналов производится анализ, демонстрирующий общий принцип работы функций и программы. При необходимости, тело функции main можно изменить и настроить вывод результатов в файл.

В функции используются переменные из библиотеки для работы с большими числами - Miracl.

```
void main()
{
setlocale(LC_CTYPE,"Russian");
int             P = 0, L = 0, minQ = 2;
long int        wh = 0, qqount = 0, k = 0, y = 0;
cout << "Введите значение P:\n";              //вводим наше простое число
cin  >> P;
system("cls");
//FILE *fwrite = fopen("E:\\***.txt","wt");   - дескриптор вывода в файл.
L = P - 1;
if (L <= 1)
{
        cout << "Значение слишком малое, построение невозможно.\n\n";
        return;
};
                long int eyl = euler(L);
        long int countt = eyl;
```

```
        long int *phiL = new long int[eyl];
        long int *pervoQ = new long int[eyl];
if (eyl == 0 || eyl < 0)
{
        cout << "Количество первообразных элементов равно " << eyl << "\n";
        cout << "Построение не возможно." << "\n" << "\n";
        return;
};

cout << "Имеется: "       << eyl << " первообразных элементов." << "\n\n";
cout << "Параметры:"    << "\n";
cout << "\tПростое число:  " << P << "\n";
cout << "\tДлина:          " << L << "\n";
for (long int i = 1, j = 0; i < P; i++)
{
        if (Nod(i, L) == 1)
                {
                        phiL[j] = i;
                        j++;
                }
};

        miracl *mip = mirsys (100,0);
        big X,Z,W;

        cout<<endl;cout<<endl;

        while (wh == 0)
                {
                        X = mirvar(minQ);
```

```
                mip->IOBASE=10;
                W = mirvar(0);
                mip->IOBASE =10;
                Z = mirvar(P);
                mip->IOBASE = 10;
                power(X,(L/2),Z,W);
                        char ss[32];
                        cotstr (W,ss);
                        y = atoi(ss);
                if (y == L)
                        wh = 1;
                else
                        minQ++;
        };

cout << "Минимальный первообразный : " << minQ << "\n";

for (long int i = 0; i < eyl; i++)
{
                X = mirvar(minQ);
                mip->IOBASE=10;
                W = mirvar(0);
                mip->IOBASE =10;
                Z = mirvar(P);
                mip->IOBASE = 10;
                power(X,phiL[i],Z,W);
                        char ss[32];
                        cotstr (W,ss);
                        pervoQ[i] = atoi(ss);
};
```

```
//**** ОБЪЯВЛЕНИЕ МАССИВОВ ДЛЯ ХРАНЕНИЯ ДАННЫХ*****//

        long int *index              = new long int[L];
        fStep_Index(index, L);

        long int *ai  = new long int[L];
        long int *xi  = new long int[L];
        long int *qi  = new long int[L];
        long int *Ii   = new long int[L];
        long int *w           = new long int[L];
        long int *ww         = new long int[L];
        //переменные и массивы для децимации
        long int * coppp     = new long int[L];
        long int **decww  = new long int*[eyl];
        //массивы для функций корреляции
        long int *arrAFAK         = new long int[L];
        long int *arrPFAK= new long int[L];
        long int *arrAFVK         = new long int[L];
        long int *arrPFVK= new long int[L];
        long int *arrSFVK= new long int[L];
        long int *arrBUFFER                    = new long int[L];
        long int *arrSdvigBuffer = new long int[L];
        k = 0;
//*******************НАЧАЛО ЦИКЛА
ИСПОЛНЕНИЯ*****************************
        while (countt != 0)
        {
                decww[qqount] = new long int[L];
                        if(k==0)
                                {
```

```
                        sStep_Ai(ai, L, pervoQ[qqount], P);
                        thStep_Xi(ai, xi, L);
                        fStep_qi(qi, ai, L, P);
                        lastStep_Ii(Ii, xi, qi, L);
                        diskr_forming(Ii, w, L);
                        inverting(w, ww, L);
                        for(int i=0; i<L; i++)
                                coppp[i] = ww[i];
                };

    decimaciya(coppp, decww[qqount], L, phiL[k], P);

        if(k>=2)
        {
        cout<<"После генерирования 3-х последовательностей, полу-
ченные результаты:\n"<<endl;
        for(int i=0; i<3; i++)
                {
                cout<<"\n\tПоследовательность "<<i<<" образующий -
"<<phiL[i] <<" : \n" <<endl;
        arrPrint(decww[i], L);
                        int     pls = 0,mins = 0;
                        for(int t=0; t<L; t++)
                                {
                                        if(decww[i][t]==1)
                                                pls++;
                                        if(decww[i][t]==-1)
                                                mins++;
                                };
```

```
                                cout<<"\n\n Баланс: \t'+': "<<pls<< "   '-':
"<<mins<<endl;
                                };
                                        AFAK(decww[0], arrAFAK, L);
                                        PFAK(decww[0], arrPFAK, L);
                                        PFVK(decww[0],decww[1],arrPFVK,L);
                                        AFVK(decww[0],decww[1],arrAFVK,L);

        SFVK(decww[0],decww[1],decww[2],arrSFVK,L);
                                                inverting(decww[0],arrBUFFER,L);
                        std::cout << "\n\nAFAK:\t";
                        arrPrint(arrAFAK, L);
                        cout<<"\n\n\tМат.
ожидание:\t"<<matO(arrAFAK,L)/sqrt((float)L)<<endl;
        cout<<"\tМат. ожидание:
(модуль):\t"<<absmatO(arrAFAK,L)/sqrt((float)L)<<endl;
                        cout<<"\tДисперсия:\t"<<disp(arrAFAK,L)/sqrt((float)L)<<endl;
                        cout<<"\tДисперсия
(модуль):\t"<<absdisp(arrAFAK,L)/sqrt((float)L)<<endl;
                        cout<<"\tMin:\t"<<getMin(arrAFAK,L,1)<<endl;
                        cout<<"\tMax:\t"<<getMax(arrAFAK,L,1)<<endl;
                        std::cout << "\nPFAK:\t";
                        arrPrint(arrPFAK, L);
                        cout<<"\n\n\tМат.
ожидание:\t"<<matO(arrPFAK,L)/sqrt((float)L)<<endl;
                        cout<<"\tМат. ожидание:
(модуль):\t"<<absmatO(arrPFAK,L)/sqrt((float)L)<<endl;
                        cout<<"\tДисперсия:\t"<<disp(arrPFAK,L)/sqrt((float)L)<<endl;
                        cout<<"\tДисперсия
(модуль):\t"<<absdisp(arrPFAK,L)/sqrt((float)L)<<endl;
```

```
                cout<<"\tMin:\t"<<getMin(arrPFAK,L,1)<<endl;
                cout<<"\tMax:\t"<<getMax(arrPFAK,L,1)<<endl;
                std::cout << "\nAFVK (0 1):\t";
                arrPrint(arrAFVK, L);
                cout<<"\n\n\tМат.
ожидание:\t"<<matO(arrAFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tМат. ожидание:
(модуль):\t"<<absmatO(arrAFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tДисперсия:\t"<<disp(arrAFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tДисперсия
(модуль):\t"<<absdisp(arrAFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tMin:\t"<<getMin(arrAFVK,L,1)<<endl;
                cout<<"\tMax:\t"<<getMax(arrAFVK,L,1)<<endl;
                std::cout << "\nPFVK (0 1):\t";
                arrPrint(arrPFVK, L);
                cout<<"\n\n\tМат.
ожидание:\t"<<matO(arrPFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tМат. ожидание:
(модуль):\t"<<absmatO(arrPFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tДисперсия:\t"<<disp(arrPFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tДисперсия
(модуль):\t"<<absdisp(arrPFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tMin:\t"<<getMin(arrPFVK,L,1)<<endl;
                cout<<"\tMax:\t"<<getMax(arrPFVK,L,1)<<endl;

                std::cout << "\nSFVK (0,1,2):\t";
                arrPrint(arrSFVK, L);
                cout<<"\n\n\tМат.
ожидание:\t"<<matO(arrSFVK,L)/sqrt((float)L)<<endl;
```

```
                cout<<"\tМат. ожидание:
(модуль):\t"<<absmatO(arrSFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tДисперсия:\t"<<disp(arrSFVK,L)/sqrt((float)L)<<endl;
                cout<<"\tДисперсия
(модуль):\t"<<absdisp(arrSFVK,L)/sqrt((float)L)<<endl
                        getch();
                        return;
                    };
            k++;
            qqount++;
            countt--;
            };
};
```

После завершения этапа формирования базового изоморфизма, осуществляют анализ статистических характеристик корреляционных функций сигналов.

Результаты работы, которые выводятся в пользовательскую консоль:

```
Параметры:
    Простое число:  19
    Длина:      18
Минимальный первообразный: 2
Результаты генерирования 3-х последовательностей:
Последовательность 0, первообразный элемент поля - 1 :
-1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 1
 Баланс символов:    '+': 9   '-': 9
    Последовательность 1, первообразный - 5 :
-1 -1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 1 1 1 -1 1
 Баланс:     '+': 9   '-': 9
    Последовательность 2, первообразный - 7 :
-1 -1 1 1 -1 1 -1 1 1 1 1 -1 -1 -1 -1 -1 1 1
 Баланс:     '+': 9   '-': 9
 AFAK(0):   18 0 2 -2 -4 2 -2 4 0 2 2 2 2 2 4 2 0 0
Мат. ожидание:  0.209513
Мат. ожидание: (модуль):    0.419026
Дисперсия:    1.01196
```

Дисперсия (модуль): 0.617584
Min: 2
Max: -4

PFAK(0): 18 -2 -2 -2 -2 2 -2 2 -2 -2 -2 2 -2 2 -2 -2 -2 -2
Мат. ожидание: -0.235702
Мат. ожидание: (модуль): 0.445215
Дисперсия: 0.679377
Дисперсия (модуль): 0.235702
Min: -2
Max: -2

AFVK (0 1): 2 4 -2 -2 8 6 10 0 0 -2 2 6 2 2 0 2 0 0
Мат. ожидание: 0.471405
Мат. ожидание: (модуль): 0.628539
Дисперсия: 2.82843
Дисперсия (модуль): 2.16291
Min: 2
Max: 10
PFVK (0 1): 2 2 -6 -6 2 2 6 -10 -2 -2 -2 10 2 2 2 2 -2 -2
Мат. ожидание: -0.0261891
Мат. ожидание: (модуль): 0.811863
Дисперсия: 4.93263
Дисперсия (модуль): 4.74777
Min: 2
Max: -10
SFVK (0,1,2): 2 2 -6 -4 6 0 6 -2 -6 -2 2 6 6 -6 0 -6 -4 2
Мат. ожидание: -0.0785674
Мат. ожидание: (модуль): 0.864242
Дисперсия: 4.68478
Дисперсия (модуль): 4.13018.

Функция нахождения математического ожидания боковых выбросов функции корреляции

Параметры:

- long int *arr - массив, для которого необходимо провести подсчет;

- long int L - длина массива с данными.

```
float absmatO(long int *arr, long int L)
{
  float r = 0;
  for (int i = 0; i < L; i++)
        r = r + abs(arr[i]);
  r = r / L;
  return r;
};
```

Пример работы функции:

Данные: -1 1 1 1 1 -1 1 1 1 -1

Результат: 1

Данные: 1 2 -3 4 5 6 -7 8 9 -10

Результат: 5.5

Данные: -5 -4 -3 -2 -1 1 2 3 4 5

Результат: 3

Функция euler реализует расчет функции Эйлера.

Параметром n – число, для которого производится вычисление значения функции Эйлера.

```
int euler(int n)
{
  double t = sqrt((double)n) + 1;
  double answ = 1, ta;
  for (int i = 2; i<t; i++)
  {
        ta = 0;
        while (n%i == 0)
```

```
            {
                ta++;
                n /= i;
            };
            if (ta)
                answ *= pow((double)i, ta - 1)*(i - 1);
        }
        if (n - 1)
            answ *= (n - 1);
        return (int)answ;
};
```

Пример работы:

Значение: 13

Результат: 12

Значение: 50

Результат: 20

Значение: 87

Результат: 56

Функция Nod предназначена для нахождения наибольшего общего делителя (НОД) двух чисел.

```
long int Nod(long int a, long int b)
{
        while (a && b)
            if (a >= b)
                a %= b;
            else
                b %= a;
        return a | b;
};
```

Пример работы функции:

A: 7

B: 9

Результат: 1
A: 32
B: 38
Результат: 2
A: 36
B: 48

Функция реализует расчет значений боковых пиков периодической функции автокорреляции (ПФАК) нелинейных сигналов

Параметры функции:
- long int *arr - последовательность для поиска ПФАК;
- long int *ress - результирующий массив;
- long int size - длина последовательности;

```
void PFAK(long int *arr, long int *ress, long int size)
{
		int summ = 0;
		int s = 0;
			int *doubleArr = new int[size * 2];
		for (int i = 0; i < size; i++)
		{
			doubleArr[i] = arr[i];
			doubleArr[i + size] = arr[i];
		};
		for (int i = 0; i < size; i++)
		{
			for (int j = 0, k = i; j < size; j++, k++)
				if(arr[j]==doubleArr[k])
					summ++;

			s = summ-(size-summ);
			ress[i] = s;
			summ = 0;
			s = 0;
		};
};
```

Результаты выполнения функции:
Сигнал: -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 1
ПФАК: 18 -2 -2 -2 -2 2 -2 2 -2 -2 -2 2 -2 2 -2 -2 -2 -2
Сигнал: -1 -1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 -1 1 1
ПФАК: 28 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0

Функция реализует расчет значений боковых пиков апериодической функции взаимной корреляции (АФВК) нелинейных сигналов.

Параметры функции:
- long int *arrToRun - последовательность 1;
- long int* arrToForm - последовательность 2;
- long int *ress - результирующий массив;
- long int size - длина последовательностей;

```
void AFVK(long int *arrToRun, long int* arrToForm, long int *ress, long int size)
{
	int summ = 0;
	int s = 0;

	int *doubleArr	= new int[size];
	int *arr		= new int[size];

		for (int i = 0; i < size; i++)
			{
				doubleArr[i] = arrToForm[i];
				arr[i] = arrToRun[i];
			}

		for(int i = 0; i < size; i++)
		{

			for(int q = 0; q<i; q++)
				arr[q] = -1;
			for(int z = i, x = 0; z<size; z++, x++)
				arr[z] = arrToRun[x];
```

```
                for (int j = 0; j < size; j++)
                        if(arr[j]==doubleArr[j])
                                summ++;

                s = summ-(size-summ);
                ress[i] = s;
                summ = 0;
                s = 0;

        };
};
```

Результаты выполнения функции:

Сигнал 1: -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 1

Сигнал 2: -1 -1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 1 1 1 -1 1

АФВК: 2 4 -2 -2 8 6 10 0 0 -2 2 6 2 2 0 2 0 0

Сигнал 1: -1 -1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 -1 1 1

Сигнал 2: -1 1 1 1 -1 1 -1 -1 -1 1 1 1 1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 -1 1 -1

АФВК: 0 2 -4 0 4 -8 6 6 0 8 -4 -2 2 0 -6 -6 -6 -10 -6 -4 -6 -4 -6 0 0 -2 0 0

Функция реализует расчет значений боковых пиков апериодической функции автокорреляции (АФАК) нелинейных сигналов нелинейных сигналов

Параметры функции:

- long int * arr1 - последовательность для поиска АФАК;
- long int *ress - результирующий массив;
- long int size - длина последовательности;

```
void AFAK(long int *arr1, long int *ress, long int size)
{
        int summ = 0;
        int s = 0;

        int *doubleArr      = new int[size];
        int *arr            = new int[size];

        for(int i = 0; i < size; i++)
        {
```

```
            doubleArr[i] = arr1[i];
            arr[i] = arr1[i];
        };
        for(int i = 0; i < size; i++)
        {

            for(int q = 0; q<i; q++)
                arr[q] = -1;
            for(int z = i, x = 0; z<size; z++, x++)
                arr[z] = doubleArr[x];

            for (int j = 0; j < size; j++)
                if(arr[j]==doubleArr[j])
                    summ++;

            s = summ-(size-summ);
            ress[i] = s;
            summ = 0;
            s = 0;

        };
};
```

Результаты выполнения функции:
Сигнал: -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 1
АФАК: 18 0 2 -2 -4 2 -2 4 0 2 2 2 2 2 4 2 0 0
Сигнал: -1 -1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 -1 1 1
АФАК: 28 2 0 0 -8 0 2 -2 -4 -4 -8 -2 6 0 -2 -2 -10 -2 -2 0 2 0 -2 0 4 2 0 0

Функция реализует расчет значений боковых пиков периодической функции взаимной корреляции (ПФВК) нелинейных сигналов

Параметры функции:
- long int *arrToRun - последовательность 1;
- long int* arrToForm - последовательность 2;
- long int *ress - результирующий массив;
- long int size - длина последовательностей;

```
void PFVK(long int *arrToRun, long int* arrToForm, long int *ress, long int size)
{
	int summ = 0;
	int s = 0;
		int *doubleArr = new int[size * 2];
		for (int i = 0; i < size; i++)
		{
			doubleArr[i] = arrToForm[i];
			doubleArr[i + size] = arrToForm[i];
		};
			for (int i = 0; i < size; i++)
		{
			for (int j = 0, k = i; j < size; j++, k++)
			{
				if(arrToRun[j]==doubleArr[k])
					summ++;
			};
			s = summ-(size-summ);
			ress[i] = s;
			s = 0;
			summ = 0;
		};
};
```

Результаты выполнения функции:

Сигнал 1: -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 1
Сигнал 2: -1 -1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 1 1 1 -1 1
ПФВК: 2 2 -6 -6 2 2 6 -10 -2 -2 -2 10 2 2 2 2 -2 -2

Сигнал 1: -1 -1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 -1 1 1
Сигнал 2: -1 1 1 1 -1 1 -1 -1 -1 1 1 1 1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 -1 1 -1

ПФВК: 0 0 -4 4 8 -8 4 8 -4 8 -4 4 4 4 -8 -4 4 -4 -4 -8 -4 -8 4 8 8 -4 -4 0

Функция, реализует метод синтеза нелинейных дискретных сигналов в соответствии с заданным первообразным элементом конечного поля

Для реализации некоторых функций используются инструменты библиотеки Miracl , позволяющие работать с большими числами.

Параметры:

- long int *arr - массив в котором производится поиск;
- long int index - значение, которое необходимо найти;
- long int L - длина массива;

```
//вспомогательная функция для поиска в массиве индекса заданного элемента
long int indexSearch(long int *arr, long int index, long int L)
{
	for (long int i = 0; i < L; i++)
		{
			if (arr[i] == index)
				return i;
		};
	return -1;
};
```

Функции формирования ХДС.

```
//функции формирования дискретного сигнала
//шаг 1. Ряд сдвинутых индексов.
void fStep_Index(long int *arr, long int size)
{
	for (long int i = 0; i < size; i++)
		arr[i] = i + 1;
};
//шаг 2. Q^i mod(P);
void sStep_Ai(long int *arr, long int L, long int Q, long int P)
{
	miracl *mip = mirsys (100,0);
	big X,Z,W;
	for (long int i = 0; i < L; i++)
		{
			X = mirvar(Q);
			mip->IOBASE=10;
			W = mirvar(0);
```

```
                mip->IOBASE =10;
                Z = mirvar(P);
                mip->IOBASE = 10;
                power(X,i,Z,W);
                        char ss[32];
                        cotstr (W,ss);
                        int y = atoi(ss);
                arr[i] = y;
        };
};

//шаг 3. Считывание индесов по адрессам
void thStep_Xi(long int *ai, long int *xi, long int L)
{
        for (long int i = 0; i < L; i++)
                xi[i] = indexSearch(ai,i + 1,L)+1;
};
//шаг 4. Сдвигаем индексы на 1;
void fStep_qi(long int *qi, long int *ai, long int L, long int P)
{
        for (long int i = 0; i < L; i++)
        {
                long int t = (ai[i] + 1) % P;
                if (t == 0)
                        t = 1;
                qi[i] = t;
        };
};
//шаг 5.;
void lastStep_Ii(long int *Ii, long int *xi, long int *qi, long int L)
{
        for (long int i = 0; i < L; i++)
                Ii[i] = xi[qi[i]-1];
};
//шаг 6. Формирование инверсии ХДС;
void diskr_forming(long int *arr, long int *res, long int L)
{
        for (long int i = 0; i < L; i++)
        {
```

```
            if (arr[i] % 2 == 0)
                res[i] = 1;
            else
                res[i] = -1;
        };
};
//Шаг 7. Инвертируем и получаем базовый изоморфизм.
void inverting(long int *arr, long int *res, long int L)
{
        for (long int i = 0; i < L; i++)
            res[i] = arr[i]*(-1);
};
```

Пример 1.
Параметры:
Простое число: 13; длина: 12; первообразный = 2.

```
//Функция fStep_Index                1 2 3 4 5 6 7 8 9 10 11 12
//Функция sStep_Ai                       1 2 4 8 3 6 12 11 9 5 10 7
//Функция thStep_Xi                      1 2 5 3 10 6 12 4 9 11 8 7
//Функция fStep_qi                       2 3 5 9 4 7 1 12 10 6 11 8
//Функция lastStep_Ii                2 5 10 9 3 12 1 7 11 6 8 4
//Функция diskr_forming                  1 -1 1 -1 -1 1 -1 -1 -1 1 1 1
//Функция inverting                      -1 1 -1 1 1 -1 1 1 1 -1 -1 -1
```

Полученный изоморфизм может быть использован для синтеза всей системы нелинейных сигналов на основе метода децимации.
Пример 2.
Параметры:
Простое число: 19; длина: 18; первообразный: = 2.

```
//Функция sStep_Ai                       1 2 4 8 16 13 7 14 9 18 17 15 11 3 6 12 5
10
//Функция thStep_Xi                      1 2 14 3 17 15 7 4 9 18 13 16 6 8 12 5 11
10
//Функция fStep_qi                        2 3 5 9 17 14 8 15 10 1 18 16 12 4 7 13 6
11
//Функция lastStep_Ii              2 14 17 9 11 8 4 12 18 1 10 5 16 3 7 6 15 13
//Функция diskr_forming            1 1 -1 -1 -1 1 1 1 1 -1 1 -1 1 -1 -1 1 -1 -1
```

//Функция inverting -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 1
Пример 3.
Параметры: Простое число: 53; длина: 52; первообразный = 2.

//Функция sStep_Ai 1 2 4 8 16 32 11 22 44 35 17 34 15 30 7 14 28 3 6 12 24 48 43 33 13 26 52 51 49 45 37 21 42 31 9 18 36 19 38 23 46 39 25 50 47 41 29 5 10 20 40 27
//Функция thStep_Xi 1 2 18 3 48 19 15 4 35 49 7 20 25 16 13 5 11 36 38 50 32 8 40 21 43 26 52 17 47 14 34 6 24 12 10 37 31 39 42 51 46 33 23 9 30 41 45 22 29 44 28 27

//Функция fStep_qi 2 3 5 9 17 33 12 23 45 36 18 35 16 31 8 15 29 4 7 13 25 49 44 34 14 27 1 52 50 4 6 38 22 43 32 10 19 37 20 39 24 47 40 26 51 48 42 30 6 11 21 41 28

//Функция lastStep_Ii 2 18 48 35 11 24 20 40 30 37 36 10 5 34 4 13 47 3 15 25 43 29 9 12 16 52 1 27 44 41 39 8 23 6 49 38 31 50 42 21 45 51 26 28 22 33 14 19 7 32 46 17

//Функция diskr_forming 1 1 1 -1 -1 1 1 1 1 -1 1 1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 1 -1 -1 1 -1 1 -1 1 -1 1 -1 1 -1 -1 -1 1 1 1 -1 1 -1 -1 1 1 -1

//Функция inverting -1 -1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 -1 -1 1 1 1 1 1 1 1 1 -1 -1 -1 1 1 -1 1 1 -1 1 -1 1 -1 -1 1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 1

Функция позволяет найти минимальное значение бокового лепестка функции корреляции для нелинейного сигнала

Параметры функции:
- long int *arr - массив с данными;
- long int L - длина массива;
- int zirCount - флаг учета\не учета первого символа.

```
long int getMin(long int *arr, long int L, int zirCount)
{
	int min = L;
	if(zirCount == 0)
	{
		for(int i = 0; i<L; i++)
			if(abs(arr[i])<abs(min))
				min = arr[i];
	};
```

```
	if(zirCount == 1)
	{
		for(int i = 0; i<L; i++)
			if(abs(arr[i])<abs(min) && arr[i]!=0)
				min = arr[i];
	};
	return min;
};
```

Пример работы функции:

Массив с данными: 32 8 -8 0 0 8 -8 0 0 0 -8 8 0 0 -8 8
Длина: 16
Флаг: 1
Результат: 8
Массив с данными: 32 8 -8 0 0 8 -8 0 0 0 -8 8 0 0 -8 8
Длина: 16
Флаг: 0
Результат: 0

Массив с данными: 11 2 3 -4 -1 4 9 3 9 10
Длина: 10
Флаг: 0
Результат: 1

Функция реализует расчет значений боковых пиков стыковой функции взаимной корреляции (СФВК) нелинейных сигналов

Параметры функции:
- long int *arrToRun - 1я последовательность;
- long int* arrToForm1 - 2я последовательность;
- long int* arrToForm2 - 3я последовательность;
- long int *ress - результирующий массив;
- long int size - размер последовательностей;

```
void SFVK(long int *arrToRun, long int* arrToForm1, long int* arrToForm2, long int *ress, long int size)
{
	long int summ = 0;
	//делаем удвоение сигнала, который получили
```

```
        long int *doubleArr = new long int[size * 2];
        for (long int i = 0; i < size; i++)
        {
                doubleArr[i] = arrToForm1[i];
                doubleArr[i + size] = arrToForm2[i];
        };
        for (long int i = 0; i < size; i++)
        {
                for (long int j = 0, k = i; j < size; j++, k++)
                {
                        long int s = 0;
                        s = (arrToRun[j] * doubleArr[k]);
                        summ = summ + s;

                };
                ress[i] = summ;
                summ = 0;
        }
};
```

Результаты работы функции:

Сигнал 1: -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 -1 1 1

Сигнал 2: -1 -1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 1 1 1 -1 1

Сигнал 3: -1 -1 1 1 -1 1 -1 1 1 1 1 -1 -1 -1 -1 -1 1 1

СФВК: 2 2 -6 -4 6 0 6 -2 -6 -2 2 6 6 -6 0 -6 -4 2

Сигнал 1: -1 -1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 -1 1 1

Сигнал 2: -1 1 1 1 -1 1 -1 -1 -1 1 1 1 1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 -1 1 -1

Сигнал 3: -1 1 -1 1 1 -1 1 1 -1 1 1 1 -1 1 1 -1 -1 -1 1 -1 -1 -1 1 1 1 -1 -1 -1

СФВК: 0 0 -4 2 6 -4 6 8 -2 10 -6 -2 10 -4 -6 2 -8 -2 -6 -2 2 -6 -4 2 1 2 -2 2 -4

Функция реализует метод построения системы нелинейных сигналов на основе децимации базового изоморфизма

Параметры функции:

- long int *posl - базовая последовательность;
- long int *res - результирующий массив;
- long int size - размер последовательности;
- long int obraz - образующий элемент;

- long int P - простое число, по которому построен базовый изоморфизм;

```
void decimaciya(long int *posl, long int *res, long int size, long int obraz, long int P)
{
	long int box = 0;
	box = box - obraz;

	for (int i = 0; i < size; i++)
	{
		box = box + obraz;
		res[i] = posl[(box) % (P-1)];
	};
};
```

Результаты работы функции:

Базовый изоморфизм:-1 -1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 -1 1 1

Последовательность, полученная при использовании коэффициента децимации 3:

-1 1 1 1 -1 1 -1 -1 -1 1 1 1 1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 -1 -1 1 -1

Последовательность, полученная при использовании коэффициента децимации 5:

-1 1 -1 1 1 -1 1 1 -1 1 1 1 -1 1 1 -1 -1 -1 1 -1 -1 -1 1 1 1 -1 -1 -1

Базовая последовательность: -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 1 1 1 -1 1 1

Последовательность, полученная при использовании коэффициента децимации 5:

-1 -1 -1 -1 1 -1 -1 1 1 1 1 -1 -1 1 1 1 -1 1

Последовательность, полученная при использовании коэффициента децимации 7:

-1 -1 1 1 -1 1 -1 1 1 1 1 -1 -1 -1 -1 -1 1 1

ПРИЛОЖЕНИЕ Б

Таблица значений параметров, необходимых для синтеза нелинейных дискретных сигналов в конечных полях

(p – простое число (характеристика поля), Eul- функция Эйлера для заданного p, L –период синтезируемого сигнала, MINQ – минимальный первообразный элемент поля для заданного p)

1) P=2 L=1 Eul=1 MINQ=2
2) P=3 L=2 Eul=1 MINQ=2
3) P=5 L=4 Eul=2 MINQ=2
4) P=7 L=6 Eul=2 MINQ=3
5) P=11 L=10 Eul=4 MINQ=2
6) P=13 L=12 Eul=4 MINQ=2
7) P=17 L=16 Eul=8 MINQ=3
8) P=19 L=18 Eul=6 MINQ=2
9) P=23 L=22 Eul=10 MINQ=5
10) P=29 L=28 Eul=12 MINQ=2
11) P=31 L=30 Eul=8 MINQ=3
12) P=37 L=36 Eul=12 MINQ=2
13) P=41 L=40 Eul=16 MINQ=3
14) P=43 L=42 Eul=12 MINQ=2
15) P=47 L=46 Eul=22 MINQ=5
16) P=53 L=52 Eul=24 MINQ=2
17 P=59 L=58 Eul=28 MINQ=2
18) P=61 L=60 Eul=16 MINQ=2
19) P=67 L=66 Eul=20 MINQ=2
20) P=71 L=70 Eul=24 MINQ=7
21) P=73 L=72 Eul=24 MINQ=5
22) P=79 L=78 Eul=24 MINQ=3
23) P=83 L=82 Eul=40 MINQ=2
24) P=89 L=88 Eul=40 MINQ=3
25) P=97 L=96 Eul=32 MINQ=3
26) P=101 L=100 Eul=40 MINQ=2
27) P=103 L=102 Eul=32 MINQ=3
28) P=107 L=106 Eul=52 MINQ=2

29) P=109 L=108 Eul=36 MINQ=2
30) P=113 L=112 Eul=48 MINQ=3
31) P=127 L=126 Eul=36 MINQ=3
32) P=131 L=130 Eul=48 MINQ=2
33) P=137 L=136 Eul=64 MINQ=3
34) P=139 L=138 Eul=44 MINQ=2
35) P=149 L=148 Eul=72 MINQ=2
36) P=151 L=150 Eul=40 MINQ=3
37) P=157 L=156 Eul=48 MINQ=2
38) P=163 L=162 Eul=54 MINQ=2
39) P=167 L=166 Eul=82 MINQ=5
40) P=173 L=172 Eul=84 MINQ=2
41) P=179 L=178 Eul=88 MINQ=2
42) P=181 L=180 Eul=48 MINQ=2
43) P=191 L=190 Eul=72 MINQ=7
44) P=193 L=192 Eul=64 MINQ=5
45) P=197 L=196 Eul=84 MINQ=2
46) P=199 L=198 Eul=60 MINQ=3
47) P=211 L=210 Eul=48 MINQ=2
48) P=223 L=222 Eul=72 MINQ=3
49) P=227 L=226 Eul=112 MINQ=2
50) P=229 L=228 Eul=72 MINQ=2
51) P=233 L=232 Eul=112 MINQ=3
52) P=239 L=238 Eul=96 MINQ=7
53) P=241 L=240 Eul=64 MINQ=7
54) P=251 L=250 Eul=100 MINQ=2
55) P=257 L=256 Eul=128 MINQ=3
56) P=263 L=262 Eul=130 MINQ=5
57) P=269 L=268 Eul=132 MINQ=2
58) P=271 L=270 Eul=72 MINQ=3
59) P=277 L=276 Eul=88 MINQ=2
60) P=281 L=280 Eul=96 MINQ=3
61) P=283 L=282 Eul=92 MINQ=2
62) P=293 L=292 Eul=144 MINQ=2
63) P=307 L=306 Eul=96 MINQ=2
64) P=311 L=310 Eul=120 MINQ=11
65) P=313 L=312 Eul=96 MINQ=5
66) P=317 L=316 Eul=156 MINQ=2
67) P=331 L=330 Eul=80 MINQ=2

68) P=337 L=336 Eul=96 MINQ=5
69) P=347 L=346 Eul=172 MINQ=2
70) P=349 L=348 Eul=112 MINQ=2
71) P=353 L=352 Eul=160 MINQ=3
72) P=359 L=358 Eul=178 MINQ=7
73) P=367 L=366 Eul=120 MINQ=3
74) P=373 L=372 Eul=120 MINQ=2
75) P=379 L=378 Eul=108 MINQ=2
76) P=383 L=382 Eul=190 MINQ=5
77) P=389 L=388 Eul=192 MINQ=2
78) P=397 L=396 Eul=120 MINQ=2
79) P=401 L=400 Eul=160 MINQ=3
80) P=409 L=408 Eul=128 MINQ=7
81) P=419 L=418 Eul=180 MINQ=2
82) P=421 L=420 Eul=96 MINQ=2
83) P=431 L=430 Eul=168 MINQ=7
84) P=433 L=432 Eul=144 MINQ=5
85) P=439 L=438 Eul=144 MINQ=3
86) P=443 L=442 Eul=192 MINQ=2
87) P=449 L=448 Eul=192 MINQ=3
88) P=457 L=456 Eul=144 MINQ=5
89) P=461 L=460 Eul=176 MINQ=2
90) P=463 L=462 Eul=120 MINQ=3
91) P=467 L=466 Eul=232 MINQ=2
92) P=479 L=478 Eul=238 MINQ=13
93) P=487 L=486 Eul=162 MINQ=3
94) P=491 L=490 Eul=168 MINQ=2
95) P=499 L=498 Eul=164 MINQ=2
96) P=503 L=502 Eul=250 MINQ=5
97) P=509 L=508 Eul=252 MINQ=2
98) P=521 L=520 Eul=192 MINQ=3
99) P=523 L=522 Eul=168 MINQ=2
100) P=541 L=540 Eul=144 MINQ=2
101) P=547 L=546 Eul=144 MINQ=2
102) P=557 L=556 Eul=276 MINQ=2
103) P=563 L=562 Eul=280 MINQ=2
104) P=569 L=568 Eul=280 MINQ=3
105) P=571 L=570 Eul=144 MINQ=2
106) P=577 L=576 Eul=192 MINQ=5

107) P=587 L=586 Eul=292 MINQ=2
108) P=593 L=592 Eul=288 MINQ=3
109) P=599 L=598 Eul=264 MINQ=7
110) P=601 L=600 Eul=160 MINQ=7
111) P=607 L=606 Eul=200 MINQ=3
112 P=613 L=612 Eul=192 MINQ=2
113) P=617 L=616 Eul=240 MINQ=3
114) P=619 L=618 Eul=204 MINQ=2
115) P=631 L=630 Eul=144 MINQ=3
116) P=641 L=640 Eul=256 MINQ=3
117) P=643 L=642 Eul=212 MINQ=2
118) P=647 L=646 Eul=288 MINQ=5
119) P=653 L=652 Eul=324 MINQ=2
120) P=659 L=658 Eul=276 MINQ=2
121) P=661 L=660 Eul=160 MINQ=2
122) P=673 L=672 Eul=192 MINQ=5
123) P=677 L=676 Eul=312 MINQ=2
124) P=683 L=682 Eul=300 MINQ=2
125) P=691 L=690 Eul=176 MINQ=2
126) P=701 L=700 Eul=240 MINQ=2
127) P=709 L=708 Eul=232 MINQ=2
128) P=719 L=718 Eul=358 MINQ=11
129) P=727 L=726 Eul=220 MINQ=3
130) P=733 L=732 Eul=240 MINQ=2
131) P=739 L=738 Eul=240 MINQ=2
132) P=743 L=742 Eul=312 MINQ=5
133) P=751 L=750 Eul=200 MINQ=3
134) P=757 L=756 Eul=216 MINQ=2
135) P=761 L=760 Eul=288 MINQ=3
136) P=769 L=768 Eul=256 MINQ=7
137) P=773 L=772 Eul=384 MINQ=2
138) P=787 L=786 Eul=260 MINQ=2
139) P=797 L=796 Eul=396 MINQ=2
140) P=809 L=808 Eul=400 MINQ=3
141) P=811 L=810 Eul=216 MINQ=2
142) P=821 L=820 Eul=320 MINQ=2
143) P=823 L=822 Eul=272 MINQ=3
144) P=827 L=826 Eul=348 MINQ=2
145) P=829 L=828 Eul=264 MINQ=2

146) P=839 L=838 Eul=418 MINQ=11
147) P=853 L=852 Eul=280 MINQ=2
148) P=857 L=856 Eul=424 MINQ=3
149) P=859 L=858 Eul=240 MINQ=2
150) P=863 L=862 Eul=430 MINQ=5
151) P=877 L=876 Eul=288 MINQ=2
152) P=881 L=880 Eul=320 MINQ=3
153) P=883 L=882 Eul=252 MINQ=2
154) P=887 L=886 Eul=442 MINQ=5
155) P=907 L=906 Eul=300 MINQ=2
156) P=911 L=910 Eul=288 MINQ=7
157)P=919 L=918 Eul=288 MINQ=3
158) P=929 L=928 Eul=448 MINQ=3
159) P=937 L=936 Eul=288 MINQ=5
160) P=941 L=940 Eul=368 MINQ=2
161) P=947 L=946 Eul=420 MINQ=2
162) P=953 L=952 Eul=384 MINQ=3
163) P=967 L=966 Eul=264 MINQ=3
164) P=971 L=970 Eul=384 MINQ=2
165) P=977 L=976 Eul=480 MINQ=3
166) P=983 L=982 Eul=490 MINQ=5
167) P=991 L=990 Eul=240 MINQ=3
168) P=997 L=996 Eul=328 MINQ=2
169) P=1009 L=1008 Eul=288 MINQ=11
170) P=1013 L=1012 Eul=440 MINQ=2
171) P=1019 L=1018 Eul=508 MINQ=2
172) P=1021 L=1020 Eul=256 MINQ=2
173) P=1031 L=1030 Eul=408 MINQ=7
174) P=1033 L=1032 Eul=336 MINQ=5
175) P=1039 L=1038 Eul=344 MINQ=3
176) P=1049 L=1048 Eul=520 MINQ=3
177) P=1051 L=1050 Eul=240 MINQ=2
178) P=1061 L=1060 Eul=416 MINQ=2
179) P=1063 L=1062 Eul=348 MINQ=3
180) P=1069 L=1068 Eul=352 MINQ=2
181) P=1087 L=1086 Eul=360 MINQ=3
182) P=1091 L=1090 Eul=432 MINQ=2
183) P=1093 L=1092 Eul=288 MINQ=2
184) P=1097 L=1096 Eul=544 MINQ=3

185) P=1103 L=1102 Eul=504 MINQ=5
186) P=1109 L=1108 Eul=552 MINQ=2
187) P=1117 L=1116 Eul=360 MINQ=2
188) P=1123 L=1122 Eul=320 MINQ=2
189) P=1129 L=1128 Eul=368 MINQ=11
190) P=1151 L=1150 Eul=440 MINQ=13
191) P=1153 L=1152 Eul=384 MINQ=5
192) P=1163 L=1162 Eul=492 MINQ=2
193) P=1171 L=1170 Eul=288 MINQ=2
194) P=1181 L=1180 Eul=464 MINQ=2
195) P=1187 L=1186 Eul=592 MINQ=2
196) P=1193 L=1192 Eul=592 MINQ=3
197) P=1201 L=1200 Eul=320 MINQ=11
198) P=1213 L=1212 Eul=400 MINQ=2
199) P=1217 L=1216 Eul=576 MINQ=3
200) P=1223 L=1222 Eul=552 MINQ=5
201) P=1229 L=1228 Eul=612 MINQ=2
202) P=1231 L=1230 Eul=320 MINQ=3
203) P=1237 L=1236 Eul=408 MINQ=2
204) P=1249 L=1248 Eul=384 MINQ=7
205) P=1259 L=1258 Eul=576 MINQ=2
206) P=1277 L=1276 Eul=560 MINQ=2
207) P=1279 L=1278 Eul=420 MINQ=3
208) P=1283 L=1282 Eul=640 MINQ=2
209) P=1289 L=1288 Eul=528 MINQ=3
210) P=1291 L=1290 Eul=336 MINQ=2
211) P=1297 L=1296 Eul=432 MINQ=5
212) P=1301 L=1300 Eul=480 MINQ=2
213) P=1303 L=1302 Eul=360 MINQ=3
214) P=1307 L=1306 Eul=652 MINQ=2
215) P=1319 L=1318 Eul=658 MINQ=13
216) P=1321 L=1320 Eul=320 MINQ=7
217) P=1327 L=1326 Eul=384 MINQ=3
218) P=1361 L=1360 Eul=512 MINQ=3
219) P=1367 L=1366 Eul=682 MINQ=5
220) P=1373 L=1372 Eul=588 MINQ=2
221) P=1381 L=1380 Eul=352 MINQ=2
222) P=1399 L=1398 Eul=464 MINQ=3
223) P=1409 L=1408 Eul=640 MINQ=3

224) P=1423 L=1422 Eul=468 MINQ=3
225) P=1427 L=1426 Eul=660 MINQ=2
226) P=1429 L=1428 Eul=384 MINQ=2
227) P=1433 L=1432 Eul=712 MINQ=3
228) P=1439 L=1438 Eul=718 MINQ=7
229) P=1447 L=1446 Eul=480 MINQ=3
230) P=1451 L=1450 Eul=560 MINQ=2
231) P=1453 L=1452 Eul=440 MINQ=2
232) P=1459 L=1458 Eul=486 MINQ=2
233) P=1471 L=1470 Eul=336 MINQ=3
234) P=1481 L=1480 Eul=576 MINQ=3
235) P=1483 L=1482 Eul=432 MINQ=2
236) P=1487 L=1486 Eul=742 MINQ=5
237) P=1489 L=1488 Eul=480 MINQ=7
238) P=1493 L=1492 Eul=744 MINQ=2
239) P=1499 L=1498 Eul=636 MINQ=2
240) P=1511 L=1510 Eul=600 MINQ=11
241) P=1523 L=1522 Eul=760 MINQ=2
242) P=1531 L=1530 Eul=384 MINQ=2
243) P=1543 L=1542 Eul=512 MINQ=3
244) P=1549 L=1548 Eul=504 MINQ=2
245) P=1553 L=1552 Eul=768 MINQ=3
246) P=1559 L=1558 Eul=720 MINQ=17
247) P=1567 L=1566 Eul=504 MINQ=3
248) P=1571 L=1570 Eul=624 MINQ=2
249) P=1579 L=1578 Eul=524 MINQ=2
250) P=1583 L=1582 Eul=672 MINQ=5
251) P=1597 L=1596 Eul=432 MINQ=2
252) P=1601 L=1600 Eul=640 MINQ=3
253) P=1607 L=1606 Eul=720 MINQ=5
254) P=1609 L=1608 Eul=528 MINQ=7
255) P=1613 L=1612 Eul=720 MINQ=2
256) P=1619 L=1618 Eul=808 MINQ=2
257) P=1621 L=1620 Eul=432 MINQ=2
258) P=1627 L=1626 Eul=540 MINQ=2
259) P=1637 L=1636 Eul=816 MINQ=2
260) P=1657 L=1656 Eul=528 MINQ=5
261) P=1663 L=1662 Eul=552 MINQ=3
262) P=1667 L=1666 Eul=672 MINQ=2

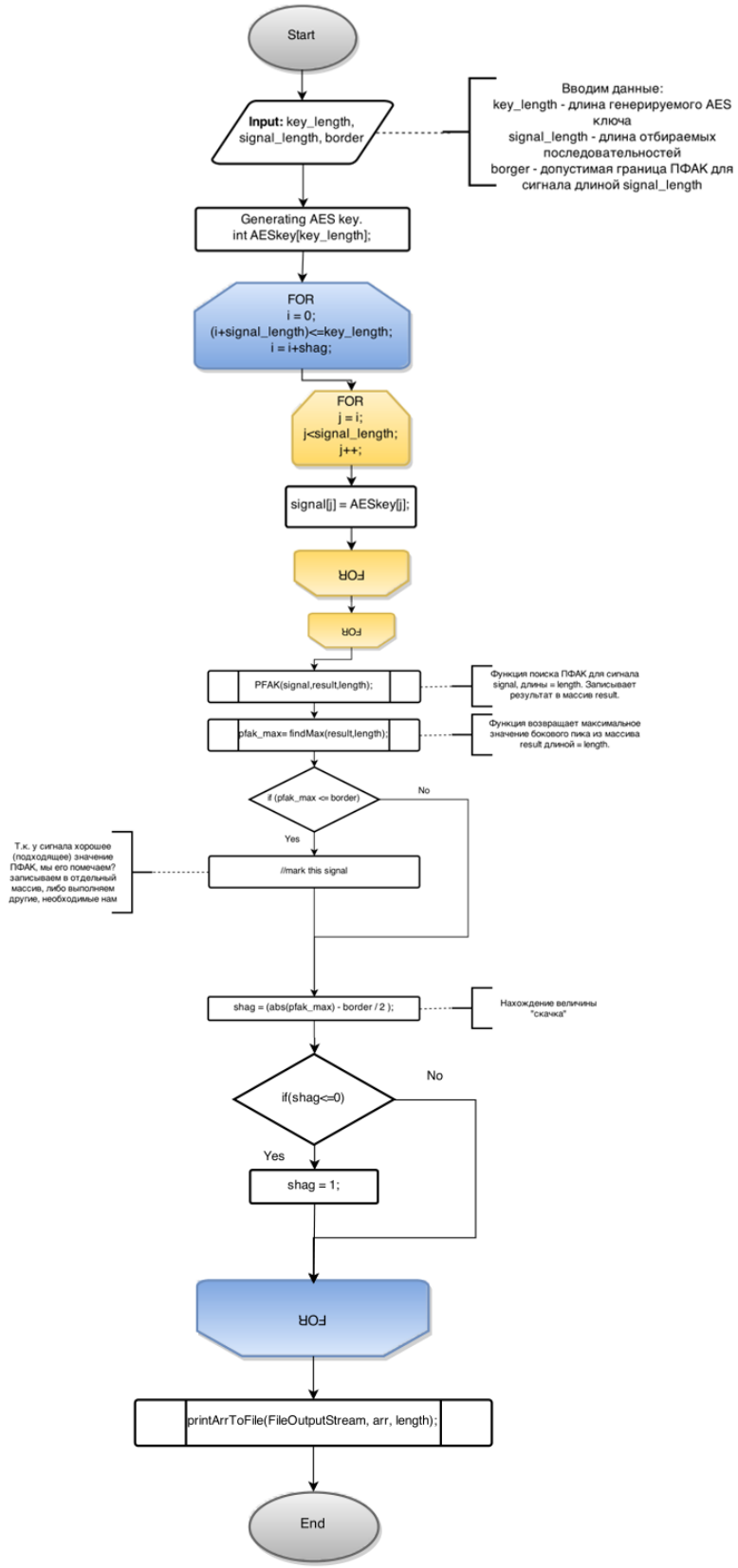
263) P=1669 L=1668 Eul=552 MINQ=2
264) P=1693 L=1692 Eul=552 MINQ=2
265) P=1697 L=1696 Eul=832 MINQ=3
266) P=1699 L=1698 Eul=564 MINQ=2
267) P=1709 L=1708 Eul=720 MINQ=2
268) P=1721 L=1720 Eul=672 MINQ=3
269) P=1723 L=1722 Eul=480 MINQ=2
270) P=1733 L=1732 Eul=864 MINQ=2
271) P=1741 L=1740 Eul=448 MINQ=2
272) P=1747 L=1746 Eul=576 MINQ=2
273) P=1753 L=1752 Eul=576 MINQ=5
274) P=1759 L=1758 Eul=584 MINQ=3
275) P=1777 L=1776 Eul=576 MINQ=5
276) P=1783 L=1782 Eul=540 MINQ=3
277) P=1787 L=1786 Eul=828 MINQ=2
278) P=1789 L=1788 Eul=592 MINQ=2
279) P=1801 L=1800 Eul=480 MINQ=11
280) P=1811 L=1810 Eul=720 MINQ=2
281) P=1823 L=1822 Eul=910 MINQ=5
282) P=1831 L=1830 Eul=480 MINQ=3
283) P=1847 L=1846 Eul=840 MINQ=5
284) P=1861 L=1860 Eul=480 MINQ=2
285) P=1867 L=1866 Eul=620 MINQ=2
286) P=1871 L=1870 Eul=640 MINQ=7
287) P=1873 L=1872 Eul=576 MINQ=5
288) P=1877 L=1876 Eul=792 MINQ=2
289) P=1879 L=1878 Eul=624 MINQ=3
290) P=1889 L=1888 Eul=928 MINQ=3
291) P=1901 L=1900 Eul=720 MINQ=2
292) P=1907 L=1906 Eul=952 MINQ=2
293) P=1913 L=1912 Eul=952 MINQ=3
294) P=1931 L=1930 Eul=768 MINQ=2
295) P=1933 L=1932 Eul=528 MINQ=2
296) P=1949 L=1948 Eul=972 MINQ=2
297) P=1951 L=1950 Eul=480 MINQ=3
298) P=1973 L=1972 Eul=896 MINQ=2
299) P=1979 L=1978 Eul=924 MINQ=2
300) P=1987 L=1986 Eul=660 MINQ=2
301) P=1993 L=1992 Eul=656 MINQ=5

302) P=1997 L=1996 Eul=996 MINQ=2
303) P=1999 L=1998 Eul=648 MINQ=3
304) P=2003 L=2002 Eul=720 MINQ=2
305) P=2011 L=2010 Eul=528 MINQ=2
306) P=2017 L=2016 Eul=576 MINQ=5
307) P=2027 L=2026 Eul=1012 MINQ=2
308) P=2029 L=2028 Eul=624 MINQ=2
309) P=2039 L=2038 Eul=1018 MINQ=7
310) P=2053 L=2052 Eul=648 MINQ=2
311) P=2063 L=2062 Eul=1030 MINQ=5
312) P=2069 L=2068 Eul=920 MINQ=2
313) P=2081 L=2080 Eul=768 MINQ=3
314) P=2083 L=2082 Eul=692 MINQ=2
315) P=2087 L=2086 Eul=888 MINQ=5
316) P=2089 L=2088 Eul=672 MINQ=7
317) P=2099 L=2098 Eul=1048 MINQ=2
318) P=2111 L=2110 Eul=840 MINQ=7
319) P=2113 L=2112 Eul=640 MINQ=5
320) P=2129 L=2128 Eul=864 MINQ=3
321) P=2131 L=2130 Eul=560 MINQ=2
322) P=2137 L=2136 Eul=704 MINQ=5
323) P=2141 L=2140 Eul=848 MINQ=2
324) P=2143 L=2142 Eul=576 MINQ=3
325) P=2153 L=2152 Eul=1072 MINQ=3
326) P=2161 L=2160 Eul=576 MINQ=7
327) P=2179 L=2178 Eul=660 MINQ=2
328) P=2203 L=2202 Eul=732 MINQ=2
329) P=2207 L=2206 Eul=1102 MINQ=5
330) P=2213 L=2212 Eul=936 MINQ=2
331) P=2221 L=2220 Eul=576 MINQ=2
332) P=2237 L=2236 Eul=1008 MINQ=2
333) P=2239 L=2238 Eul=744 MINQ=3
334) P=2243 L=2242 Eul=1044 MINQ=2
335) P=2251 L=2250 Eul=600 MINQ=2
336) P=2267 L=2266 Eul=1020 MINQ=2
337) P=2269 L=2268 Eul=648 MINQ=2
338) P=2273 L=2272 Eul=1120 MINQ=3
339) P=2281 L=2280 Eul=576 MINQ=7
340) P=2287 L=2286 Eul=756 MINQ=3

341) P=2293 L=2292 Eul=760 MINQ=2
342) P=2297 L=2296 Eul=960 MINQ=3
343) P=2309 L=2308 Eul=1152 MINQ=2
344) P=2311 L=2310 Eul=480 MINQ=3
345) P=2333 L=2332 Eul=1040 MINQ=2
346) P=2339 L=2338 Eul=996 MINQ=2
347) P=2341 L=2340 Eul=576 MINQ=2
348) P=2347 L=2346 Eul=704 MINQ=2
349) P=2351 L=2350 Eul=920 MINQ=13
350) P=2357 L=2356 Eul=1080 MINQ=2
351) P=2371 L=2370 Eul=624 MINQ=2

ПРИЛОЖЕНИЕ В

Блок синтеза алгоритма, реализующего метод синтеза нелинейных крипто-графических дискретных сигналов



Функция main, реализующая полученный метод синтеза нелинейных дискретных криптографических сигналов

```
public class test {
                    //глобальные переменные;
    static int  len         = 128;          //константа длины ключа (размерность);
    static int  key_size    = 64;       //длина последовательности;
    static int  border          = 17;       //допустимая граница для ПФАК;

                    //переменные для подсчета нулей и единиц;
    static int  zir         = 0;
    static int  one         = 0;

public static void main(String[] args) throws NoSuchAlgorithmException, NoSuchProviderException, ParseException, IOException, NoSuchPaddingException {
    //начало

                /***************Объявление переменных*****************/
    long start_time = 0;                //переменная для подсчета времени работы;

    int keyAES[]    = new int[key_size];    //сгенерированный ключ AEC в виде битов;
    int code[]  = new int[key_size];    //сгенерированный ключ AEC в виде битов;

    int good_signal[][]     = new int[len][key_size];
                    //массив сигналов, которые проходят границу отбора
    int good_pfak[][]  = new int[len][key_size+2];
                    //массив PFAK сигналов, которые проходят границу отбора                 //границы увеличины на 2, для записи "мин" и "макс" значений
                    //для экономии ресурсов (чтоб не приходилось всегда вычислять -
                    //мы вычислим их 1 раз и будем хранить.
```

```
        int ress[]     = new int[key_size];      //массив для получения результатов корр.функций


                                                  //создаем поток вывода;
        FileOutputStream fout    =                          new                FileOut-
putStream("E:\\results_"+key_size+".txt");

        BufferedWriter bw              =  new  BufferedWriter(new  OutputStreamWrit-
er(fout, "UTF8"));
        BufferedReader reader  =  new  BufferedReader(new  InputStreamRead-
er(System.in));

                                          //подключение библиотеки AES;
        Security.addProvider(new
org.bouncycastle.jce.provider.BouncyCastleProvider());
                                          //установка параметров генератора;
        KeyGenerator generator = KeyGenerator.getInstance("AES", "BC");
        generator.init(len);          //инициализация генератора;

        Key keyToBeWrapped = generator.generateKey();
        //генерируем ключ;
        String gets = new String(keyToBeWrapped.getEncoded());      //переводим его в строку;

        getBits(gets,code);          //вызов функции перевода ключа в биты;

                int iter = 0;
                int buf = 0;
                int otb = 0;
                int count_pfak = 0;

        while(true)                       //цикл отбора сигналов по ПФАК;
        {
                iter = buf + otb;
                buf  = iter;
```

```
        if(iter+key_size>=len)   //проверка: не перешли ли мы границу значений ключа;
            break;

            for(int q = 0; q<key_size; q++) //отбор каждых следующих H бит.
                {                           //из длинного ключа, сгенерированного AEC
                    code[q] = keyAES[iter];
                    iter++;
                };
            PFAK(code,ress,key_size);           //находим ПФАК сигнала;

        int min = findMinPFAK(ress,key_size);   //находим минимальный пик;
        int max = findMaxPFAK(ress,key_size);   //находим максимальный пик;

        if(Math.abs(max)<=border)               //если максимальный пик <= допустимой границы;
        {
            one = 0;
            zir = 0;

            for(int i = 0; i<key_size; i++)
            {
                good_pfak[count_pfak][i]    = ress[i];  //запоминаем ПФАК сигнала;
                good_signal[count_pfak][i] = code[i];//запоминаем сам сигнал;
            };

            good_pfak[count_pfak][key_size]     = min;  //сохраняем мин для ПФАК в          //специальное "место" в массиве;
            good_pfak[count_pfak][key_size+1] = max;//сохраняем макс для ПФАК в          //специальное "место" в массиве
            bw.write((count_pfak+1)+")");       //пишем в файл порядковый номер сигнала;
            bw.flush();
```

```
            printArrToFile(fout,good_pfak[count_pfak],key_size);    //записываем
сигнал в файл;

            OICount(good_pfak[count_pfak],key_size);          //подсчет кол-ва 1 и 0 ;

            bw.write("\t1: "+one+" 0:"+zir);                  //записываем после сигнала
кол-во 1 и 0;

            if(zir == one)                                    //если количество 0 и 1 равно ;
                  bw.write(" + ");

            bw.write("\n");
            bw.flush();

            count_pfak++;                                     //увеличиваем счетчик хоро-
ших сигналов;
      };
            otb = ((Math.abs(max) - border)+1) / 2;           //вычисление величины
"скачка";

                  if(otb<=0)                                  //если скачек <= 0
                        otb = 1;                              //устанавливаем его величи-
ну =1;
      };
            //После того, как "хорошие" сигналы отобраны и записаны в файл;
            //запишем ПФАК этих сигналов в файл.
            bw.write("\n\tПФАК отобранных сигналов:\n\n");
            bw.flush();

for(int i = 0; i<count_pfak; i++)
{
            bw.write((i+1)+")");
            bw.flush();
            printArrToFile(fout,good_pfak[i],key_size);

      bw.write("\t          min:          "+good_pfak[i][key_size]+"\tmax:
"+good_pfak[i][key_size+1]+"\t\n");
      bw.flush();
```

```
};
        bw.write("\tОтобрано по ПФАК: "+count_pfak+"\n");
        bw.flush();
};

//конец
};
```

Пример реализации метода синтеза нелинейных дискретных криптографических сигналов и расчета статистических характеристик корреляционных функций (дисперсия боковых пиков – DISP, математическое ожидание - MatO, минимальных - MIN и максимальных боковых пиков - MAX)

1) -111-111-11-11-111-11-1-111-111-1-1-1-1-1-11111 1: 17 -1: 15 DISP: 0,9906
2) -1-1-1-11-111-1-11-111-1-1-1-111-11-11-11-1-11-111 1: 14 -1: 18 DISP: 0,9906
3) -1111-111-1-11-1-1-1-11-1-1-1-1-11111-11-1-1-11-11 1: 14 -1: 18 DISP: 0,9906
4) -11-1-1-11-11-1-1-11-1111-1-11-1-1-111-1-11-1111-1 1: 14 -1: 18 DISP: 0,9906
5) -1-11-1-11-11-11-1-1-11-11-1-1-11-1-111-1111-1-111 1: 14 -1: 18 DISP: 0,9906
6) -1-1-111-111-11-1-11-1-11-1-1-1-11-111-1-1-1-11111 1: 14 -1: 18 DISP: 0,9906
7) -1-111-1-111-11-1-11-11-1-1-1-1-1-1-1-1-1-11-11-1-11-1 1: 10 -1: 22 DISP: 0,8742
8) -11-1-1-1-111-1-11-1-1-111-1-1-111-1-11-1-1-111-11-1 1: 12 -1: 20 DISP: 0,9491
9) -1-1111-11-1-1-1-1-1111-1-11-1-111-11-11-1-11-111 1: 15 -1: 17 DISP: 0,9990
10) -11-11-1111-11-1-1-111-1-11111-1-11-111111-1-1 1: 18 -1: 14 DISP: 0,9740
11) -1-11-111-11-1-1-1-1-11-1-1-111-11-11-1-11-1-1-1-11-1 1: 11 -1: 21 DISP: 0,9158
12) -1-111-1-1-11-11-11-1-111-1-111-1-1-11-11111111 1: 17 -1: 15 DISP: 0,9906

13) -11-11-11-1-1-1-11-1-1-111-1-111-111-1-1-1-1-1111-1 1: 13 -1: 19
DISP: 0,9740
14) -1-1-111-1-11-1111-1-111-1-111-111-1-11111-11-1 1: 17 -1: 15
DISP: 0,9906
15) -111-1-11-1-1-1-111-111-1-11-111-111-11-111-1-1-1 1: 15 -1: 17
DISP: 0,9990
16) -1-111-111-1-1-1-1-111-1-1-11-111-1-1-1-1-1-1-1-1-11-1 1: 10 -1: 22
DISP: 0,8742
17) -111-111-11-1-11-111-1-1-1-1-11-1-11-1-1111111-1 1: 16 -1: 16
DISP: 0,9990
18-1-1-1111-11-11-111-1-1-1-11-11-11-11-1-11-1-11-11 1: 14 -1: 18
DISP: 0,9906
19) -1-1-1111-1-1-1-1111-11-1-1-11-11-1-11-1-1-11-1-111 1: 13 -1: 19
DISP: 0,9740
20) -11-1-11-1-11-1-111111-1-11-11-1-1-11-1-1-111-111 1: 15 -1: 17
DISP: 0,9990
21) -1-111-1-111-1-1-1-111-1-1-1-111-1-1-1-1-11-1-11-1-1-1 1: 10 -1: 22
DISP: 0,8742
22) -1-11-111-1-1-1-11-1-11-1-1-1-1111111-11-1-1-1-11-1 1: 13 -1: 19
DISP: 0,9740
23) -1-1-1-1111-1-1-1-1-1-1111-11-1-11-111-1-1111-1-11 1: 14 -1: 18
DISP: 0,9906
24) -1-11-111-11-1-1111-11-1-1-1-11111-1-1-111-111-1 1: 16 -1: 16
DISP: 0,9990
25) -1-11-1-11-11-11-111111-111-11-11-1-1-111111-1 1: 18 -1: 14
DISP: 0,9740
26) -11111111-1111-11-1-1-11-1-11-111-11-11-11-1-1 1: 18 -1: 14
DISP: 0,9740
27) -1-1-11-11-1-1-1-1-1-11-1-11-1-1-1-1-1-1-11-1-1-1-11-11-1-11 1: 8 -1: 24
DISP: 0,7661
28) 111111-11-111-1111-1-1111-1-111-11-11-111-1 1: 21 -1: 11 DISP: 0,9158
29) -1-1-11-11-1-1-11-111-111-1-1-1-111-1-1-1-11-1-111-1 1: 12 -1: 20
DISP: 0,9491
30) -11-1-111-1-1-11-11-111-1-1-111-11-1-1111111-11 1: 17 -1: 15
DISP: 0,9906
31) -11-1111-1-1-111-1-11-11-1-1-1-1-1-1-11-1-111-1111 1: 14 -1: 18
DISP: 0,9906

32) -1-1-11-1111-1-1-111-11-1-111-1-1-11-1-11-1-11111 1: 15 -1: 17
DISP: 0,9990

ПФВК:

1) 32 -14 14 -14 -14 -14 -14 -14 16 14 -12 -12 -16 -12 12 10 14 10 -12 -20 -14 -12 -10 18 14 10 -10 12 10 12 -10 12 MatO: -1,4375
MIN: 10 MAX: -20

2) -14 32 16 -12 12 16 12 12 14 12 14 -10 -18 14 14 16 -16 12 -14 14 16 14 16 -12 16 8 12 -10 16 -10 12 14 MatO: 7,2500 MIN: 8 MAX: -18

3) 14 16 32 16 -20 12 12 12 10 16 18 -14 -14 14 -10 12 -16 12 18 14 8 -14 -12 12 -12 12 12 -10 16 -14 12 14 MatO: 5,1250 MIN: 8 MAX: -20

4) -14 -12 16 32 20 -12 12 12 -14 -12 -10 10 14 14 -10 16 8 8 14 -14 12 14 12 -16 16 -12 16 -14 12 -10 12 -14 MatO: 3,7500 MIN: 8 MAX: 20

5) -14 -12 -20 20 32 12 -12 12 -14 -20 -14 14 -14 -14 10 -12 16 12 18 10 8 10 8 -12 -12 -12 12 -14 12 14 12 -10 MatO: 1,2500 MIN: 8 MAX: -20

6) -14 16 -12 -12 12 32 12 16 -14 -12 -10 -10 14 -14 -18 12 16 12 14 14 12 14 16 12 -12 -12 12 -10 12 -10 12 -14 MatO: 3,1250 MIN: -10 MAX: -18

7) -14 -12 12 12 12 -12 32 16 14 -12 18 -14 14 14 10 16 12 12 10 -14 16 10 12 -8 -16 -12 16 -14 12 -10 12 10 MatO: 5,2500 MIN: -8 MAX: 18

8) -14 12 12 -12 12 16 16 32 -10 -12 10 -14 18 -14 14 12 12 16 14 14 12 10 16 -12 -8 -8 12 -22 12 -10 16 14 MatO: 5,6250 MIN: -8 MAX: -22

9) 16 14 10 -14 -14 -14 14 -10 32 -10 8 8 16 16 -12 14 -18 -10 12 -12 10 12 22 14 14 10 10 -12 -10 8 -14 -16 MatO: 2,4375 MIN: 8 MAX: 22

10) 14 12 16 -12 -20 12 12 12 -10 32 10 -14 -10 10 -14 -8 12 -12 18 -14 -12 -14 -16 12 12 16 12 18 -16 14 -12 -14 MatO: 1,0000 MIN: -8 MAX: -20

11) 12 14 18 10 -14 10 18 10 8 -10 32 16 16 -16 12 14 10 18 -12 16 14 20 10 -14 -14 -14 18 -12 14 -12 10 12 MatO: 6,3125 MIN: 8 MAX: 20

12) 12 -10 -14 10 14 10 14 -14 8 -14 16 32 -16 16 -12 -10 10 -18 -12 -12 -10 16 10 -10 10 -14 10 -16 10 12 -18 12 MatO: 0,3125 MIN: 8 MAX: -18

13) -16 -18 -14 14 14 14 14 18 16 -10 16 -16 32 -16 -12 22 -10 10 12 16 10 12 -14 -14 -14 14 14 -16 -14 -12 14 -16 MatO: 2,0625 MIN: -10 MAX: 22

14) -12 14 -14 14 14 -14 -14 -14 16 -10 -16 16 -16 32 16 -10 -14 -10 16 -12 -10 16 -14 10 14 -14 -14 -12 -14 -12 -10 16 MatO: -1,5625 MIN: -10 MAX: 16

15) -12 14 -10 -10 -10 -18 -10 14 12 -14 12 -12 12 16 32 14 18 -18 -8 12 -10 12 18 14 10 14 10 -12 18 12 -14 -16 MatO: 3,1875 MIN: -8 MAX: -18

16) -10 16 12 16 12 12 16 12 14 -8 14 -10 22 -10 14 32 -12 12 14 14 16 18 12 16 12 -12 16 -14 16 -10 12 -14 MatO: 8,1250 MIN: -8 MAX: 22

17) 14 -16 -16 8 16 16 12 12 -18 12 10 10 10 -14 -18 12 32 -16 10 -18 -12 -14 12 16 -12 8 12 14 -16 -14 12 -14 MatO: 1,1250 MIN: 8 MAX: -18

18) 10 12 12 8 -12 -12 12 16 10 12 18 -18 10 -10 -18 12 -16 32 10 10 8 10 -8 -12 12 -16 12 -18 12 14 16 10 MatO: 4,0000 MIN: 8 MAX: 18
19) -12 -14 18 14 18 -14 10 14 -12 18 12 -12 12 16 -8 14 -10 -10 32 12 18 12 -18 18 -14 -10 18 -12 10 -16 10 -16 MatO: 3,4375 MIN: -8 MAX: 18
20) -20 14 14 14 -10 14 -14 14 -12 -14 16 -12 -16 -12 12 14 -18 -10 12 32 -14 16 -10 -14 14 14 10 12 14 16 -14 -12 MatO: 2,1875 MIN: -10 MAX: -20
21) -14 16 8 12 8 12 16 12 10 -12 14 -10 10 10 10 16 12 8 18 -14 32 14 12 12 -12 -16 16 -14 16 -14 12 10 MatO: 7,0000 MIN: 8 MAX: 18
22) 12 14 14 14 10 14 10 10 12 -14 20 16 12 16 12 18 -14 10 -12 16 14 32 10 10 18 -14 18 -12 14 12 -14 -12 MatO: 7,9375 MIN: 10 MAX: 20
23) -10 16 -12 -12 8 16 12 16 22 -16 10 10 14 -14 18 12 -12 -8 -18 10 12 10 32 -16 12 -12 12 -14 16 10 12 -14 MatO: 4,1250 MIN: 8 MAX: 22
24) 18 12 -12 -16 -12 12 8 -12 14 -12 -14 10 14 10 14 16 16 12 18 -14 12 10 -16 32 12 16 12 14 12 18 -8 -14 MatO: 5,1250 MIN: 8 MAX: 18
25) 14 16 12 16 -12 -12 -16 8 14 12 -14 10 -14 14 10 12 -12 -12 -14 14 -12 18 12 12 32 -12 -16 14 12 -10 -8 -14 MatO: 1,8750 MIN: 8 MAX: 18
26) 10 8 12 -12 -12 -12 12 -8 -10 16 -14 -14 14 -14 14 -12 8 -16 10 -14 -16 -14 -12 16 -12 32 -12 14 12 10 -16 10 MatO: -1,0000 MIN: 8 MAX: 16
27) -10 -12 12 16 -12 12 16 12 10 12 18 10 14 -14 -10 16 12 12 18 10 16 18 12 12 -16 -12 32 -18 16 10 8 10 MatO: 7,5000 MIN: 8 MAX: 18
28) -12 10 -10 -14 -14 -10 -14 -22 -12 18 -12 -16 -16 -12 12 -14 14 -18 -12 12 -14 -12 -14 -14 14 14 -18 32 -14 16 -14 -12 MatO: -5,1875 MIN: 10 MAX: -22
29) 10 16 16 12 -12 12 12 12 10 -16 14 -10 14 -14 18 16 -16 12 10 14 16 14 16 12 12 12 16 -14 32 14 12 -14 MatO: 7,7500 MIN: 10 MAX: 18
30) -12 10 -14 10 -14 -10 -10 10 8 -14 12 12 -12 12 12 -10 14 14 -16 16 -14 12 10 -18 10 -10 10 16 14 32 -14 -12 MatO: 2,0625 MIN: 8 MAX: -18
31) 10 12 -12 12 12 12 12 16 -14 -12 10 -18 14 -10 -14 12 -12 16 10 -14 12 -14 -12 -8 -8 -16 8 -14 12 -14 32 18 MatO: 0,8750 MIN: -8 MAX: -18
32) 12 14 14 14 -10 -14 10 14 -16 14 12 12 -16 -16 -16 -14 -14 -10 -16 -12 10 -12 -14 -14 -14 -10 10 -12 -14 -12 18 32 MatO: -2,5625 MIN: -10 MAX: 18
ALL: MIN: 8 MAX: -22
ПФАК:
1) 32 -4 0 8 -8 -4 -4 0 0 0 4 -4 -4 8 -8 -4 12 -4 -8 8 -4 -4 4 0 0 0 -4 -4 -8 8 0 -4
MatO: -0,8750 MIN: -8 MAX: 12
2) 32 -8 0 0 -12 0 8 0 4 0 -8 4 0 4 0 4 -8 4 0 4 0 4 -8 0 4 0 8 0 -12 0 0 -8
MatO: -0,5000 MIN: -12 MAX: 8
3) 32 0 4 0 4 -8 0 -8 4 0 -8 0 4 0 -4 4 0 4 -4 0 4 0 -8 0 4 -8 0 -8 4 0 4 0
MatO: -0,5000 MIN: -8 MAX: 4

4) 32 -4 -4 -4 8 -8 -4 4 4 -4 0 4 -8 0 -4 12 0 12 -4 0 -8 4 0 -4 4 4 -4 -8 8 -4 -4 -4
MatO: -0,5000 MIN: -8 MAX: 12
5) 32 -8 -4 0 12 -8 0 0 8 -8 0 0 4 -8 4 0 0 0 4 -8 4 0 0 -8 8 0 0 -8 12 0 -4 -8
MatO: -0,5000 MIN: -8 MAX: 12
6) 32 0 -4 4 -16 0 4 0 16 0 -4 0 -12 4 -4 -4 16 -4 -4 4 -12 0 -4 0 16 0 4 0 -16 4 -4 0
MatO: -0,5000 MIN: -16 MAX: 16
7) 32 0 4 8 4 12 0 4 4 4 0 8 0 4 4 -4 8 -4 4 4 0 8 0 4 4 4 0 12 4 8 4 0 MatO: 3,5000 MIN: -4 MAX: 12
8) 32 0 -12 0 4 8 -4 -4 8 8 0 -4 0 12 4 -4 0 -4 4 12 0 -4 0 8 8 -4 -4 8 4 0 -12 0
MatO: 1,0000 MIN: -12 MAX: 12
9) 32 -4 -4 0 -4 -4 -4 0 8 -4 4 8 -16 0 4 4 -4 4 4 0 -16 8 4 -4 8 0 -4 -4 -4 0 -4 -4
MatO: -0,8750 MIN: -16 MAX: 8
10) 32 0 0 -8 0 -8 4 -8 4 0 8 0 8 0 0 -8 0 -8 0 0 8 0 8 0 4 -8 4 -8 0 -8 0 0
MatO: -0,5000 MIN: -8 MAX: 8
11) 32 -4 4 4 0 8 -4 0 0 4 -4 0 8 4 4 8 4 8 4 4 8 0 -4 4 0 0 -4 8 0 4 4 -4
MatO: 2,1250 MIN: -4 MAX: 8
12) 32 0 -4 -4 12 0 -8 -4 4 -4 -8 0 12 -8 -8 -4 20 -4 -8 -8 12 0 -8 -4 4 -4 -8 0 12 -4 -4 0
MatO: -0,8750 MIN: -8 MAX: 20
13) 32 0 -4 -4 4 0 -8 8 0 4 -8 0 0 0 8 0 4 0 8 0 0 0 -8 4 0 8 -8 0 4 -4 -4 0
MatO: 0,1250 MIN: -8 MAX: 8
14) 32 0 -12 0 4 -4 -4 4 4 -4 -8 8 0 -8 0 4 4 4 0 -8 0 8 -8 -4 4 4 -4 -4 4 0 -12 0
MatO: -0,8750 MIN: -12 MAX: 8
15) 32 -4 -8 8 -8 0 8 -12 4 12 -4 -4 4 -12 4 4 -12 4 4 -12 4 -4 -4 12 4 -12 8 0 -8 8 -8 -4
MatO: -0,8750 MIN: -12 MAX: 12
16) 32 8 0 4 4 0 0 12 4 -4 4 4 -4 0 12 12 0 12 12 0 -4 4 4 -4 4 12 0 0 4 4 0 8
MatO: 3,5000 MIN: -4 MAX: 12
17) 32 0 -4 12 -8 -4 4 0 4 4 -8 -4 0 -16 0 8 -8 8 0 -16 0 -4 -8 4 4 0 4 -4 -8 12 -4 0
MatO: -1,0000 MIN: -16 MAX: 12
18) 32 -12 8 -8 0 0 4 -4 8 -8 8 -16 12 -8 12 -4 0 -4 12 -8 12 -16 8 -8 8 -4 4 0 0 -8 8 -12
MatO: -0,5000 MIN: -16 MAX: 12
19) 32 0 -4 -8 0 -4 4 8 4 4 -4 -4 0 8 -8 4 4 4 -8 8 0 -4 -4 4 4 8 4 -4 0 -8 -4 0
MatO: 0,1250 MIN: -8 MAX: 8
20) 32 -4 -4 8 -4 -4 4 -8 -4 0 -4 -4 0 4 0 0 12 0 0 4 0 -4 -4 0 -4 -8 4 -4 -4 8 -4 -4
MatO: -0,8750 MIN: -8 MAX: 12
21) 32 8 -8 0 0 4 16 8 -8 4 12 4 4 4 -4 4 16 4 -4 4 4 4 12 4 -8 8 16 4 0 0 -8 8
MatO: 3,5000 MIN: -8 MAX: 16
22) 32 4 4 4 -4 0 -4 -4 0 0 -8 0 4 -4 0 8 4 8 0 -4 4 0 -8 0 0 -4 -4 0 -4 4 4 4
MatO: 0,1250 MIN: -8 MAX: 8

23) 32 4 -4 -4 -8 0 -4 -4 4 12 4 4 -8 -4 4 -4 0 -4 4 -4 -8 4 4 12 4 -4 -4 0 -8 -4 -4 4
MatO: -0,5000 MIN: -8 MAX: 12
24) 32 0 -4 -4 -12 -4 -8 12 8 4 8 -16 -4 -8 -4 12 8 12 -4 -8 -4 -16 8 4 8 12 -8 -4 -12 -4 -4
0 MatO: -1,0000 MIN: -16 MAX: 12
25) 32 -4 8 -4 0 -4 -4 0 0 0 -4 0 -4 4 -8 12 0 12 -8 4 -4 0 -4 0 0 0 -4 -4 0 -4 8 -4
MatO: -0,5000 MIN: -8 MAX: 12
26) 32 -4 8 0 4 -4 0 0 -4 -4 0 -8 4 -4 4 -8 16 -8 4 -4 4 -8 0 -4 -4 0 0 -4 4 0 8 -4
MatO: -0,5000 MIN: -8 MAX: 16
27) 32 0 8 8 4 8 8 12 4 12 8 8 8 0 8 12 8 12 8 0 8 8 8 12 4 12 8 8 4 8 8 0
MatO: 7,0000 MIN: 0 MAX: 12
28) 32 -4 0 0 4 12 -4 4 0 4 8 -4 8 0 0 4 4 4 0 0 8 -4 8 4 0 4 -4 12 4 0 0 -4
MatO: 2,1250 MIN: -4 MAX: 12
29) 32 0 -4 0 -4 0 12 -4 0 12 -4 4 0 -12 4 12 0 12 4 -12 0 4 -4 12 0 -4 12 0 -4 0 -4 0
MatO: 1,0000 MIN: -12 MAX: 12
30) 32 -4 0 -4 0 4 -4 0 4 -4 8 -16 4 -4 0 4 -4 4 0 -4 4 -16 8 -4 4 0 -4 4 0 -4 0 -4
MatO: -0,8750 MIN: -16 MAX: 8
31) 32 0 0 0 8 0 8 -4 0 -8 4 -4 0 -8 4 -8 0 -8 4 -8 0 -4 4 -8 0 -4 8 0 8 0 0 0 MatO: -0,5000 MIN: -8 MAX: 8
32) 32 0 -8 -4 -4 -4 4 4 4 -4 -4 4 -4 4 0 0 -4 0 0 4 -4 4 -4 -4 4 4 4 -4 -4 -4 -8 0
MatO: -0,8750 MIN: -8 MAX: 4
ALL: MIN: -16 MAX: 20
АФАК:
1) 32 -3 0 7 -8 -7 -6 1 -2 1 6 -1 -2 3 -4 -5 6 1 -4 5 -2 -3 -2 -1 2 -1 2 3 0 1 0 -1
MatO: -0,4375 MIN: -8 MAX: 7
2) 32 -7 2 1 -10 -1 6 1 -2 3 -6 1 4 3 -2 5 -4 -1 2 1 -4 3 -2 -3 6 -1 2 1 -2 -1 -2 -1
MatO: -0,2500 MIN: -10 MAX: 6
3) 32 1 2 1 2 -7 -2 -3 4 1 -8 5 -2 -3 -4 1 0 3 0 3 6 -5 0 -1 0 -5 2 -1 2 -1 2 -1 MatO: -0,2500 MIN: -8 MAX: 6
4) 32 -5 -2 -5 8 -9 2 1 6 -5 0 -1 0 -1 -2 7 0 5 -2 1 -8 5 0 1 -2 3 -6 1 0 1 -2 1 MatO: -0,2500 MIN: -9 MAX: 8
5) 32 -7 -2 -1 10 -5 2 -1 8 -7 4 -1 2 -1 0 -5 0 5 4 -7 2 1 -4 -1 0 1 -2 -3 2 1 -2 -1
MatO: -0,2500 MIN: -7 MAX: 10
6) 32 1 -2 7 -14 -1 2 -5 12 1 -4 3 -8 1 0 -5 8 1 -4 3 -4 -3 0 -1 4 5 2 1 -2 -3 -2 -1
MatO: -0,2500 MIN: -14 MAX: 12
7) 32 -1 4 9 2 11 2 5 2 1 2 5 0 5 -4 1 4 -5 8 -1 0 3 -2 3 2 -1 -2 1 2 -1 0 1
MatO: 1,7500 MIN: -5 MAX: 11
8) 32 -1 -10 -3 6 7 -6 -1 8 9 -4 -7 -2 15 2 -5 0 1 2 -3 2 3 4 -1 0 -3 2 1 -2 3 -2 1
MatO: 0,5000 MIN: -10 MAX: 15

9) 32 -3 -2 -1 -6 -5 -6 1 8 1 4 9 -10 -5 0 -1 -2 5 4 5 -6 -1 0 -5 0 -1 2 1 2 1 -2 -1
MatO: -0,4375 MIN: -10 MAX: 9
10) 32 -1 0 -7 0 -7 4 -5 4 1 2 1 2 -1 2 -3 0 -5 -2 1 6 -1 6 -1 0 -3 0 -1 0 -1 0 1
MatO: -0,2500 MIN: -7 MAX: 6
11) 32 -5 4 5 -4 9 -6 -1 4 -1 0 -1 4 7 -2 7 2 1 6 -3 4 1 -4 5 -4 1 2 -1 4 -1 0 1 MatO: 1,0625 MIN: -6 MAX: 9
12) 32 1 -2 -3 12 1 -6 -1 4 -3 -6 1 10 -5 -4 -3 10 -1 -4 -3 2 -1 -2 -1 0 -3 -2 -1 0 -1 -2 -1
MatO: -0,4375 MIN: -6 MAX: 12
13) 32 -1 -2 -5 6 -3 -6 5 0 3 -4 3 -2 -1 4 1 2 -1 4 1 2 -3 -4 1 0 3 -2 3 -2 1 -2 1
MatO: 0,0625 MIN: -6 MAX: 6
14) 32 -1 -12 -1 6 -3 -2 7 4 -9 -6 9 6 -9 -4 5 2 -1 4 1 -6 -1 -2 5 0 -3 -2 -1 -2 1 0 1 MatO: -0,4375 MIN: -12 MAX: 9
15) 32 -5 -8 9 -6 -1 4 -11 4 9 -6 -5 6 -5 0 3 -6 1 4 -7 -2 1 2 3 0 -1 4 1 -2 -1 0 1
MatO: -0,4375 MIN: -11 MAX: 9
16) 32 7 0 5 2 -3 2 11 2 -3 4 3 -4 3 8 5 0 7 4 -3 0 1 0 -1 2 1 -2 3 2 -1 0 1
MatO: 1,7500 MIN: -4 MAX: 11
17) 32 -1 -2 13 -10 -3 4 -3 2 1 -6 -5 -2 -7 -2 5 -4 3 2 -9 2 1 -2 3 2 3 0 -1 2 -1 -2 1
MatO: -0,5000 MIN: -10 MAX: 13
18) 32 -11 8 -7 -2 -1 2 -3 6 -5 4 -11 10 -7 12 -3 0 -1 0 -1 2 -5 4 -3 2 -1 2 1 2 -1 0 -1
MatO: -0,2500 MIN: -11 MAX: 12
19) 32 1 -2 -7 -2 -7 2 9 4 5 -4 -3 -4 5 -6 3 2 1 -2 3 4 -1 0 -1 0 -1 2 3 2 -1 -2 -1
MatO: 0,0625 MIN: -7 MAX: 9
20) 32 -3 -4 7 0 -5 2 -3 -6 -1 -2 -5 -4 3 -4 -1 6 1 4 1 4 1 -2 1 2 -5 2 1 -4 1 0 -1
MatO: -0,4375 MIN: -6 MAX: 7
21) 32 7 -10 -1 2 5 12 7 -4 3 6 1 4 3 -2 5 8 -1 -2 1 0 3 6 1 -4 1 4 -1 -2 1 2 1
MatO: 1,7500 MIN: -10 MAX: 12
22) 32 3 4 5 -8 1 -6 -5 2 -1 -4 -1 0 -3 0 3 2 5 0 -1 4 1 -4 1 -2 1 2 -1 4 -1 0 1
MatO: 0,0625 MIN: -8 MAX: 5
23) 32 5 -4 -5 -8 -1 -2 -1 6 11 0 3 -4 -1 0 -5 0 1 4 -3 -4 1 4 1 -2 -3 -2 1 0 1 0 -1
MatO: -0,2500 MIN: -8 MAX: 11
24) 32 -1 -4 -1 -14 -3 -4 7 8 3 4 -9 -2 -7 -4 9 4 3 0 -1 -2 -7 4 1 0 5 -4 -1 2 -3 0 1
MatO: -0,5000 MIN: -14 MAX: 9
25) 32 -5 8 -1 0 -3 0 -1 0 -1 -2 -3 -4 5 -8 11 0 1 0 -1 0 3 -2 1 0 1 -4 -1 0 -3 0 1
MatO: -0,2500 MIN: -8 MAX: 11
26) 32 -5 8 3 4 -1 0 3 -4 -3 0 -7 4 -5 0 -3 8 -5 4 1 0 -1 0 -1 0 -3 0 -3 0 -3 0 1
MatO: -0,2500 MIN: -7 MAX: 8
27) 32 1 8 7 2 9 8 11 6 5 8 5 6 1 4 5 4 7 4 -1 2 3 0 7 -2 1 0 -1 2 1 0 -1
MatO: 3,5000 MIN: -2 MAX: 11

28) 32 -3 0 -1 4 11 -4 1 2 3 6 -1 2 5 -4 3 2 1 4 -5 6 -3 2 1 -2 3 0 1 0 1 0 -1
MatO: 1,0625 MIN: -5 MAX: 11
29) 32 -1 -4 1 -2 -3 12 -5 -2 9 -2 -1 2 -9 -2 7 0 5 6 -3 -2 5 -2 3 2 1 0 3 -2 -1 0 1
MatO: 0,5000 MIN: -9 MAX: 12
30) 32 -3 -2 -1 0 3 -2 3 4 -5 8 -11 -2 3 2 3 -2 1 -2 -7 6 -5 0 1 0 -3 -2 1 0 -3 2 -1
MatO: -0,4375 MIN: -11 MAX: 8
31) 32 1 0 1 6 1 4 -5 2 -5 0 -3 0 -5 4 -9 0 1 0 -3 0 -1 4 -3 -2 1 4 -1 2 -1 0 -1
MatO: -0,2500 MIN: -9 MAX: 6
32) 32 1 -6 -1 -2 -3 2 1 2 -7 -6 9 -2 -1 0 -1 -2 1 0 5 -2 -5 2 3 2 3 2 -1 -2 -3 -2 -1
MatO: -0,4375 MIN: -7 MAX: 9
ALL: MIN: -14 MAX: 15
АФВК:
1) 32 10 6 7 6 12 9 6 10 8 8 6 13 6 8 11 12 10 9 8 7 9 5 10 14 10 6 10 10 11 6 12
MatO: 8,5938 MIN: 5 MAX: 14
2) 8 32 12 10 7 10 14 12 14 9 9 7 9 9 13 13 9 11 8 14 16 14 10 9 7 8 9 6 12 8 7 8
MatO: 10,5000 MIN: 6 MAX: 16
3) 10 6 32 9 6 10 11 13 11 12 10 9 8 13 6 9 9 8 15 10 8 10 5 7 10 12 8 8 10 8 8 12
MatO: 9,7813 MIN: 5 MAX: 15
4) 8 11 11 32 18 8 7 11 7 8 9 10 14 10 8 8 8 8 11 8 9 9 8 7 16 8 9 8 9 7 12 10
MatO: 9,9688 MIN: 7 MAX: 18
5) 9 8 10 8 32 9 9 11 8 8 10 14 9 8 6 9 13 10 15 11 8 10 9 9 8 8 11 8 15 10 14 9
MatO: 10,2188 MIN: 6 MAX: 15
6) 12 11 8 6 9 32 11 10 14 6 12 7 10 7 10 10 9 10 12 12 9 7 11 11 7 6 8 8 10 6 10 12
MatO: 9,7188 MIN: 6 MAX: 14
7) 7 10 8 8 8 8 32 9 10 11 13 10 8 8 10 13 6 7 6 13 16 10 8 7 5 9 11 8 8 8 11 10
MatO: 9,6563 MIN: 5 MAX: 16
8) 7 9 8 8 10 10 8 32 7 8 11 10 10 6 11 9 8 7 16 14 13 11 12 6 4 6 10 7 8 8 13 7
MatO: 9,5938 MIN: 4 MAX: 16
9) 10 14 12 13 8 10 10 10 32 7 9 9 12 13 7 14 6 8 10 8 10 8 11 10 8 5 11 5 11 9 10 12
MatO: 10,0625 MIN: 5 MAX: 14
10) 11 11 8 9 10 11 5 11 7 32 5 10 7 10 10 4 5 12 9 8 8 8 12 11 8 12 10 10 6 10 8 11
MatO: 9,3125 MIN: 4 MAX: 12
11) 8 12 10 7 10 10 15 12 8 7 32 5 7 9 11 14 12 9 9 10 10 20 8 6 10 10 17 15 11 7 6 8
MatO: 10,5313 MIN: 5 MAX: 20
12) 12 10 8 12 14 8 10 10 7 10 13 32 13 16 8 8 7 8 10 9 12 9 10 7 10 8 9 8 6 12 10 15
MatO: 10,2813 MIN: 6 MAX: 16
13) 6 9 10 14 14 13 11 13 8 12 11 10 32 12 6 10 9 10 11 15 8 8 10 7 10 10 10 10 11 6
12 8 MatO: 10,6250 MIN: 6 MAX: 15

14) 7 13 9 16 12 7 6 8 10 8 7 16 12 32 5 7 9 8 8 7 7 7 9 10 10 6 9 8 11 10 8 15
MatO: 9,6875 MIN: 5 MAX: 16
15) 7 14 10 7 10 8 7 11 11 10 11 7 8 12 32 6 10 10 9 12 9 12 15 9 8 14 9 8 13 8 8 6
MatO: 10,1250 MIN: 6 MAX: 15
16) 9 11 11 11 8 10 12 8 14 5 14 6 14 7 14 32 7 10 9 9 16 10 7 9 7 8 13 6 13 6 10 8
MatO: 10,1563 MIN: 5 MAX: 16
17) 8 10 8 8 12 16 12 6 9 8 10 9 9 6 13 9 32 11 9 10 12 10 11 16 8 8 11 14 13 6 8 6
MatO: 10,3125 MIN: 6 MAX: 16
18) 10 12 10 9 10 9 8 11 9 10 13 6 9 7 10 10 5 32 11 8 8 11 8 8 7 14 12 10 12 12 12 6
MatO: 9,9688 MIN: 5 MAX: 14
19) 8 11 15 9 5 8 8 10 8 11 10 5 8 8 5 9 7 7 32 12 12 9 7 10 6 6 11 7 10 9 10 10
MatO: 9,2188 MIN: 5 MAX: 15
20) 9 14 10 7 8 7 12 14 8 10 12 4 8 6 12 8 13 8 12 32 9 12 11 6 11 10 10 10 12 10 9 10
MatO: 10,1563 MIN: 4 MAX: 14
21) 6 16 9 10 6 8 16 10 10 9 10 8 10 8 9 16 8 7 8 7 32 9 6 12 5 12 12 9 14 8 8 10 MatO: 10,0625 MIN: 5 MAX: 16
22) 10 14 13 9 10 18 9 10 10 8 20 13 8 13 12 11 12 9 8 11 11 32 10 10 11 7 17 8 12 10 10 10 MatO: 11,4375 MIN: 7 MAX: 20
23) 9 14 10 11 8 10 12 9 18 8 7 7 9 11 11 9 7 12 7 8 8 8 32 12 8 6 10 4 10 7 9 10 MatO: 9,7500 MIN: 4 MAX: 18
24) 11 9 8 11 9 12 7 10 9 9 9 10 12 10 10 8 16 11 10 7 10 11 11 32 12 11 9 9 12 13 7 6
MatO: 10,3125 MIN: 6 MAX: 16
25) 14 11 9 16 8 8 6 8 8 8 10 10 9 7 10 6 8 8 9 9 7 14 8 12 32 8 9 11 12 8 8 10
MatO: 9,5938 MIN: 6 MAX: 16
26) 10 12 12 5 7 6 11 6 8 12 10 8 6 13 14 8 8 12 9 10 6 6 5 7 7 32 7 14 6 8 8 8
MatO: 9,0938 MIN: 5 MAX: 14
27) 6 11 9 14 10 13 16 11 11 5 12 10 11 8 8 13 8 12 13 8 14 7 9 8 5 10 32 4 16 10 8 10
MatO: 10,5000 MIN: 4 MAX: 16
28) 6 8 8 5 7 4 6 9 7 10 8 6 5 7 12 5 14 8 7 8 2 8 9 9 8 14 3 32 7 8 6 4
MatO: 7,9375 MIN: 2 MAX: 14
29) 10 11 13 14 12 9 8 6 7 10 8 6 11 8 14 10 8 12 10 12 12 8 12 12 12 12 16 4 32 6 8 10
MatO: 10,4063 MIN: 4 MAX: 16
30) 9 8 6 10 10 10 8 13 8 10 9 8 9 8 11 8 15 12 11 8 12 11 9 15 11 8 11 8 8 32 8 8
MatO: 10,0938 MIN: 6 MAX: 15
31) 10 8 6 8 12 10 10 9 8 6 7 6 8 7 10 11 8 14 11 10 11 7 8 9 7 8 10 8 11 6 32 20 MatO: 9,5625 MIN: 6 MAX: 20
32) 12 15 9 10 10 11 10 10 9 7 10 8 9 10 8 8 6 8 8 11 11 9 9 11 10 5 10 7 8 9 7 32
MatO: 9,5313 MIN: 5 MAX: 15
ALL: MIN: 2 MAX: 20

Анализ по ПФАК: 9

ПФАК 32 0 4 0 4 -8 0 -8 4 0 -8 0 4 0 -4 4 0 4 -4 0 4 0 -8 0 4 -8 0 -8 4 0 4 0 MatO: -0,5000 MIN: -8 MAX: 4

3) -1111-111-1-11-1-1-1-11-1-1-1-1-11111-11-1-1-11-11 1: 14 -1: 18 DISP: 0,9906

ПФАК 32 0 0 -8 0 -8 4 -8 4 0 8 0 8 0 0 -8 0 -8 0 0 8 0 8 0 4 -8 4 -8 0 -8 0 0 MatO: -0,5000 MIN: -8 MAX: 8

10) -11-11-1111-11-1-1-111-1-11111-1-11-111111-1-1 1: 18 -1: 14 DISP: 0,9740

ПФАК 32 0 -4 -4 4 0 -8 8 0 4 -8 0 0 0 8 0 4 0 8 0 0 0 -8 4 0 8 -8 0 4 -4 -4 0 MatO: 0,1250 MIN: -8 MAX: 8

13) -11-11-11-1-1-1-11-1-1-111-1-111-111-1-1-1-1-1111-1 1: 13 -1: 19 DISP: 0,9740

ПФАК 32 0 -4 -8 0 -4 4 8 4 4 -4 -4 0 8 -8 4 4 4 -8 8 0 -4 -4 4 4 8 4 -4 0 -8 -4 0 MatO: 0,1250 MIN: -8 MAX: 8

19) -1-1-1111-1-1-1-1111-11-1-1-11-11-1-11-1-1-11-1-111 1: 13 -1: 19 DISP: 0,9740

ПФАК 32 0 0 0 8 0 8 -4 0 -8 4 -4 0 -8 4 -8 0 -8 4 -8 0 -4 4 -8 0 -4 8 0 8 0 0 0 MatO: -0,5000 MIN: -8 MAX: 8

31) -11-1111-1-1-111-1-11-11-1-1-1-1-1-1-1-11-1-111-1111 1: 14 -1: 18 DISP: 0,9906

ПФАК 32 0 -8 -4 -4 -4 4 4 4 -4 -4 4 -4 4 0 0 -4 0 0 4 -4 4 -4 -4 4 4 4 -4 -4 -4 -8 0 MatO: -0,8750 MIN: -8 MAX: 4

32) -1-1-11-1111-1-1-111-11-1-111-1-1-11-1-11-1-11111 1: 15 -1: 17 DISP: 0,9990

Сигналы, значения боковых выбросов ПФВК которых, не превышают предельно достижимой границы: 9

1) -4 -4 -4 -4 8 -4 0 0 -4 -8 4 0 -4 4 0 4 4 0 0 -4 -4 0 -4 0 8 -8 0 0 -8 8 0 8 MatO: -0,3750

Signals: 2 26

-1-1-1-11-111-1-11-111-1-1-1-111-11-11-11-1-11-111 1: 14 -1: 18 DISP: 0,9906

-11111111-1111-11-1-1-11-1-11-111-11-11-11-1-1 1: 18 -1: 14 DISP: 0,9740

3) 0 0 -4 4 8 8 0 0 -4 0 4 0 0 8 8 0 8 0 -4 4 0 -4 4 0 0 4 0 -8 0 8 4 0 MatO: 1,5000

Signals: 3 21

-1111-111-1-11-1-1-1-11-1-1-1-1-11111-11-1-1-11-11 1: 14 -1: 18 DISP: 0,9906

-1-111-1-111-1-1-1-111-1-1-1-111-1-1-1-1-11-1-11-1-1-1 1: 10 -1: 22 DISP: 0,8742

5) 8 -4 -8 -4 4 0 0 4 4 -8 -8 8 4 -4 8 8 4 -8 -4 0 -8 4 4 0 -4 -4 -4 -8 4 8 -4 8 MatO: -0,2500

Signals: 4 17

-11-1-1-11-11-1-1-11-1111-1-11-1-1-111-1-11-1111-1 1: 14 -1: 18 DISP: 0,9906

-111-111-11-1-11-111-1-1-1-1-11-1-11-1-1111111-1 1: 16 -1: 16 DISP: 0,9990

7) 0 -4 -4 0 0 -4 8 0 8 -4 0 0 0 4 4 0 4 -8 4 -8 -4 8 4 0 0 4 4 -8 4 0 8 -4 MatO: 0,5000

Signals: 4 18

-11-1-1-11-11-1-1-11-1111-1-11-1-1-111-1-11-1111-1 1: 14 -1: 18 DISP: 0,9906

-1-1-1111-11-11-111-1-1-1-11-11-11-11-1-11-1-11-11 1: 14 -1: 18 DISP: 0,9906

9) 4 -4 -4 4 4 4 0 -4 4 4 0 0 8 8 0 0 4 -4 -4 8 8 0 -4 4 -4 4 8 -4 -4 4 4 0 MatO: 1,3750

Signals: 5 21

-1-11-1-11-11-11-1-1-11-11-1-1-11-1-111-1111-1-111 1: 14 -1: 18 DISP: 0,9906

-1-111-1-111-1-1-1-111-1-1-1-111-1-1-1-1-11-1-11-1-1-1 1: 10 -1: 22 DISP: 0,8742

11) 8 8 -4 -8 4 0 0 0 4 -4 -4 0 0 4 -4 8 -4 -8 4 0 -4 4 4 4 8 -4 -4 0 0 8 0 -4 MatO: 0,2500

Signals: 5 23

-1-11-1-11-11-11-1-1-11-11-1-1-11-1-111-1111-1-111 1: 14 -1: 18 DISP: 0,9906

-1-1-1-1111-1-1-1-1-1-1111-11-1-11-111-1-1111-1-11 1: 14 -1: 18 DISP: 0,9906

13) 4 -4 4 -4 0 4 -8 4 0 4 -4 -8 8 0 0 0 0 4 0 0 0 -4 -4 0 4 0 -8 8 4 -4 0 0 MatO: -0,1250

Signals: 7 24

-1-111-1-111-11-1-11-11-1-1-1-1-1-1-1-1-1-1-11-11-1-11-1 1: 10 -1: 22 DISP: 0,8742

-1-11-111-11-1-1111-11-1-1-1-11111-1-1-111-111-1 1: 16 -1: 16 DISP: 0,9990

15) 0 0 -4 0 -4 -8 0 8 0 -8 -4 4 -4 -4 4 -4 4 -4 -8 4 4 -4 4 -4 4 -8 -4 4 -8 0 0 8 MatO: -1,0000

Signals: 8 25

-11-1-1-1-111-1-11-1-1-111-1-1-111-1-11-1-1-111-11-1 1: 12 -1: 20 DISP: 0,9491

-1-11-1-11-11-11-111111-111-11-11-1-1-111111-1 1: 18 -1: 14 DISP: 0,9740

17) 0 -8 -4 4 -4 -4 4 0 0 -4 4 -4 -4 0 0 8 0 -8 -4 8 -8 -4 8 -4 0 -8 0 4 0 4 -8 0 MatO: -1,0000

Signals: 8 26

-11-1-1-1-111-1-11-1-1-111-1-1-111-1-11-1-1-111-11-1 1: 12 -1: 20 DISP: 0,9491

-11111111-1111-11-1-1-11-1-11-111-11-11-11-1-1 1: 18 -1: 14 DISP: 0,9740

19) 8 4 0 0 0 8 0 -4 0 4 -8 4 -8 0 8 -4 8 0 0 4 0 -4 8 -4 8 -4 0 0 -4 0 -8 4 MatO: 0,3750

Signals: 9 11

-1-1111-11-1-1-1-1-1111-1-11-1-111-11-11-1-11-111 1: 15 -1: 17 DISP: 0,9990

-1-11-111-11-1-1-1-1-11-1-1-111-11-11-1-11-1-1-1-11-1 1: 11 -1: 21 DISP: 0,9158

21) 0 0 -4 0 -4 8 4 -4 -4 0 -4 4 0 4 0 0 4 -4 -4 -8 -4 0 4 0 -4 0 4 8 -4 4 4 -4 MatO: -0,1250

Signals: 9 12

-1-1111-11-1-1-1-1-1111-1-11-1-111-11-11-1-11-111 1: 15 -1: 17 DISP: 0,9990

-1-111-1-1-11-11-11-1-111-1-111-1-1-11-11111111 1: 17 -1: 15 DISP: 0,9906

23) -4 8 -4 -4 -8 4 4 4 4 -8 -4 0 4 0 -4 8 4 -8 -8 -8 4 -4 4 8 -4 8 -4 -4 0 4 4 0 MatO: 0,0000

Signals: 9 30

-1-1111-11-1-1-1-1-1111-1-11-1-111-11-11-1-11-111 1: 15 -1: 17 DISP: 0,9990

-11-1-111-1-1-11-11-111-1-1-111-11-1-1111111-11 1: 17 -1: 15 DISP: 0,9906

25) 4 -4 -4 -4 -8 -4 0 0 -4 -4 4 4 4 -8 -4 -4 4 4 0 -4 -4 0 -8 -4 4 4 0 -4 -4 0 -8 4 MatO: -1,6250

Signals: 10 16
-11-11-1111-11-1-1-111-1-11111-1-11-111111-1-1 1: 18 -1: 14
DISP: 0,9740
-1-111-111-1-1-1-1-111-1-1-11-111-1-1-1-1-1-1-1-1-11-1 1: 10 -1: 22
DISP: 0,8742

27) 4 4 -4 4 0 -8 -8 0 4 8 8 -8 -4 4 -4 -4 4 8 4 0 -4 0 4 0 0 8 0 0 -8 0 4 -4 MatO: 0,2500
Signals: 15 19
-111-1-11-1-1-1-111-111-1-11-111-111-11-111-1-1-1 1: 15 -1: 17
DISP: 0,9990
-1-1-1111-1-1-1-1111-11-1-1-11-11-1-11-1-1-11-1-111 1: 13 -1: 19
DISP: 0,9740
29) 8 4 -8 0 0 0 0 4 8 4 8 -4 4 4 -8 8 4 -4 -8 -8 -4 -8 -4 0 0 -4 0 0 -4 4 4 0 MatO: -0,2500
Signals: 17 26
-111-111-11-1-11-111-1-1-1-1-11-1-11-1-1111111-1 1: 16 -1: 16
DISP: 0,9990
-11111111-1111-11-1-1-11-1-11-111-11-11-11-1-1 1: 18 -1: 14
DISP: 0,9740
31) 0 0 8 0 0 -4 0 4 8 8 -4 -4 -4 4 4 4 8 -4 0 0 -4 4 4 0 0 0 0 4 4 0 0 8 MatO: 1,5000
Signals: 18 21
-1-1-1111-11-11-111-1-1-1-11-11-11-11-1-11-1-11-11 1: 14 -1: 18
DISP: 0,9906
-1-111-1-111-1-1-1-111-1-1-1-111-1-1-1-1-11-1-11-1-1-1 1: 10 -1: 22
DISP: 0,8742

33) 0 4 4 0 -8 4 0 -4 4 0 8 4 -4 -8 0 4 4 4 0 8 0 -4 -8 4 4 -4 8 -4 4 4 -8 -4 MatO: 0,5000
Signals: 18 23
-1-1-1111-11-11-111-1-1-1-11-11-11-11-1-11-1-11-11 1: 14 -1: 18
DISP: 0,9906
-1-1-1-1111-1-1-1-1-1-1111-11-1-11-111-1-1111-1-11 1: 14 -1: 18
DISP: 0,9906

35) 0 4 -4 4 0 0 0 0 4 0 -4 4 -4 -4 -8 8 8 -4 -4 4 -4 4 0 0 -4 8 4 -8 0 0 -8 4 MatO: 0,0000
Signals: 24 31

-1-11-111-11-1-1111-11-1-1-1-11111-1-1-111-111-1 1: 16 -1: 16
DISP: 0,9990
-11-1111-1-1-111-1-11-11-1-1-1-1-1-1-1-11-1-111-1111 1: 14 -1: 18
DISP: 0,9906
37) 0 4 -4 0 -4 -8 -4 -4 4 0 -8 0 -4 4 0 8 4 0 8 4 0 0 0 -8 4 0 -8 -4 4 0 0 -4 MatO: -0,5000
Signals: 25 31
-1-11-1-11-11-11-111111-111-11-11-1-1-111111-1 1: 18 -1: 14
DISP: 0,9740
-11-1111-1-1-111-1-11-11-1-1-1-1-1-1-1-11-1-111-1111 1: 14 -1: 18
DISP: 0,9906
39) 4 4 8 -4 4 8 0 0 0 4 8 -4 4 -4 0 4 8 -4 -4 4 0 4 0 -4 8 -4 4 4 4 -8 8 8 MatO: 1,8750
Signals: 27 31
-1-1-11-11-1-1-1-1-11-1-11-1-1-1-1-1-1-11-1-1-1-11-11-1-11 1: 8 -1: 24
DISP: 0,7661
-11-1111-1-1-111-1-11-11-1-1-1-1-1-1-1-11-1-111-1111 1: 14 -1: 18
DISP: 0,9906

Сигналы, значения боковых выбросов АФАК которых, не превышают предельно достижимой границы: 9

АФАК 32 -3 0 7 -8 -7 -6 1 -2 1 6 -1 -2 3 -4 -5 6 1 -4 5 -2 -3 -2 -1 2 -1 2 3 0 1 0 -1 MatO: -0,4375 MIN: -8 MAX: 7
1) -111-111-11-11-111-11-1-111-111-1-1-1-1-1-11111 1: 17 -1: 15
DISP: 0,9906
АФАК 32 1 2 1 2 -7 -2 -3 4 1 -8 5 -2 -3 -4 1 0 3 0 3 6 -5 0 -1 0 -5 2 -1 2 -1 2 -1 MatO: -0,2500 MIN: -8 MAX: 6
3) -1111-111-1-11-1-1-1-11-1-1-1-1-11111-11-1-1-11-11 1: 14 -1: 18
DISP: 0,9906
АФАК 32 -5 -2 -5 8 -9 2 1 6 -5 0 -1 0 -1 -2 7 0 5 -2 1 -8 5 0 1 -2 3 -6 1 0 1 -2 1 MatO: -0,2500 MIN: -9 MAX: 8
4) -11-1-1-11-11-1-1-11-1111-1-11-1-1-111-1-11-1111-1 1: 14 -1: 18
DISP: 0,9906
АФАК 32 -1 0 -7 0 -7 4 -5 4 1 2 1 2 -1 2 -3 0 -5 -2 1 6 -1 6 -1 0 -3 0 -1 0 -1 0 1 MatO: -0,2500 MIN: -7 MAX: 6

10) -11-11-1111-11-1-1-111-1-11111-1-11-111111-1-1 1: 18 -1: 14 DISP: 0,9740
АФАК 32 -5 4 5 -4 9 -6 -1 4 -1 0 -1 4 7 -2 7 2 1 6 -3 4 1 -4 5 -4 1 2 -1 4 -1 0 1
MatO: 1,0625 MIN: -6 MAX: 9
11) -1-11-111-11-1-1-1-1-11-1-1-111-11-11-1-11-1-1-1-11-1 1: 11 -1: 21
DISP: 0,9158
АФАК 32 -1 -2 -5 6 -3 -6 5 0 3 -4 3 -2 -1 4 1 2 -1 4 1 2 -3 -4 1 0 3 -2 3 -2 1 -2 1
MatO: 0,0625 MIN: -6 MAX: 6
13) -11-11-11-1-1-1-11-1-1-111-1-111-111-1-1-1-1-1111-1 1: 13 -1: 19
DISP: 0,9740
АФАК 32 1 -2 -7 -2 -7 2 9 4 5 -4 -3 -4 5 -6 3 2 1 -2 3 4 -1 0 -1 0 -1 2 3 2 -1 -2 -1
MatO: 0,0625 MIN: -7 MAX: 9
19) -1-1-1111-1-1-1-1111-11-1-1-11-11-1-11-1-1-11-1-111 1: 13 -1: 19
DISP: 0,9740
АФАК 32 -3 -4 7 0 -5 2 -3 -6 -1 -2 -5 -4 3 -4 -1 6 1 4 1 4 1 -2 1 2 -5 2 1 -4 1 0 -1
MatO: -0,4375 MIN: -6 MAX: 7
20) -11-1-11-1-11-1-111111-1-11-11-1-1-11-1-1-111-111 1: 15 -1: 17
DISP: 0,9990
АФАК 32 3 4 5 -8 1 -6 -5 2 -1 -4 -1 0 -3 0 3 2 5 0 -1 4 1 -4 1 -2 1 2 -1 4 -1 0 1
MatO: 0,0625 MIN: -8 MAX: 5
22) -1-11-111-1-1-1-11-1-11-1-1-1-1111111-11-1-1-1-11-1 1: 13 -1: 19
DISP: 0,9740
АФАК 32 -5 8 3 4 -1 0 3 -4 -3 0 -7 4 -5 0 -3 8 -5 4 1 0 -1 0 -1 0 -3 0 -3 0 -3 0 1
MatO: -0,2500 MIN: -7 MAX: 8
26) -11111111-1111-11-1-1-11-1-11-111-11-11-11-1-1 1: 18 -1: 14 DISP: 0,9740

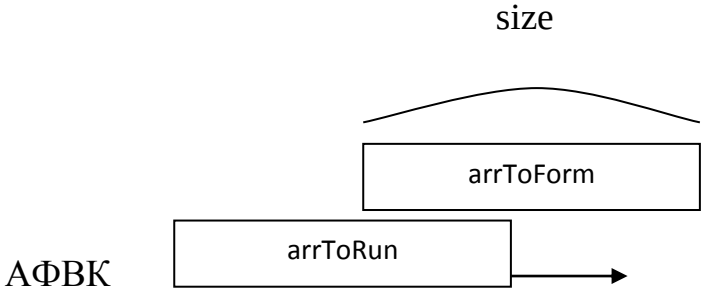
ПРИЛОЖЕНИЕ Г

Результаты исследования свойств нелинейных дискретных криптографических сигналов

Исходный код функции, для нахождения значения апериодической функции взаимной корреляции (АФВК) сигналов на языке Java .

Параметры:

- **int** []arrToRun - массив, содержащий 1й сигнал для АФВК;
- **int** []arrToForm - массив, содержащий 2й сигнал для АФКВ;
- **int** []ress - пустой массив, для записи результата значения АФВК;
- **int** size - переменная - длина поступивших сигналов.




```
public static void AFVK(int []arrToRun, int []arrToForm, int []ress,int size)
{
  int summ    = 0;
  int buf     = 0;

  int []doubleArr   = new int[size];
  int []arr         = new int[size];

  for (int i = 0; i < size; i++)
  {
        doubleArr[i] = arrToForm[i];
        arr[i] = arrToRun[i];
  };
  for(int i = 0; i < size; i++)
```

```
    {
        for(int q = 0; q<i; q++)
            arr[q] = 0;
        for(int z = i, x = 0; z<size; z++, x++)
            arr[z] = arrToRun[x];

        for (int j = 0; j < size; j++)
            if(arr[j]==doubleArr[j])
                summ++;

        buf    = summ-(size-summ);//число совпадений - число не совпадений
        ress[i] = buf;
        summ        = 0;
        buf    = 0;
    };
};
```

Примеры результатов работы функции:

Входные данные: - Сигнал 1: 0 0 1 1 0 1 1 1 - Сигнал 2: 1 1 1 1 1 1 0 1 - Длина: 8 *Полученный результат:* - Значение АФВК: 0 -2 0 -6 -6 -4 -6 -6	*Входные данные:* - Сигнал 1: 0 1 0 0 1 0 1 0 - Сигнал 2: 0 0 1 0 0 0 0 0 - Длина: 8 *Полученный результат:* - Значение АФВК: 0 4 2 2 4 4 4 6
Входные данные: - Сигнал 1: 0 1 0 1 1 1 0 0 - Сигнал 2: 0 1 1 1 1 1 0 1 - Длина: 8 *Полученный результат:* - Значение АФВК: 4 0 0 -2 0 -6 -2 -4	*Входные данные:* - Сигнал 1: 0 1 0 1 0 1 1 0 - Сигнал 2: 0 1 1 1 1 0 0 0 - Длина: 8 *Полученный результат:* - Значение АФВК: 0 0 -2 0 -4 -2 -2 0

Входные данные: - Сигнал 1: 0 1 0 1 0 1 1 1 0 0 1 0 1 1 0 0 - Сигнал 2: 0 0 0 0 0 0 0 0 0 0 1 0 1 1 1 0 - Длина: 16 *Полученный результат:* - Значение АФВК: 4 0 0 2 4 4 6 14 6 12 6 12 8 10 6 8

Входные данные:

- Сигнал 1: 0 1 0 0 0 1 0 0 0 1 0 1 1 0 0 0 0 0 0 1 1 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0 0 0 0 1 0 1 0 0 0 0 1 1 0 1 0 1 1 0 0 1 0 0 0 1 1 0 1 0
- Сигнал 2: 0 0 1 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 1 1 1 1 1 1 0 1 1 0 0 0 1 0 0 0 0 1 1 0 0 0 0 1 0 1 0 1 1 0 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 1
- Длина: 64

Полученный результат:

- Значение АФВК: 6 6 8 8 6 12 0 12 4 6 10 10 12 10 18 12 16 14 16 8 12 12 12 14 22 16 12 12 4 8 8 16 16 6 22 14 14 8 8 8 20 10 18 14 16 18 14 10 10 14 14 14 16 18 18 16 16 16 20 18 18 18 22 20

Входные данные:

- Сигнал 1: 0 1 1 0 1 1 1 1 0 0 0 0 1 0 1 0 0 0 1 0 1 0 0 0 0 1 0 0 0 1 0 1 0 0 1 1 0 0 0 0 0 1 0 1 0 0 1 0 0 0 0 1 1 0 1 1 0 0 0 1 0 1 0 0
- Сигнал 2: 0 0 0 1 1 0 1 0 0 1 0 0 0 1 1 0 0 0 1 0 1 1 1 0 0 1 1 0 1 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 1 1 1 0 1 1 0 0 0 1 1 0 0 0 0 1 0 1 0
- Длина: 64

Полученный результат:

- Значение АФВК: -4 4 0 6 6 -12 -8 -4 20 -2 -4 0 2 8 8 4 8 0 -2 18 6 12 -8 -2 14 10 6 2 -2 0 -2 6 6 4 -4 10 2 10 2 -4 12 4 12 8 6 2 0 -4 12 0 2 -6 -4 4 0 0 0 -2 4 2 4 4 2 4

Входные данные:

- Сигнал 1: 0 0 1 1 1 1 0 0 0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 1 1 0 0 0 0 0 1 1 0 1 0 0 1 0 1 1 1 1 0 0 0 0 1 0 1 1 0 0 0 0 1 0 1 0 0 0 1 1 0 0 0 1 0 0 0 1 1 1 0 0 0 0 0 1 1 0 1 0 0 0 0 0 1 1 0 0 0 0 0 0 1 0 0 1 0 0 1 1 0 1 1 1
- Сигнал 2: 0 0 0 1 1 0 1 1 0 1 1 0 0 0 0 1 0 0 1 1 1 0 0 1 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 1 0 0 0 1 1 0 1 1 0 0 0 0 1 0 0 1 0 1 0 0 1 0 1 0 0 1 0 0 0 1 1 1 0 1 0 1 1 1 1 0 0 0 1 0 1 1 1 0 0 1 0 0 1 0 1 0 0 0 0 0 0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 0 1 0
- Длина: 128

Полученный результат:

- Значение АФВК: 16 10 12 10 -22 4 -6 18 6 4 16 -12 -18 6 6 18 -2 14 10 -12 -2 -2 18 14 14 -2 20 0 -10 -8 12 12 28 12 4 14 -4 6 -2 26 34 24 4 16 8 10 -8 8 28 16 26 30 16 16 -4 16 24 14 24 16 22 14 10 30 22 16 22 16 26 22 20 16 12 30 18 20 22 18 18 18 30 26 24 22 10 20 14 10 22 22 20 18 22 18 16 14 14 14 20 22 20 26 18 14 18 18 20 22 28 32 24 34 26 20 22 22 28 30 32 32 28 28 24 26 28 26 28 28

Входные данные:

- Сигнал 1: 0 1 0 1 0 0 1 0 0 0 1 1 1 0 1 0 0 0 1 0 0 0 0 1 0 0 1 1 1 0 1 1 0 0 0 1 1 1 1 0 0 0 1 0 0 1 0 0 0 1 0 0 1 1 0 1 0 0 0 0 0 1 1 1 0 0 1 0 0 1 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 1 1 0 1 1 1 0 1 0 1 0 1 1 1 0 0 1 1 1 0 1 0 0 1 1 1 1 0 1 0 0 0 1 1 1 0 1 1
- Сигнал 2: 0 0 0 0 0 1 0 0 1 1 1 1 1 1 0 1 0 0 0 0 1 0 0 1 0 1 0 1 0 1 0 1 1 0 0 1 0 1 1 0 0 0 0 1 1 0 1 0 0 1 1 1 1 0 1 1 0 1 0 0 1 0 0 0 0 0 0 1 1 0 1 0 0 0 0 1 1 1 0 1 0 0 1 0 1 0 0 0 0 0 1 0 0 0 1 0 0 1 0 1 1 0 1 0 0 1 1 1 0 1 1 1 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 1
- Длина: 128

Полученный результат:

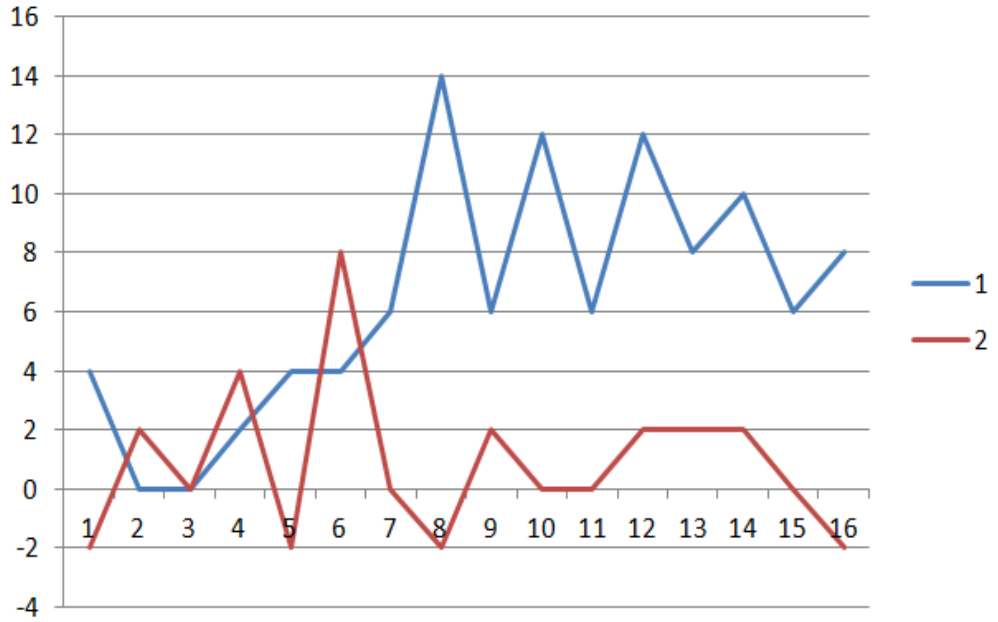
- Значение АФВК: 2 12 2 -14 12 14 8 12 16 20 -18 -14 16 10 16 22 6 2 -8 8 6 16 -2 -2 10 4 6 - 8 8 2 -6 12 16 2 8 -10 -2 28 6 18 26 14 14 4 24 20 8 8 16 24 -2 -2 6 6 14 -10 14 8 4 2 -2 6 4 0 20 10 12 18 2 18 14 10 18 16 20 6 20 0 12 22 14 6 6 12 16 8 2 14 14 10 0 18 16 14 14 14 26 20 10 30 16 22 8 16 28 18 14 10 18 18 16 12 16 12 14 14 20 18 16 20 16 24 18 18 22 20 24 22

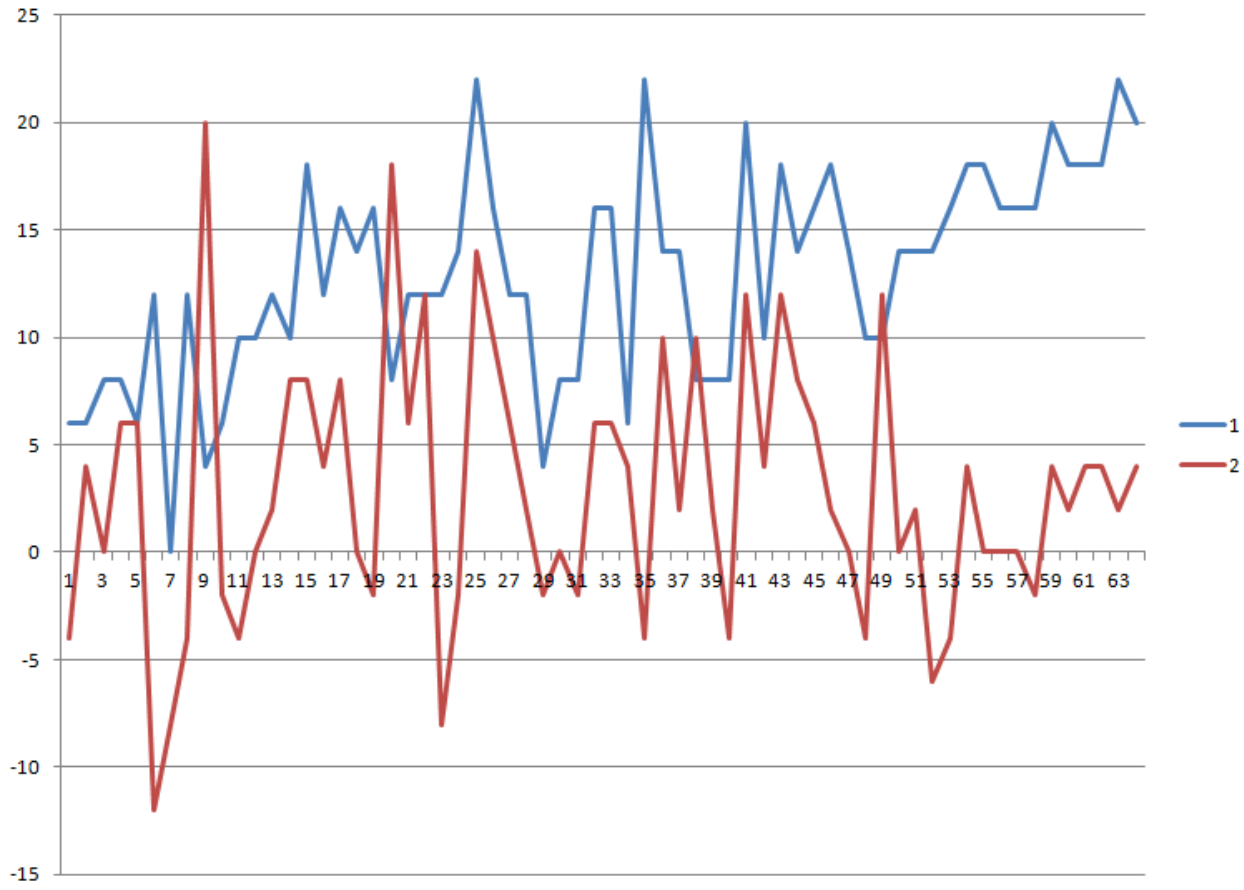
Входные данные:

- Сигнал 1: 0 1 1 0 0 1 0 1 0 1 0 1 1 0 1 0
- Сигнал 2: 0 1 0 0 1 0 1 1 0 0 1 0 1 1 1 1
- Длина: 16

Полученный результат:

- Значение АФВК: -2 2 0 4 -2 8 0 -2 2 0 0 2 2 2 0 -2





Функция, реализующая поиск максимального значения в массиве значений периодической функции авто- корреляции (ПФАК), на языке Java . В результате выполнения, функция возвращает результат (максимальное по модулю число в массиве), типа int.

Параметры:

- **int** []arr - массив данных, для обработки (ПФАК сигнала);
- **int** size - переменная - длина поступившего массива.

```
public static int findMaxPFAK(int []arr, int size)
{
   //функци находит максимум, игнорируя максимальный пик
   int max = 0;
```

```
    for(int j = 0; j<size; j++)
        if(Math.abs(arr[j]) > Math.abs(max) && Math.abs(arr[j])!=size)
            max = arr[j];

    return max;
};
```

Примеры результатов работы функции:

Входные данные: - Сигнал : 0 0 0 0 1 0 0 1 - ПФАК: 8 0 0 4 0 4 0 0 - Длина: 8 *Полученный результат:* Максимум = 4	*Входные данные:* - Сигнал : 0 0 0 1 1 0 0 1 - ПФАК: 8 0 -4 0 4 0 -4 0 - Длина: 8 *Полученный результат:* Максимум = -4
Входные данные: - Сигнал : 0 1 0 1 0 1 1 0 - ПФАК: 8 -4 0 0 0 0 0 -4 - Длина: 8 *Полученный результат:* Максимум = -4	*Входные данные:* - Сигнал : 0 0 0 1 1 1 0 1 - ПФАК: 8 0 0 -4 0 -4 0 0 - Длина: 8 *Полученный результат:* Максимум = -4

Входные данные: - Сигнал : 0 1 0 1 1 1 1 0 0 1 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 0 1 1 0 0 1 0 1 1 1 1 1 0 1 0 0 1 1 1 1 0 0 0 1 0 1 0 1 0 1 1 1 1 0 0 1 ПФАК: 64 0 4 -12 -20 -12 4 4 24 4 12 -12 -4 -12 0 0 12 4 16 -8 -4 -8 0 -4 16 8 8 -4 -8 -12 4 8 20 8 4 -12 -8 -4 8 8 16 -4 0 -8 -4 -8 16 4 12 0 0 -12 -4 -12 12 4 24 4 4 -12 -20 -12 4 0 - Длина: 64 *Полученный результат:* Максимум = 24
Входные данные: - Сигнал : 0 1 0 0 1 0 0 1 0 0 1 1 0 1 0 1 0 0 1 1 1 1 1 0 0 1 1 0 1 1 0 0 0 0 1 0 1 1 0 1 0 1 0 1 0 0 1 1 0 0 0 1 0 1 1 1 0 0 1 0 0 0 0 1 0 0 0 1 1 0 0 0 0 0 1 1 0

0 0 1 0 1 1 1 1 1 1 0 1 1 0 0 0 1 0 0 1 1 0 1 0 0 1 0 1 0 0 1 1 1 1 0 1 0 0 1 0 1 0 0 0 1 1 1 1 0 0 - ПФАК: 128 -8 -8 4 -8 0 -12 12 12 -16 -8 4 -8 -4 4 8 8 -12 -8 8 -28 12 -4 -24 16 -4 12 0 4 4 0 -4 12 -4 -8 8 0 -20 8 -4 12 -8 4 12 -12 0 0 -8 -4 0 -4 -8 -24 4 0 -12 16 20 -4 4 4 4 4 -8 36 -8 4 4 4 4 -4 20 16 -12 0 4 -24 -8 -4 0 -4 -8 0 0 -12 12 4 -8 12 -4 8 -20 0 8 -8 -4 12 -4 0 4 4 0 12 -4 16 -24 -4 12 -28 8 -8 -12 8 8 4 -4 -8 4 -8 -16 12 12 -12 0 -8 4 -8 -8 - Длина: 128 *Полученный результат:* Максимум = 36
Входные данные: - Сигнал : 0 0 0 1 0 0 1 1 0 1 1 0 1 1 1 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1 1 0 1 1 0 1 1 1 1 0 0 1 0 1 0 0 0 1 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 0 0 0 1 1 1 0 0 1 1 0 0 0 0 1 1 1 0 0 1 1 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 1 0 0 0 1 0 1 0 1 1 1 0 1 0 0 1 1 1 0 1 1 0 1 0 1 0 1 0 1 0 0 1 1 0 0 0 0 0 1 0 1 0 1 1 1 0 1 1 1 0 0 1 0 0 0 1 0 0 0 1 1 0 0 1 0 0 1 0 0 0 1 1 0 1 0 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 0 0 0 0 1 1 0 0 0 1 0 0 1 1 1 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 1 0 1 1 1 0 1 0 1 1 1 0 1 0 0 0 1 1 1 0 0 - ПФАК: 256 -12 0 -12 20 8 36 -20 4 -16 8 8 0 -16 -24 0 52 -44 12 4 8 -24 -12 -8 40 -4 -12 - 8 -4 36 0 0 24 -20 -8 16 4 -20 -8 -20 28 -20 16 -12 4 -20 0 16 36 -24 4 16 8 12 -4 -28 20 -12 - 12 -12 12 -20 16 -24 4 0 20 12 -4 -8 -12 20 52 -20 0 -8 20 24 20 -4 52 -12 40 -8 20 -4 0 -28 32 -16 20 -16 8 -28 4 16 40 -28 -4 0 24 4 8 -4 24 -4 28 0 12 -8 -4 -8 32 -4 16 -16 -20 -12 -4 8 12 - 12 4 -16 16 0 -4 -20 40 -20 -4 0 16 -16 4 -12 12 8 -4 -12 -20 -16 16 -4 32 -8 -4 -8 12 0 28 -4 24 -4 8 4 24 0 -4 -28 40 16 4 -28 8 -16 20 -16 32 -28 0 -4 20 -8 40 -12 52 -4 20 24 20 -8 0 -20 52 20 -12 -8 -4 12 20 0 4 -24 16 -20 12 -12 -12 -12 20 -28 -4 12 8 16 4 -24 36 16 0 -20 4 -12 16 -20 28 -20 -8 -20 4 16 -8 -20 24 0 0 36 -4 -8 -12 -4 40 -8 -12 -24 8 4 12 -44 52 0 -24 -16 0 8 8 -16 4 -20 36 8 20 -12 0 -12 - Длина: 256 *Полученный результат:* Максимум = 52

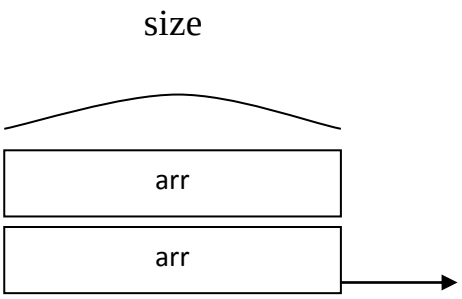
Исходный код функции, для нахождения значения апериодической функции авто- корреляции (АФАК) сигнала на языке Java .

Параметры:

- **int** []arr - массив, содержащий сигнал для нахождения АФАК;

- **int** []ress - пустой массив, для записи результата значения АФАК;

- **int** size - переменная - длина поступившего сигнала.



АФАК

```
public static void AFAK(int []arr,int []ress,int size)
{
 int summ = 0;
 int buf = 0;

 int []doubleArr   = new int[size];
 int []arrBuf  = new int[size];

 for (int i = 0; i < size; i++)
 {
        doubleArr[i] = arr[i];
        arrBuf [i] = arr[i];
 }

 for(int i = 0; i < size; i++)
 {
        for(int q = 0; q<i; q++)
               arrBuf[q] = 0;
        for(int z = i, x = 0; z<size; z++, x++)
               arrBuf[z] = doubleArr[x];

        for (int j = 0; j < size; j++)
               if(arrBuf[j]==doubleArr[j])
                      summ++;

        buf = summ-(size-summ);
        ress[i] = buf;
        summ = 0;
        buf = 0;
 };
```

};

Примеры результатов работы функции:

Входные данные: - Сигнал : 0 0 1 0 1 1 0 1 - Длина: 8 *Полученный результат:* - Значение АФАК: 8 -2 2 4 -2 2 0 0	*Входные данные:* - Сигнал : 0 1 0 1 0 1 0 1 - Длина: 8 *Полученный результат:* - Значение АФАК: 8 -6 6 -4 4 -2 2 0
Входные данные: - Сигнал : 0 0 1 1 0 1 1 1 - Длина: 8 *Полученный результат:* - Значение АФАК: 8 2 0 2 2 0 -2 -2	*Входные данные:* - Сигнал : 0 1 0 0 0 0 0 1 - Длина: 8 *Полученный результат:* - Значение АФАК: 8 2 2 2 2 2 6 4

Входные данные: - Сигнал : 0 0 0 0 1 1 1 1 0 0 1 1 1 0 1 0 - Длина: 16 *Полученный результат:* - Значение АФАК: 16 4 2 -2 0 2 4 4 0 -2 0 -2 0 0 0 0
Входные данные: - Сигнал : 0 1 0 1 0 0 1 1 0 0 1 1 0 1 1 0 - Длина: 16 *Полученный результат:* - Значение АФАК: 16 -4 -6 4 4 -2 0 4 0 -2 4 0 0 2 -2 0

Входные данные: - Сигнал : 0 1 1 1 0 1 1 1 0 1 0 1 1 0 0 1 0 0 0 0 1 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 0 1 1 1 1 0 1 0 0 1 0 1 1 0 1 0 0 0 0 1 1 1 0 - Длина: 64 *Полученный результат:* - Значение АФАК: 64 8 2 0 -10 6 2 -10 2 -4 0 -10 -20 -8 -2 -6 2 4 0 -2 -12 -14 0 0 0 -2 -12 -2 -4 -8 8 4 8 8 0 12 8 4 8 2 14 14 4 2 4 0 4 0 0 6 6 2 0 2 2 4 0 2 4 10 6 4 2 4
Входные данные: - Сигнал : 0 0 1 1 0 0 1 0 0 0 0 1 0 1 1 0 0 0 1 1 0 0 1 0 0 1 0 0 1 0 1 0 0 0 1 1 0 0 0 1 0 0 1 1 1 0 0 1 0 0 0 1 0 1 1 0 0 0 1 0 0 0 1 0 - Длина: 64

Полученный результат:

- Значение АФАК: 64 -4 -14 2 10 6 -8 4 12 12 -2 16 12 -6 6 6 14 12 -8 16 6 4 6 14 10 12 8 -4 20 14 4 8 16 16 6 2 16 12 4 10 26 14 8 8 12 14 4 12 16 12 10 20 16 10 10 14 18 10 12 16 16 14 16 16

Входные данные:

- Сигнал : 0 1 0 1 1 1 1 0 0 0 0 1 0 0 0 1 0 1 0 1 0 1 0 0 0 0 1 0 0 1 0 1 0 1 1 0 1 0 1 0 0 0 1 0 1 1 0 1 0 0 0 0 0 1 1 0 0 0 1 0 0 0 1 0 0 1 1 0 0 1 0 1 0 0 1 0 0 0 0 0 0 0 1 1 1 0 1 1 0 1 1 0 0 1 0 0 0 1 1 1 1 1 0 0 0 0 1 0 0 0 0 0 0 1 0 1 0 0 1 0 0 0 1 1 1 0 0
- Длина: 128

Полученный результат:

- Значение АФАК: 128 -4 12 2 0 2 -14 2 2 6 -4 8 12 6 2 12 24 8 16 -8 0 -4 -10 -2 18 14 -2 16 18 12 6 12 24 12 -8 18 14 6 0 18 14 20 10 10 12 6 4 8 20 8 12 12 16 28 18 18 14 16 4 18 14 18 12 18 18 22 16 16 28 12 22 26 14 10 0 6 10 14 22 26 30 24 32 18 24 20 22 26 10 26 12 12 26 14 32 26 30 24 24 18 18 14 20 20 20 16 16 22 22 24 24 18 30 24 28 20 16 26 26 30 30 26 28 26 28 26 26 28

Входные данные:

- Сигнал : 0 0 1 0 0 1 1 1 0 1 1 0 1 0 0 0 0 0 1 1 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 1 0 0 1 0 1 0 0 1 0 0 1 0 1 0 0 0 1 0 0 0 0 0 0 0 1 1 1 0 0 1 0 0 0 1 1 1 1 0 0 0 0 1 0 0 1 0 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 0 0 0 1 1 0 0 1 1 0 1 0 0 1 1 1 1 0 0 1 0 0 1 0 0
- Длина: 128

Полученный результат:

- Значение АФАК: 128 8 -4 14 -18 -2 8 0 16 22 4 -6 16 -16 0 30 -2 28 10 2 2 -8 -2 6 22 22 -2 12 -4 4 8 4 16 2 18 4 2 2 -10 26 22 10 24 4 4 2 10 14 14 30 0 10 12 -6 2 6 14 24 20 16 6 16 6 2 26 22 30 18 6 14 16 16 20 28 18 10 24 8 4 10 10 26 12 16 26 18 14 20 24 20 24 26 18 16 14 22 26 22 26 28 24 30 16 20 32 24 26 28 26 28 30 30 30 30 22 26 28 24 22 24 28 22 24 30 26 26 28 28

Входные данные:

- Сигнал : 0 0 0 1 1 1 0 0 0 1 0 0 1 1 0 1 0 1 0 0 0 1 0 0 1 1 1 1 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 0 0 1 1 0 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 1 1 1 1 0 1 1 0 0 1 0 1 0 0 0 1 0 0 1 0 1 0 1 0 0 0 1 0 0 1 0 1 0 0 1 0 0 1 1 0 1 0 1 0 0 1 1 0 0 0 1 0 0 1 0 1 1 0 0 0 0 1 0 0 1 0 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 1 1 1 0 1 1 0 0 0 0 0 1 0 1 0 1 0 1 1 1 1 1 0 1 1 1 0 0 1 1 0 0 0 1 1 1 0 0 0 1 0 1 1 0 1 1 0 1 1 0 1 1 1 1 0 0 0 1 1 1 1 0 0 1 1 0 1 0 1 1

0 1 0 0 0 1 0 0 0 1 0 0 1 1 0 0
- Длина: 256
Полученный результат:
- Значение АФАК: 256 -40 8 -6 12 8 8 -30 34 6 6 16 12 4 -8 -6 42 -20 18 14 -12 12 -2 -4 60 - 8 -10 0 -22 12 4 -16 20 -2 12 6 -12 4 -18 -4 12 10 4 -4 -6 12 -8 10 22 10 2 -4 -14 8 8 -28 20 -14 24 8 0 -18 4 -18 22 -4 2 -8 22 -4 -12 -2 6 -12 -4 -14 -6 2 22 -30 18 -12 14 -14 -12 -10 20 -16 20 -12 24 -16 -4 -6 -14 0 8 -24 20 8 -2 18 2 -10 34 -24 16 -6 -6 -2 28 0 12 -8 12 10 -4 -4 14 2 14 -24 32 -8 -16 26 0 12 8 -2 -2 12 -8 10 20 16 20 14 6 2 -8 4 2 14 26 0 32 8 8 22 14 4 12 6 24 4 -4 30 18 34 26 -4 24 18 14 6 36 14 42 4 30 4 18 12 12 18 26 12 40 14 6 24 20 26 30 8 34 22 12 20 26 26 10 20 26 18 12 16 6 26 30 8 30 14 12 20 18 18 26 14 16 14 22 18 14 16 12 18 18 8 6 14 4 8 28 18 14 8 14 12 10 8 18 10 10 12 20 12 8 6 18 12 8 10 16 12 12 14 18 18 14 12 14 16 16 16

Исходный код функции, для поиска минимального значения в массиве значений периодической функции автокорреляции (ПФАК), на языке Java.

Параметры:

- **int** []arr - массив данных, для обработки (ПФАК сигнала);
- **int** size - переменная - длина поступившего массива.

```
public static int findMinPFAK(int []arr, int size)
{
	//функция находит минимум, игнорируя 0
	int min = size;

	for(int j = 0; j<size; j++)
		if(Math.abs(arr[j]) < Math.abs(min) && Math.abs(arr[j]) != 0)
			min = arr[j];

	return min;
};
```

Примеры результатов работы функции:

Входные данные: - Сигнал : 0 0 0 0 1 0 0 1 - ПФАК: 8 0 0 4 0 4 0 0 - Длина: 8 *Полученный результат:* Минимум = 4	*Входные данные:* - Сигнал : 0 0 0 1 1 0 0 1 - ПФАК: 8 0 -4 0 4 0 -4 0 - Длина: 8 *Полученный результат:* Минимум = -4
Входные данные: - Сигнал : 0 1 0 1 0 1 1 0 - ПФАК: 8 -4 0 0 0 0 0 -4 - Длина: 8 *Полученный результат:* Минимум = -4	*Входные данные:* - Сигнал : 0 0 0 1 1 1 0 1 - ПФАК: 8 0 0 -4 0 -4 0 0 - Длина: 8 *Полученный результат:* Минимум = -4

Входные данные: - Сигнал : 0 0 0 1 0 1 1 1 0 1 1 1 0 0 1 1 - ПФАК: 16 0 -4 -4 8 0 -4 -4 4 -4 -4 0 8 -4 -4 0 - Длина: 16 *Полученный результат:* Минимум = -4
Входные данные: - Сигнал : 0 1 0 1 1 1 1 0 0 1 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 0 1 1 0 0 1 0 1 1 1 1 1 0 1 0 0 1 1 1 1 0 0 0 1 0 1 0 1 0 1 1 1 1 0 0 1 - ПФАК: 64 0 4 -12 -20 -12 4 4 24 4 12 -12 -4 -12 0 0 12 4 16 -8 -4 -8 0 -4 16 8 8 -4 -8 -12 4 8 20 8 4 -12 -8 -4 8 8 16 -4 0 -8 -4 -8 16 4 12 0 0 -12 -4 -12 12 4 24 4 4 -12 -20 -12 4 0 - Длина: 64 *Полученный результат:* Минимум = 4
Входные данные: - Сигнал : 0 1 0 0 1 0 0 1 0 0 1 1 0 1 0 1 0 0 1 1 1 1 1 0 0 1 1 0 1 1 0 0 0 0 1 0 1 1 0 1 0 1 0 1 0 0 1 1 0 0 0 1 0 1 1 1 0 0 1 0 0 0 0 1 0 0 0 1 1 0 0 0 0 0 1 1 0 0 0 1 0 1 1 1 1 1 1 1 0 1 1 0 0 0 1 0 0 1 1 0 1 0 0 1 0 1 0 0 1 1 1 1 0 1 0 0 1 0 1 0 0 0 1 1 1 1 0 0 - ПФАК: 128 -8 -8 4 -8 0 -12 12 12 -16 -8 4 -8 -4 4 8 8 -12 -8 8 -28 12 -4 -24 16 -4 12 0 4 4 0 -4 12 -4 -8 8 0 -20 8 -4 12 -8 4 12 -12 0 0 -8 -4 0 -4 -8 -

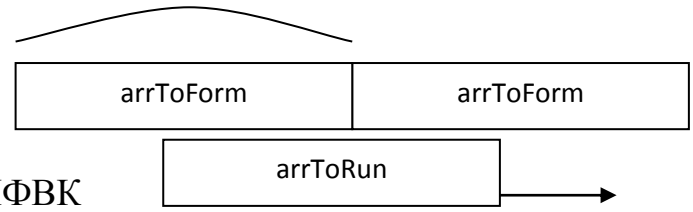
24 4 0 -12 16 20 -4 4 4 4 4 -8 36 -8 4 4 4 4 -4 20 16 -12 0 4 -24 -8 -4 0 -4 -8 0 0 -12 12 4 -8 12 -4 8 -20 0 8 -8 -4 12 -4 0 4 4 0 12 -4 16 -24 -4 12 -28 8 -8 -12 8 8 4 -4 -8 4 -8 -16 12 12 -12 0 -8 4 -8 -8 - Длина: 128 *Полученный результат:* Минимум = 4
Входные данные: - Сигнал : 0 0 0 1 0 0 1 1 0 1 1 0 1 1 1 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1 1 0 1 1 0 1 1 1 1 0 0 1 0 1 0 0 0 1 1 1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 0 0 0 1 1 1 0 0 1 1 0 0 0 0 1 1 1 0 0 1 1 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 1 1 0 0 0 1 0 1 0 1 1 1 0 1 0 0 1 1 1 0 1 1 0 1 0 1 0 1 0 0 1 1 0 0 0 0 0 1 0 1 0 1 1 1 0 1 1 1 0 0 1 0 0 0 1 0 0 0 1 1 0 0 1 0 0 1 0 0 0 1 1 0 1 0 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 0 0 0 0 1 1 0 0 0 1 0 0 1 1 1 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 1 0 1 1 1 0 1 0 1 1 1 0 1 0 0 0 1 1 1 0 0 - ПФАК: 256 -12 0 -12 20 8 36 -20 4 -16 8 8 0 -16 -24 0 52 -44 12 4 8 -24 -12 -8 40 -4 -12 - 8 -4 36 0 0 24 -20 -8 16 4 -20 -8 -20 28 -20 16 -12 4 -20 0 16 36 -24 4 16 8 12 -4 -28 20 -12 - 12 -12 12 -20 16 -24 4 0 20 12 -4 -8 -12 20 52 -20 0 -8 20 24 20 -4 52 -12 40 -8 20 -4 0 -28 32 -16 20 -16 8 -28 4 16 40 -28 -4 0 24 4 8 -4 24 -4 28 0 12 -8 -4 -8 32 -4 16 -16 -20 -12 -4 8 12 - 12 4 -16 16 0 -4 -20 40 -20 -4 0 16 -16 4 -12 12 8 -4 -12 -20 -16 16 -4 32 -8 -4 -8 12 0 28 -4 24 -4 8 4 24 0 -4 -28 40 16 4 -28 8 -16 20 -16 32 -28 0 -4 20 -8 40 -12 52 -4 20 24 20 -8 0 -20 52 20 -12 -8 -4 12 20 0 4 -24 16 -20 12 -12 -12 -12 20 -28 -4 12 8 16 4 -24 36 16 0 -20 4 -12 16 -20 28 -20 -8 -20 4 16 -8 -20 24 0 0 36 -4 -8 -12 -4 40 -8 -12 -24 8 4 12 -44 52 0 -24 -16 0 8 8 -16 4 -20 36 8 20 -12 0 -12 - Длина: 256 *Полученный результат:* Минимум = 4

Исходный код функции для нахождения значения периодической функции взаимной корреляции (ПФВК) двух сигналов на языке Java.

Параметры:

- **int** []arrToRun - массив, содержащий 1й сигнал для ПФВК;
- **int** []arrToForm - массив, содержащий 2й сигнал для ПФКВ;
- **int** []ress - пустой массив, для записи результата значения ПФВК;

size



ПФВК

```
public static void PFVK(int []arrToRun,int  []arrToForm,int []ress, int size)
{
int summ = 0;
int buf = 0;

int []doubleArr = new int[size * 2];

for (int i = 0; i < size; i++)
{
        doubleArr[i] = arrToForm[i];
        doubleArr[i + size] = arrToForm[i];
};

for (int i = 0; i < size; i++)
{
        for (int j = 0, k = i; j < size; j++, k++)
                if(arrToRun[j]==doubleArr[k]) //подсчет количества совпадений
                        summ++;

        buf = summ-(size-summ);              //число совпадений - число не совпадений
        ress[i] = buf;                       //запись результата
        buf = 0;
summ = 0;
}
```

Примеры результатов работы функции:

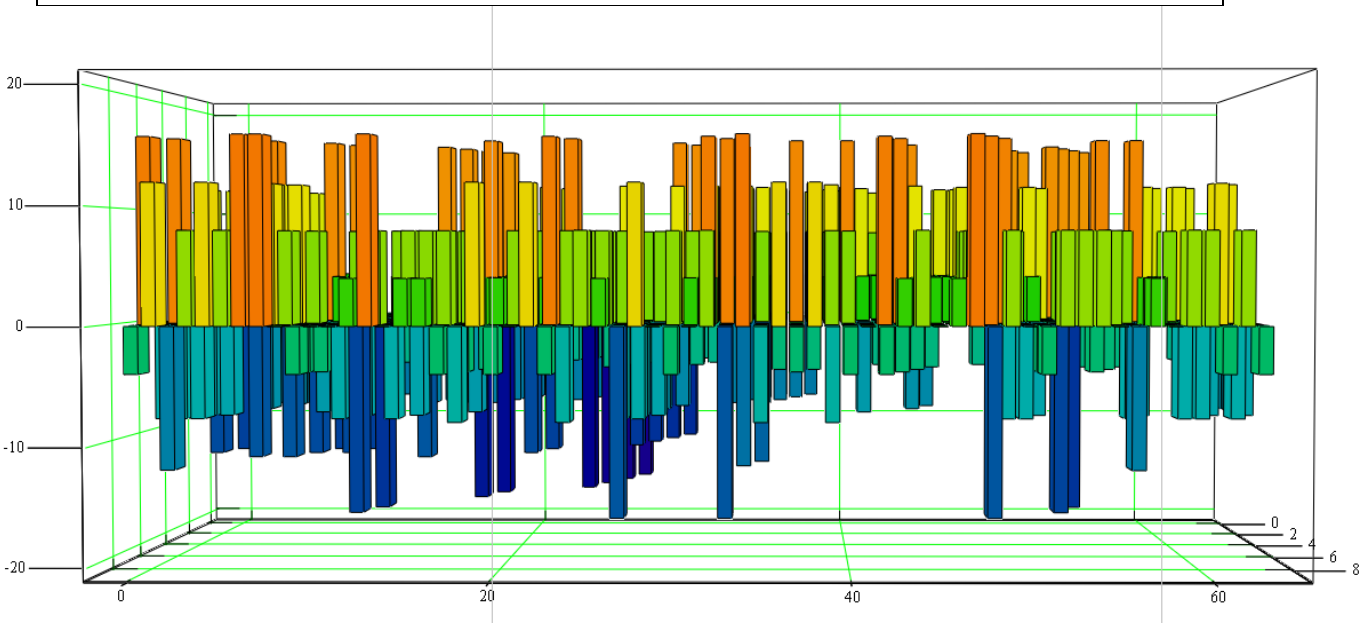
Входные данные: - Сигнал 1: 0 0 0 1 1 0 0 0 - Сигнал 2: 0 1 0 1 0 0 1 1 - Длина: 8 *Полученный результат:* - Значение ПФВК: 0 -4 0 4 0 0 0 0	*Входные данные:* - Сигнал 1: 0 0 1 0 1 1 0 1 - Сигнал 2: 0 1 0 1 1 1 1 1 - Длина: 8 *Полученный результат:* - Значение ПФВК: 0 0 4 -4 0 0 -4 4

Входные данные: - Сигнал 1: 0 0 1 1 1 1 0 1 - Сигнал 2: 0 0 0 1 1 1 0 0 - Длина: 8 *Полученный результат:* - Значение ПФВК: 4 4 0 -4 -4 -4 0 0	*Входные данные:* - Сигнал 1: 0 0 1 0 1 0 0 1 - Сигнал 2: 0 0 1 1 1 1 0 0 - Длина: 8 *Полученный результат:* - Значение ПФВК: 2 2 -2 2 -2 -2 2 -2

Входные данные: - Сигнал 1: 0 1 0 1 0 0 0 1 0 1 0 1 0 0 1 0 - Сигнал 2: 0 0 1 0 0 1 0 0 0 1 0 0 0 1 1 1 - Длина: 16 *Полученный результат:* - Значение ПФВК: 0 0 4 -4 8 -4 4 4 0 -4 0 4 4 -4 4 0
Входные данные: - Сигнал 1: 0 0 0 0 1 1 1 0 0 0 0 1 1 0 0 0 - Сигнал 2: 0 1 0 0 1 1 0 1 0 1 0 1 0 0 1 0 - Длина: 16 *Полученный результат:* - Значение ПФВК: 4 0 0 4 -4 4 0 -4 0 4 0 0 0 0 0 4

Входные данные: - Сигнал 1: 0 1 0 1 0 0 1 0 0 0 0 1 1 0 1 0 0 1 1 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 1 1 0 0 0 0 0 1 0 0 0 0 1 1 1 0 0 1 0 1 1 0 0 0 1 1 0 1 0 0 - Сигнал 2: 0 1 0 1 0 1 0 1 0 0 0 1 1 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 0 1 0 0 0 1 1 0 1 0 1 1 0 1 1 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 1 1 0 0 1 - Длина: 64 *Полученный результат:* - Значение ПФВК: 12 8 4 -12 8 0 8 0 8 0 -4 8 8 -4 8 0 4 4 0 0 8 0 12 8 8 12 -16 0 16 -8 12 0 12 4 -20 8 4 -4 -4 4 0 8 0 -8 20 -4 4 8 0 12 -8 4 20 0 -4 0 0 8 4 4 -4 -4 0 4
Входные данные: - Сигнал 1: 0 0 1 0 0 0 0 0 0 0 1 1 0 0 1 1 0 0 0 1 1 1 0 1 0 0 1 1 1 1 0 0 0 1 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 1 1 1 1 0 0 0 1 0 0 0 0 1 1 0 0 1 0 0 1 1 0 0 1 0 0 1 1 0 1 0 1 0 1 0 0 0 0 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 1 0 1 0 0 1 1 0 0 1 1 0 1 0 1 - Сигнал 2: 0 0 0 0 0 0 0 1 0 1 1 1 0 0 0 1 0 0 0 1 0 1 1 0 0 1 1 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 0 0 0 0 1 0 0 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 0 0 0 0 0 0 0 1 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 1 1 1 1 01 0 0 0 0 1 0 1 0 0 0 1 1 0 0 0 1 0 0 1 0 0

0 1 1 0 1 0 0 1 0 0 1
- Длина: 128
Полученный результат:
- Значение ПФВК: 18 18 14 -14 -2 18 2 6 26 2 -10 10 34 2 6 6 22 -10 -10 2 18 14 -6 2 18 14 22 2 2 10 18 22 18 -6 14 10 18 18 14 6 14 10 -6 -14 30 14 -6 -6 18 10 -6 14 -18 -10 6 6 26 -2 6 -2 22 10 18 30 -2 2 18 18 22 10 10 -6 30 10 10 6 -2 10 -2 10 22 18 -10 2 14 18 14 10 6 -14 -2 22 14 26 -18 10 22 10 14 2 22 14 -6 2 22 10 -10 -6 18 14 14 10 18 -14 2 14 18 14 -10 2 14 6 -6 -2 22 14 10 26



Вид ПФВК

Входные данные:
- Сигнал 1: 0 0 1 0 1 0 1 0 0 0 1 0 1 1 0 0 0 0 1 1 0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0 0 1 1 1 0 1 0 1 0 1 1 1 1 1 0 0 0 1 1 0 1 0 1 0 0 0 1 1 1 0 0 0 1 0 1 0 1 0 1 0 1 1 0 1 0 0 0 0 1 1 1 0 1 0 0 0 1 0 0 0 0 0 0 1 1 0 0 1 1 0 0 1 0 0 0 0 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 1 0 0 0 1 0 0 0 1 1 0 1 0 0 0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 1 0 1 1 0 0 0 0 0 0 0 1 0 0 1 0 1 0 1 1 1 0 0 0 1 0 0 0 0 0 1 0 1 0 0 1 0 1 1 1 0 0 1 0 0 1 0 1 1
- Сигнал 2: 0 0 0 0 0 1 1 1 0 0 0 0 1 0 0 0 0 1 1 0 0 1 1 1 0 0 1 1 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 1 1 1 0 0 0 1 1 0 0 0 0 0 1 1 1 0 0 1 0 0 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 0 1 0 1 1 0 0 0 1 0 1 0 0 0 0 0 1 0 0 1 0 0 1 1 0 0 0 0 1 0 0 1 0 1 0 1 1 0 0 1 1 1 0 0 0 0 0 1 1 0 1 1 1 0 0 0 0 1 0 0 0 0 0 0 1 1 0 1 1 0 1 0 0 1 0 0 1 0 0 1 0 1 1 0 0 0 0 1 1 1 0 1 1 0 0 0 1 0 0 0 1 0 1 0 1 0 0 0 0 0 1 1 1 0 1 0 0 1 1 0 1 0 1 1 0 1 1 1 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 1 0 1 0 1 0 0 1 0

- Длина: 256

Полученный результат:

- Значение ПФВК: 34 10 2 2 26 30 -10 -6 42 6 -6 -34 18 -6 -14 -2 46 42 22 -2 -10 14 -18 -2 30 38 -14 -18 2 34 2 -2 18 6 -2 6 30 30 -22 2 50 18 -22 -14 2 10 -22 30 42 18 -22 -6 26 22 -18 6 42 30 -18 -22 30 30 -10 -10 66 30 -2 6 14 14 -26 -10 30 10 -22 -10 14 18 10 26 34 2 6 -22 6 22 -18 -22 42 34 2 22 18 2 -14 -10 54 34 -2 -6 6 22 -6 6 6 10 14 -6 46 26 -22 18 30 14 -14 -6 2 30 -22 -6 70 18 -10 -14 38 10 14 -2 34 26 6 -14 2 14 -14 -10 38 14 14 10 22 6 2 18 18 14 10 -14 18 10 6 -6 50 6 -2 -10 18 34 -26 14 62 50 -6 -22 -18 22 -26 -2 62 38 -2 6 38 26 -6 -18 34 6 -10 -22 22 26 -30 -2 34 18 -10 2 10 6 -18 14 38 -6 -6 -14 18 10 -22 2 42 -6 10 -18 18 18 -6 -6 38 18 6 6 26 30 2 -26 22 14 2 -18 22 22 -14 -10 14 22 2 2 10 30 -14 6 54 54 -2 -14 -18 14 -30 2 46 30 18 -18 6 -2 -18 -6 22 6 2 6 14 2 -34 10

ПРИЛОЖЕНИЕ Д

Поиск нелинейных дискретных сигналов с заданными значениями боковых пиков ПФАК и АФАК

(n – номер сигнала; koef – коэффициент децимации; sdvig – сдвиг последовательности на j - тактов)

n:1 koef:1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1 1 -1 -1 -1 1 -1 -1

Баланс символов последовательности: '+': 128 '-': 128

AFAK (1,1): 256 0 0 -2 -6 2 -2 0 -6 0 2 0 2 2 8 0 4 0 4 0 -6 -2 -14 -4 -14 -4 -6 -4 -4 0 2 -4 -4 0 8 0 -4 0 -14 -4 -12 -2 6 2 -10 0 -14 2 18 0 0 2 10 4 0 6 0 8 6 4 0 6 26 8 10 8 -2 8 0 12 10 8 12 10 14 12 0 16 -2 14 4 12 16 12 -2 10 8 8 -14 4 4 8 0 6 -16 8 -4 8 20 6 16 6 10 10 4 6 14 8 -6 10 4 6 12 8 22 6 28 2 4 4 18 2 -10 0 -16 2 0 2 4 4 2 2 14 2 6 0 -14 0 2 2 -24 -2 -16 -2 -8 0 -2 -4 14 -2 -14 -2 0 -6 -6 -2 -16 -4 -20 -6 2 -4 18 -2 -2 -4 0 0 14 -4 -6 -4 6 -4 -8 -2 4 -2 12 -2 10 2 -6 2 -2 2 0 -2 6 2 8 0 -2 -2 -22 -2 -2 -2 -4 -6 0 -4 -4 -4 -16 -4 -4 -4 -24 -6 8 -4 4 -6 -10 -2 6 -2 4 -6 -6 -4 -12 -2 -2 2 -8 -2 2 2 0 0 10 -2 2 -4 2 -4 -8 -2 -6 0 -6 0 2 2 0 0 6 -2 -6 -4 0 0 -4 -2

Мат. ожидание AFAK: 0.039063; Мат. ожидание AFAK: (модуль): 0.354492; Дисперсия AFAK: 3.893042; Дисперсия (модуль) AFAK: 3.497208; Max AFAK: 28.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 -1 1 1 -1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 1 -1 1 1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 1 1 1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1 1 -1 -1 -1 1 -1

AFAK (n: 1, sdv: 1, dec: 1) : 256 0 2 -2 -6 2 0 2 -4 2 4 2 2 4 8 0 4 0 4 2 -6 -2 -12 -2 -12 -2 -4 -4 -4 2 4 -4 -4 0 8 0 -4 2 -12 -4 -10 -2 6 2 -8 2 -14 2 20 0 2 2 12 4 2 8 0 10 8 4 2 6 28 10 12 10 0 8 0 14 12 8 14 10 16 12 0 18 -2 16 4 12 16 14 -2 12 8 10 -12 4 4 8 2 8 -16 8 -4 8 22 8 18 6 10 12 6 6 16 10 -6 12 6 8 12 10 22 8 30 4 4 6 18 2 -8 0 -14 4 2 4 4 6 2 2 14 2 8 2 -12 2 2 4 -22 0 -14 0 -8 2 0 -2 14 -2 -14 0 2 -6 -6 0 -16 -4 -18 -6 4 -2 18 -2 0 -4 0 2 16 -2 -4 -2 8 -4 -6 0 6 0 14 -2 10 2 -6 2 -2 4 2 -2 6 4 8 2 -2 -2 -22 -2 -2 0 -2 -4 0 -4 -4 -4 -16 -4 -4 -4 -22 -4 8 -4 6 -6 -10 -2 6 0 6 -6 -4 -4 -10 -2 -2 4 -6 -2 2 4 0 2 10 -2 4 -2 4 -4 -6 -2 -4 2 -4 2 2 4 0 2 6 -2 -4 -4 0 0 -2 0

Мат. ожидание AFAK: 0.101563; Мат. ожидание AFAK: (модуль): 0.370117; Дисперсия AFAK: 3.963078; Дисперсия (модуль) AFAK: 3.086853; Max AFAK: 30.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:2 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 -1 1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1

1 1 1 -1 1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 1 -1 1 1 -1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1 1 -1 -1 -1 1

AFAK (n: 1, sdv: 2, dec: 1) : 256 2 2 -2 -6 4 2 4 -2 4 6 2 4 4 8 0 4 0 6 2 -6 0 -10 0 -10 0 -4 -4 -2 4 4 -4 -4 0 8 0 -2 4 -12 -2 -10 -2 6 4 -6 2 -14 4 20 2 2 4 12 6 4 8 2 12 8 6 2 8 30 12 14 12 0 8 2 16 12 10 14 12 16 12 2 18 0 16 4 12 18 14 0 12 10 12 -12 4 4 10 4 8 -16 8 -4 10 24 10 18 6 12 14 6 8 18 10 -4 14 8 8 14 10 24 10 32 4 6 6 18 4 -8 2 -12 6 4 4 6 6 2 2 14 4 10 4 -10 2 4 6 -20 2 -12 0 -6 4 2 -2 14 -2 -12 2 2 -6 -4 0 -16 -2 -18 -4 6 -2 18 0 0 -4 2 4 18 0 -2 0 8 -2 -4 2 8 2 14 -2 10 2 -6 2 0 6 2 -2 8 4 10 2 -2 -2 -22 -2 0 2 0 -4 0 -4 -4 -4 -16 -4 -4 -2 -20 -4 8 -2 6 -6 -10 -2 8 2 6 -4 -4 -2 -10 -2 0 6 -6 -2 4 4 2 2 10 0 6 0 4 -2 -6 0 -2 4 -2 2 4 4 2 2 6 0 -4 -4 0 2 0 0

Мат. ожидание AFAK: 0.164063; Мат. ожидание AFAK: (модуль): 0.388672; Дисперсия AFAK: 4.024782; Дисперсия (модуль) AFAK: 2.840958; Max AFAK: 32.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:3 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 1 -1 -1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 1 -1 1 1 1 -1 1 1 -1 1 1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 1 -1 1 -1 1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1 1 -1 -1 -1

AFAK (n: 1, sdv: 3, dec: 1 256 0 0 0 -6 0 -2 0 -2 0 4 2 2 6 6 2 6 0 8 0 -6 -4 -10 0 -10 -2 -6 -4 -6 6 2 -6 -2 2 6 -4 -2 2 -12 -4 -8 0 2 0 -8 0 -14 2 16 4 2 2 8 2 2 4 -2 10 4 8 2 8 26 8 10 10 -2 8 -2 18 8 8 14 14 14 8 0 14 -2 14 6 12 20 14 2 8 10 14 -10 6 4 10 2 6 -14 6 -8 10 24 8 20 2 8 16 2 4 20 10 -8 10 6 8 16 10 20 10 34 4 8 8 14 6 -8 2 -12 2 2 0

4 8 0 4 14 4 10 0 -8 -2 0 6 -24 2 -10 0 -10 4 0 0 16 -2 -16 4 4 -10 -2 2 -20 -4 -18 -4 8 -4 14 -2 -2 -4 2 0 14 -4 -2 2 4 -2 -8 2 4 0 12 0 8 4 -8 -2 0 4 4 -6 10 4 8 0 0 0 -20 -2 0 -2 2 -6 2 -2 -6 -2 -14 -6 -4 -6 -18 -6 8 -4 4 -4 -8 -6 4 0 6 -6 -4 0 -12 -6 -4 4 -8 -6 6 4 0 0 10 0 6 2 4 -4 -10 0 -6 0 -4 -2 2 4 0 4 6 2 -2 -2 0 -2 -2-2 Мат. ожидание AFAK: 0.101563; Мат. ожидание AFAK: (модуль): 0.374023; Дисперсия AFAK: 4.017980; Дисперсия (модуль) AFAK: 3.129010; Max AFAK: 34.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:4 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 1 1 -1 1 1 -1 1 1 -1 1 1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1 1 -1 -1

AFAK (n: 1, sdv: 4, dec: 1) : 256 0 0 2 -4 2 0 2 0 0 6 2 2 6 6 2 8 0 8 2 -4 -2 -8 2 -10 -2 -4 -2 -6 6 2 -6 -2 2 8 -2 -2 4 -12 -4 -8 2 4 0 -8 2 -14 4 16 6 2 4 10 2 4 6 -2 12 4 10 4 10 28 10 10 10 0 10 -2 20 8 10 14 14 16 8 2 14 -2 14 8 12 22 14 4 10 10 14 -10 8 6 10 2 6 -14 8 -6 12 24 8 22 4 8 18 4 4 22 12 -6 10 8 8 18 12 22 10 36 4 8 10 14 8 -6 4 -10 2 4 0 4 8 0 6 16 6 12 0 -6 0 2 8 -22 2 -8 2 -8 4 0 0 18 0 -16 4 6 -10 -2 4 -20 -2 -16 -4 8 -2 14 -2 0 -2 4 2 16 -2 -2 4 6 0 -6 4 4 0 12 0 8 4 -6 0 0 4 6 -6 12 4 8 0 0 0 -18 0 2 -2 2 -6 2 -2 -6 -2 -14 -4 -2 -6 -18 -4 8 -4 4 -4 -6 -4 4 2 6 -4 -4 0 -10 -4 -4 4 -6 -6 8 4 0 2 12 2 6 4 4 -2 -8 2 -4 0 -2 -2 4 4 0 6 6 2 -2 0 2 -2 -2 0

Мат. ожидание AFAK: 0.164063; Мат. ожидание AFAK: (модуль): 0.390625; Дисперсия AFAK: 4.075762; Дисперсия (модуль) AFAK: 2.881644; Max AFAK: 36.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:5 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1 1 -1

AFAK (n: 1, sdv: 5, dec: 1) : 256 0 2 4 -2 4 2 4 0 2 6 2 2 6 6 4 8 0 10 4 -2 0 -6 2 -10 0 -2 -2 -6 6 2 -6 -2 4 10 -2 0 4 -12 -4 -6 4 4 0 -6 2 -12 4 18 6 4 6 10 4 6 6 0 12 6 12 6 12 30 10 10 12 2 10 0 20 10 10 14 16 16 10 2 14 -2 16 8 14 22 16 6 10 10 14 -8 10 6 10 2 6 -12 10 -4 12 24 10 24 4 10 20 4 6 24 14 -6 12 8 10 20 14 22 12 36 4 10 10 16 10 -4 6 -10 4 4 0 4 8 2 8 18 8 12 2 -4 2 4 10 -22 4 -6 4 -8 4 0 2 20 0 -16 6 6 -10 0 4 -18 0 -16 -4 10 -2 14 0 2 0 6 4 18 -2 0 6 8 2 -4 4 4 0 12 0 8 6 -4 0 0 6 6 -4 12 4 8 0 0 2 -16 2 2 -2 2 -6 2 -2 -6 -2 -12 -2 -2 -6 -16 -4 8 -4 4 -2 -4 -4 6 2 8 -4 -4 2 -8 -4 -4 6 -6 -4 8 4 2 4 14 2 8 4 6 0 -6 4 -4 2 -2 0 4 4 2 6 6 2 0 2 2 -2 0 0

Мат. ожидание AFAK: 0.226563; Мат. ожидание AFAK: (модуль): 0.414063; Дисперсия AFAK: 4.101681; Дисперсия (модуль) AFAK: 2.736975; Max AFAK: 36.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:6 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 1 1 -1 -1 1 1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 -1 -1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1 1

AFAK (n: 1, sdv: 6, dec: 1) : 256 2 4 6 0 6 4 4 2 2 6 2 2 6 8 4 8 2 12 6 0 2 -6 2 -8 2 -2 -2 -6 6 2 -6 0 6 10 0 0 4 -12 -2 -4 4 4 2 -6 4 -12 6 18 8 6 6 12 6 6 8 0 14 8 14 8 14 30 10 12 14 2 12 0 22 10 10 16 16 18 10 2 14 0 16 10 14 24 18 6 10 10 16 -6 10 6 10 2 8 -10 12 -4 12 26 12 24 6 12 20 6 8 26 14 -4 12 10 12 22 14 24 12 36 6 10 12 18 12 -2 6 -8 4 4 0 4 10 4 10 20 8 14 4 -2 4 6 10 -20 6 -4 4 -8 4 2 4 20 0 -14 6 6 -8 0 6 -16 0 -16 -2 10 -2 16 2 4 2 8 6 18 0 2 8 10 4 -4 4 4 0 12 0 10 8 -4 0 2 6 8 -4 12 4 8 0 2 4 -14 2 2 -2 2 -6 2 -2 -6 0 -10 -2 -2 -4 -16 -4 8 -4 6 0 -4 -2 6 4 8 -4 -2 4 -8 -4 -2 6 -4 -4 8 6 4 6 14 4 8 6 8 2 -4 4 -2 2 0 0 4 6 2 6 6 4 2 2 2 0 0 0

Мат. ожидание AFAK: 0.289063; Мат. ожидание AFAK: (модуль): 0.443359; Дисперсия AFAK: 4.103581; Дисперсия (модуль) AFAK: 2.670738; Max AFAK: 36.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:7 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 1 1 -1 -1 1 1 -1 -1 1 1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1

1 1 -1 1 -1 1 1 1 -1 1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1

AFAK (n: 1, sdv: 7, dec: 1) : 256 -2 0 2 0 2 2 4 4 0 4 0 4 2 6 6 4 2 8 6 0 4 -4 -2 -8 0 0 0 -4 4 0 -6 -4 8 6 -2 2 6 -16 -6 -2 2 4 0 -6 6 -16 4 14 4 8 2 8 8 6 6 -4 10 4 10 4 12 28 10 12 16 -2 10 -4 20 8 10 14 16 16 8 4 14 -2 12 8 10 20 16 8 12 10 16 -4 8 8 12 2 8 -10 14 -6 8 26 10 20 6 14 16 6 4 24 14 -6 8 10 12 20 10 22 14 36 8 6 12 18 12 0 6 -10 6 6 2 4 6 0 6 18 8 10 4 -2 4 8 6 -20 2 -6 6 -10 4 2 6 18 0 -16 8 6 -6 -4 6 -14 -2 -16 0 8 -6 16 2 4 -2 4 4 14 0 2 4 6 2 -2 6 2 2 10 0 6 6 -6 0 0 6 6 -6 14 2 10 -4 2 4 -16 0 4 0 4 -4 4 -4 -4 -6 -4 -8 0 -6 -2 -14 -6 10 -8 6 -2 -4 -4 2 6 10 -8 -6 2 -6 -8 0 6 -6 -6 4 2 0 4 14 6 4 2 8 2 -2 4 0 -2 -2 2 0 4 0 4 2 4 0 4 2 2 2 2

Мат. ожидание AFAK: 0.226563; Мат. ожидание AFAK: (модуль): 0.413086; Дисперсия AFAK: 3.933054; Дисперсия (модуль) AFAK: 2.575456; Max AFAK: 36.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:8 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 1 -1 1 -1 -1 1 -1 -1 1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 1 1 -1 -1 -1 1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 1 1 -1 1 1 1 1 1

AFAK (n: 1, sdv: 8, dec: 1) : 256 -2 -4 -2 -4 4 -2 2 6 2 2 -2 0 4 4 2 4 -2 8 2 2 6 -4 -2 -10 2 -2 2 -2 6 -4 -10 -2 4 8 -4 0 6 -16 -8 -4 2 2 0 -8 6 -14 0 10 2 4 2 6 4 8 6 -8 6 0 6 2 10 24 6 14 16 0 6 -6 18 4 8 14 14 18 6 0 16 -2 10 4 6 18 14 6 12 10 18 -2 10 6 12 2 8 -8 16 -6 4 24 10 16 4 14 16 2 6 20 12 -6 4 6 14 20 8 20 10 38 8 6 8 18 14 0 8 -8 4

8 2 4 6 -4 4 14 4 10 0 -2 6 8 6 -24 4 -8 4 -10 0 4 8 18 -2 -14 4 8 -6 -4 4 -12 -2 -18 2 8 -10 12 2 4 -2 2 0 10 -4 2 4 4 0 -4 8 4 0 10 -4 8 4 -10 -2 0 4 8 -8 12 4 6 -4 -2 6 -14 -2 2 2 6 -2 6 -4 -10 -2 -10 0 -4 -4 -12 -4 6 -8 4 -2 -6 -4 0 4 10 -8 -8 0 -10 -6 -4 8 -4 -10 0 -2 -2 0 12 6 4 -2 4 4 -2 6 0 0 -4 -2 2 2 -2 0 -2 2 2 0 4 4 4 2

Мат. ожидание AFAK: 0.164063; Мат. ожидание AFAK: (модуль): 0.391602; Дисперсия AFAK: 3.883605; Дисперсия (модуль) AFAK: 2.684340; Max AFAK: 38.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:9 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 1 1 1 -1 -1 1 1 1 -1 1 -1 1 1 -1 -1 -1 1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1 1

AFAK (n: 1, sdv: 9, dec: 1) : 256 -2 -4 -6 -6 0 0 0 4 4 4 -6 -2 2 4 -2 0 -2 4 4 0 6 -4 0 -8 0 0 0 0 6 -4 -12 -6 6 6 -2 -4 2 -14 -6 -8 0 2 -2 -8 4 -14 0 8 -2 0 0 6 2 4 6 -8 2 -4 4 0 6 20 4 10 18 0 8 -8 14 2 4 12 16 16 6 -2 12 0 10 0 4 16 12 2 8 12 20 0 12 6 8 2 10 -6 16 -6 6 20 6 18 0 10 16 4 2 22 8 -10 4 4 10 22 10 16 8 34 8 6 8 16 14 2 10 -6 6 4 2 4 6 -2 0 10 0 6 0 -4 6 8 6 -22 2 -6 0 -14 2 2 8 20 0 -18 6 4 -6 -2 6 -16 0 -16 -2 8 -10 8 -2 4 0 2 -4 6 -8 -2 6 6 -2 -6 6 6 0 6 -2 6 4 -12 -6 -2 6 6 -6 10 0 6 -8 0 4 -12 0 0 0 8 0 6 -4 -8 -4 -10 -2 -2 -2 -14 -4 6 -10 4 -4 -6 -6 2 0 6 -6 -6 -4 -12 -10 -2 6 -4 -10 -4 -4 -6 -2 8 2 4 -2 2 0 0 6 2 2 -4 -4 0 4 -6 -4 -4 0 -2 2 2 6 4 2

Мат. ожидание AFAK: 0.101563; Мат. ожидание AFAK: (модуль): 0.363281; Дисперсия AFAK: 3.680725; Дисперсия (модуль) AFAK: 2.826804; Max AFAK: 34.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:10 1 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1 1

AFAK (n: 1, sdv: 10, dec: 1) : 256 -2 -4 -4 -10 -2 -2 2 2 2 4 -4 -4 -2 0 -2 -4 -6 6 2 0 2 -2 2 -6 2 -2 2 -4 6 -2 -12 -8 4 8 -6 -4 0 -16 -6 -6 -4 0 -2 -10 4 -18 2 8 -6 -2 -4 4 2 0 2 -8 2 -6 2 -4 2 18 0 8 14 2 10 -8 12 -2 2 10 14 16 4 -2 10 -4 10 2 2 14 8 -2 6 10 22 2 12 6 8 0 12 -6 16 -4 6 20 4 14 0 6 14 4 4 18 8 -14 2 4 8 20 10 18 4 30 4 6 10 16 12 4 12 -4 6 4 -2 4 8 -2 0 6 -4 2 -2 -4 2 8 8 -20 4 -10 0 -16 0 2 6 22 0 -16 2 4 -8 0 6 -14 -2 -16 -2 4 -10 8 -6 2 0 2 -4 2 -12 -4 4 8 0 -8 4 2 0 8 -4 6 2 -12 -8 -4 4 8 -8 10 -4 2 -6 -2 6 -14 2 2 -2 6 0 6 -2 -6 -4 -12 0 -4 0 -14 -8 8 -10 2 -4 -8 -4 -2 0 4 -8 -6 -2 -16 -12 -4 6 -8 -10 -2 -8 -8 -6 4 -2 0 0 2 -2 -4 8 4 2 -2 -2 -2 0 -6 -6 -6 -4 -4 0 4 2 4 2

Мат. ожидание AFAK: 0.039063; Мат. ожидание AFAK: (модуль): 0.363281; Дисперсия AFAK: 3.685198; Дисперсия (модуль) AFAK: 3.278336; Max AFAK: 30.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:11 1 1 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 1 -1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1 1

AFAK (n: 1, sdv: 11, dec: 1) : 256 -2 -2 -4 -8 -4 -4 0 4 -2 2 -2 -4 -6 -4 -6 -4 -8 4 2 -4 4 -4 4 -4 4 0 -2 -4 4 -2 -10 -6 2 4 -6 -6 2 -20 -8 -6 -2 -4 -4 -10 0 -16 -2 8 -4 -6 -6 0 -2 0 -2 -12 4 -4 -2 -8 0 14 -2 4 12 0 10 -6 12 -4 0 8 10 14 4 -4 10 -8 8 4 4 10 4 -4 4 8 20 2 12 6 10 2 8 -6 18 -4 6 22 4 10 -4 8 10 2 4 18 4 -12 -2 2 10 16 8 18 4 26 0 4 10 18 14 2 14 -4 6 4 -2 2 8 -2 0 6 -8 0 -6 -8 2 6 10 -18 4 -10 -2 -14 -4 0 8 18 2 -16 2 2 -6 -4 8 -12 -2 -20 -2 4 -14 8 -4 -2 -4 2 -4 2 -14 -6 2 6 2 -6 0 -2 -2 10 -4 4 2 -14 -6 -6 2 6 -8 6 -4 0 -8 0 4 -12 0 4 0 2 -4 8 0 -6 -2 -10 -2 -2 -4 -14 -6 4 -8 2 -6 -6 -8 -2 -2 6 -12 -8 -2 -14 -14 -8 2 -8 -12 -2 -6 -12 -10 0 -6 -2 -4 4 -2 -6 6 4 4 0 0 -2 -4 -8 -4 -10 -6 -6 -2 0 2 0 2

Мат. ожидание AFAK: -0.023438; Мат. ожидание AFAK: (модуль): 0.364258; Дисперсия AFAK: 3.559769; Дисперсия (модуль) AFAK: 3.303152; Max AFAK: 26.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500 Мат. ожидание PFAK: (модуль): 0.062500 Дисперсия PFAK: 0.187990 Дисперсия (модуль) PFAK: 0.187990 Max PFAK: -4

n:1 sdvig:12 1 1 1 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 1 -1 -1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1

-1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 -1

AFAK (n: 1, sdv: 12, dec: 1) : 256 0 -2 -2 -6 -2 -6 -2 0 0 0 -6 -4 -6 -8 -10 -6 -6 0 -2 -2 2 -2 2 -2 6 0 -2 -6 4 -4 -8 -4 2 0 -8 -4 -2 -18 -12 -8 -2 -2 -8 -14 2 -20 -2 6 -4 -4 -10 -4 -6 -4 -2 -14 2 -4 -2 -10 -4 12 -6 2 10 -4 8 -6 14 -2 -2 4 8 10 2 -4 6 -6 6 2 4 10 2 -6 2 6 16 -2 12 8 12 2 8 -8 18 -4 8 22 4 10 -6 4 12 -2 0 18 6 -16 0 0 6 18 4 14 4 26 -2 0 8 20 16 4 10 -4 6 4 0 2 4 -2 0 6 -6 -4 -10 -12 0 8 8 -18 4 -8 0 -18 -2 -2 4 20 -2 -16 4 4 -10 -2 6 -12 -2 -20 -6 4 -14 6 -4 -2 -8 -2 -4 4 -12 -8 0 4 0 -6 0 -4 -4 6 -2 4 0 -12 -8 -4 0 2 -12 6 -6 2 -10 -2 6 -14 2 2 0 2 -6 6 0 -4 0 -8 0 -6 -4 -16 -6 6 -12 4 -4 -10 -8 -4 0 2 -10 -12 -4 -12 -14 -12 -2 -10 -12 -4 -6 -12 -14 -4 -8 -6 -6 0 0 -4 2 2 6 2 0 -2 -2 -10 -8 -8 -8 -8 -6 -4 -2 0 -2

Мат. ожидание AFAK: -0.085938 Мат. ожидание AFAK: (модуль): 0.371094 Дисперсия AFAK: 3.661301 Дисперсия (модуль) AFAK: 2.874046 Max AFAK: 26

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500 Мат. ожидание PFAK: (модуль): 0.062500 Дисперсия PFAK: 0.187990 Дисперсия (модуль) PFAK: 0.187990 Max PFAK: -4

n:1 sdvig:13 -1 1 1 1 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 -1 1 1 -1 -1 1 1 1 -1 -1 -1 -1 1 1 -1 -1 -1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1 1 1

AFAK (n: 1, sdv: 13, dec: 1) : 256 2 -2 -2 -6 -2 -6 0 0 0 2 -4 -2 -4 -6 -10 -6 -4 2 -2 -2 2 -2 2 -2 8 2 -2 -4 4 -4 -8 -2 4 0 -8 -2 -2 -16 -12 -6 -2 0 -6 -14 4 -18 -2 8 -4 -2 -8 -2 -4 -2 -2 -14 4 -2 -2 -8 -4 14 -6 2 12 -4 10 -6 14 -2 0 4 10 10 4 -2 6 -6 6 4 6 10 2 -6

2 8 18 0 12 8 14 4 8 -6 20 -4 10 24 6 10 -4 4 14 0 2 18 8 -16 0 2 6 20 6 16 6 26 0 0 8 20 16 6 12 -2 8 4 2 4 6 0 2 6 -4 -2 -8 -12 0 8 10 -16 4 -8 2 -18 -2 0 4 22 0 -16 4 6 -10 -2 8 -10 0 -18 -4 6 -14 8 -2 0 -6 0 -4 4 -12 -8 0 4 2 -4 0 -4 -2 6 0 4 0 -12 -8 -4 2 4 -10 6 -6 2 -10 -2 6 -14 2 4 2 2 -6 8 0 -4 0 -8 2 -4 -4 -14 -6 8 -12 4 -2 -8 -8 -4 2 2 -8 -12 -4 -10 -12 -10 -2 -8 -12 -2 -4 -10 -12 -4 -6 -6 -4 0 0 -2 2 2 6 4 2 -2 -2 -8 -8 -8 -8 -6 -4 -2 0 2 0

Мат. ожидание AFAK: -0.023438 Мат. ожидание AFAK: (модуль): 0.365234 Дисперсия AFAK: 3.724475 Дисперсия (модуль) AFAK: 3.467122 Max AFAK: 26

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:14 1 -1 1 1 1 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 -1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1 -1

AFAK (n: 1, sdv: 14, dec: 1): 256 0 0 0 -4 0 -6 2 -2 -4 -2 -4 -6 -8 -4 -8 -10 -8 0 0 -4 0 0 0 -2 4 4 -2 -2 6 -6 -8 -6 6 2 -8 -4 -6 -14 -16 -4 -6 -4 -4 -14 0 -20 -2 6 -4 -6 -8 -2 -8 -4 -4 -18 4 -4 -6 -6 -4 12 -8 -2 10 -8 8 -8 12 -2 2 4 8 6 0 -4 4 -4 2 4 4 8 4 -4 -2 4 14 -2 10 4 14 6 8 -6 22 -8 10 24 8 10 -2 4 10 -4 4 14 6 -14 0 0 6 16 2 16 4 22 2 2 6 18 12 6 12 -2 6 4 2 4 6 0 0 6 -4 -2 -6 -14 -2 4 6 -14 2 -8 4 -16 -2 -2 4 18 -2 -14 0 8 -8 -2 4 -10 -4 -18 -4 8 -18 8 -2 -4 -6 2 -6 2 -10 -6 2 0 -2 -6 -2 -4 0 2 -2 2 2 -10 -10 -4 -2 4 -12 4 -8 4 -12 0 4 -16 2 0 4 0 -6 10 -2 -6 2 -8 2 -2 -4 -16 -6 6 -10 4 -6 -6 -6 -8 4 -2 -6 -14 -4 -14 -16 -8 -2 -10 -16 -6 -4 -14 -10 -4 -8 -10 -6 -2 -4 -4 4 4 2 0 4 0 -2 -6 -6 -10 -12 -6 -8 -6 -4 -2 -2

Мат. ожидание AFAK: -0.085938; Мат. ожидание AFAK: (модуль): 0.373047; Дисперсия AFAK: 3.551497; Дисперсия (модуль) AFAK: 2.758850; Max AFAK: 24.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 Мат. ожидание PFAK: -0.062500

Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:15 -1 1 -1 1 1 1 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 1 -1 1 -1 -1 1 -1 1 1 1 -1 1 -1 -1 1 -1 -1 1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1 -1

AFAK (n: 1, sdv: 15, dec: 1) : 256 0 0 0 -4 2 -6 2 0 -2 0 -2 -4 -8 -4 -6 -8 -8 0 0 -4 0 0 2 0 4 6 -2 -2 6 -4 -6 -6 6 4 -8 -2 -6 -12 -16 -2 -4 -4 -2 -12 0 -18 -2 8 -2 -4 -6 0 -8 -4 -2 -16 4 -2 -6 -4 -4 12 -6 -2 12 -8 8 -8 14 -2 4 4 10 8 0 -4 4 -2 4 4 4 8 4 -2 0 6 14 -2 12 6 14 8 10 -6 24 -6 12 24 10 10 0 6 12 -4 6 14 6 -12 0 2 8 18 4 16 6 22 2 2 6 20 14 8 14 -2 8 6 4 6 8 0 2 8 -2 -2 -6 -14 0 6 6 -14 4 -8 4 -14 -2 0 6 18 -2 -12 0 8 -6 0 6 -8 -2 -16 -4 10 -16 10 0 -2 -6 2 -6 2 -10 -6 4 2 -2 -6 0 -4 2 2 -2 2 2 -10 -8 -2 0 4 -12 4 -8 4 -12 0 4 -14 4 0 4 2 -6 10 -2 -6 4 -6 2 0 -4 -14 -6 6 -8 6 -6 -6 -4 -8 6 -2 -6 -12 -2 -12 -16 -6 -2 -8 -14 -4 -2 -14 -8 -4 -6 -10 -6 0 -4 -4 4 6 4 0 4 2 -2 -6 -6 -8 -10 -4 -6 -4 -2 -2 0

Мат. ожидание AFAK: -0.023438; Мат. ожидание AFAK: (модуль): 0.364258; Дисперсия AFAK: 3.551926; Дисперсия (модуль) AFAK: 3.295309: Max AFAK: 24.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0

0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

n:1 sdvig:16 -1 -1 1 -1 1 1 1 1 1 1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 1 1 1 -1 1 -1 1 1 1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 1 -1 1 -1 1 1 1 -1 -1 -1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 -1 -1 -1 1 1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 -1 -1 1 1 1 1 1 -1 1 1 1 1 1 1 -1 -1 1 -1 -1 1 1 -1 1 -1 -1 1 -1 -1 1 1 -1 -1 -1 1 1 1 -1 1 1 1 1 1 -1 1 1 1 1 -1 -1 -1 -1 1 -1 1 1 1 -1 1 -1 1 1 1 -1 1 1 1 -1 1 1 -1 1 1 -1 1 -1 -1 1 1 1 -1 1 -1 1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 -1 1 1 -1 -1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1 -1 -1 1 -1 1 1 -1 -1 -1 -1 -1 -1 1 1 -1 -1 1 1 1 1 1 -1 -1 1 -1 -1 -1

AFAK (n: 1, sdv: 16, dec: 1): 256 0 0 0 -2 2 -6 4 2 0 2 0 -4 -8 -2 -4 -8 -8 0 0 -4 0 2 4 0 6 6 -2 -2 8 -2 -6 -6 8 4 -6 -2 -4 -12 -14 0 -4 -2 0 -12 2 -18 0 10 0 -2 -4 0 -8 -2 0 -16 6 -2 -4 -4 -4 14 -6 0 12 -8 8 -6 14 0 4 6 12 8 0 -4 6 0 4 4 4 8 6 0 2 6 14 0 14 6 16 10 10 -4 26 -4 12 26 10 12 2 8 12 -2 6 14 8 -12 2 4 10 20 4 18 6 22 2 2 8 22 16 10 14 0 10 8 6 8 8 2 4 10 -2 -2 -6 -12 2 6 6 -12 4 -8 6 -14 0 2 6 18 0 -12 0 10 -4 2 8 -6 0 -16 -2 12 -14 12 2 -2 -6 2 -6 2 -10 -4 6 2 -2 -4 0 -2 2 2 -2 2 2 -8 -6 0 0 4 -12 4 -8 4 -12 0 6 -12 4 0 6 2 -6 10 -2 -4 6 -6 4 0 -2 -14 -6 8 -6 6 -6 -4 -4 -6 6 -2 -4 -10 0 -12 -14 -6 0 -6 -12 -2 -2 -12 -8 -2 -6 -10 -4 0 -4 -4 6 8 4 0 6 2 -2 -6 -4 -6 -8 -2 -4 -2 -2 0 0

Мат. ожидание AFAK: 0.039063 Мат. ожидание AFAK: (модуль): 0.360352; Дисперсия AFAK: 3.634218; Дисперсия (модуль) AFAK: 3.231032; Max AFAK: 26.

PFAK: 256 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 0 0 -4 0 0 0 0 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 -4 0 -4 0 0 0 -4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 -4 0 -4 0 0 0

Мат. ожидание PFAK: -0.062500; Мат. ожидание PFAK: (модуль): 0.062500; Дисперсия PFAK: 0.187990; Дисперсия (модуль) PFAK: 0.187990; Max PFAK: -4.

Таблица Д.1

Значения боковых пиков АФАК нелинейных систем сигналов в конечных полях Галуа (Период сигнала N = 256)

Значение АФАК	№ п.п.	Коэф. деци-мации	Номера циклических сдвигов
-18	6	11	94,95
	14	27	91
	20	39	153
	24	47	96, 106, 107
	70	139	151
	74	147	239, 240
	84	167	99, 100
	101	201	85,86
	105	209	147, 150, 155, 157
	110	219	138
	123	245	159, 160, 162
18	6	11	92, 93, 96
	9	17	42
	10	19	93
	12	23	141
	24	47	97, 98, 100, 104, 105, 108
	28	55	169, 170
	41	81	166
	44	87	235
	45	89	155,156
	56	111	32
	59	117	104
	88	175	149,450,151
	105	209	148,149,158,159
	109	217	107
	110	219	139
	115	229	164
	120	239	214,215
	122	243	149
	123	245	161
Всего сигналов с Rбмакс = +-18 существует 56			

Продолжение Таблицы Д1

20	3	5	92,106,108,114,150
	4	7	33
	6	11	91,97,98,99,100
	9	17	8,43
	10	19	94,95,148,149,151
	11	21	224,225,227,228,229,234,233,234,236
	12	23	126,134,142
	14	27	57,92
	15	29	234
	17	33	9,10,243,251,252
	20	39	156,157
	21	41	234
	22	43	212,213,214
	23	45	185,186
	24	47	101,102,112,180
	25	49	46,47,48
	27	53	216,219,221,233
	28	55	171,241
	29	57	156
	32	63	28,29,203,204
	33	65	25,245,246
	38	75	225
	39	77	19,20,27,35
	41	81	68,162,163,167
	44	87	231,232,233,234,236
	45	89	151,154,157,158,159
	48	95	20,24,26,27
	49	97	148,231
	50	99	92,201
	51	101	86,84,88
	52	103	95,103,104,107,108,109
	53	105	98
	54	107	79,80,139,140,141,142
	55	109	100,101
	56	111	33

	58	115	113,202
	59	117	73,87,91,93,100,101,102,105,106,107,110
	60	119	58
	61	121	18
	62	123	93,149
	64	127	13,17,20
	69	137	197
	70	139	155,162,164,168,177,178,179,182
	71	141	23,40,41
	72	143	29,33,38
	73	145	218,224,227,230
	74	147	153,238
	75	149	220,221
	76	151	157,158,159
	77	153	143,144,149,150,160,163,173
	78	155	167,168,169,201,202,203
	79	157	54
	80	159	102,103,106
	81	161	39,40,41,229
	85	169	24
	88	175	90,92,142,145,147,148,152,187
	90	179	237,238
	91	181	30
	92	183	91
	96	191	152
	97	193	52,53
	100	199	100,101,102
	101	201	87,9
	102	203	34,36,39
	104	207	66,208,209,212
	105	209	66,156,160
	107	213	41,42,103,105,108
	109	217	104,105,106
	110	219	140
	112	223	14,15,16,246,249,250
	116	231	48

	117	233	177
	118	235	150,151,152,154,158,218,219,223,224,226,240
	119	237	149,165,166
	120	239	207,209,212,216
	122	243	13,15,24,140,141,142,143,150,248
	123	245	165,166,167,172
	124	247	68
	126	251	100,102,105,151,164
	127	253	95
-20	2	3	157,16
	3	5	91,105,153,155
	4	7	32,103
	5	9	84,187
	6	11	83,88,89,90
	7	13	106,112,113,114,115,116,118,189,231,240,242,243,247
	9	17	9,10,39,40,41,46,48
	10	19	91,92
	11	21	31,32,33,34,97,101,103,104,105,223232,235
	12	23	78,124,130,140,224,236
	13	25	207,227
	14	27	224
	17	33	8
	19	37	117
	20	39	152
	22	43	67
	24	47	95,99,109,110,111,189
	25	49	43,186,187,189
	28	55	165,167,168
	32	63	27,202
	33	65	102,103,227
	38	75	80,101
	39	77	18
	41	92	105,165
	43	85	7,8
	48	95	216

	49	97	137
	51	101	52,53,54
	52	103	92,204,229,230
	54	107	34
	55	109	14,16,102
	56	111	31
	57	113	217
	58	115	112,204,215
	59	117	76,77,78
	62	123	148
	63	125	56
	64	127	11,12
	66	131	199
	67	133	162
	68	135	152,155
	70	139	149,150,153,154
	71	141	24,51,53
	73	145	217,222,223
	74	147	154,155,241,242
	75	149	175,176
	76	151	215
	77	153	25,35,51
	79	157	163
	80	159	24
	84	167	96,97,98,101
	88	175	93
	90	179	228,235,236
	91	181	154,175
	97	193	51,145,227,228
	100	199	99
	101	201	84,88
	104	207	68,69,207
	105	209	75,145,146,151,153,154
	106	211	69
	107	213	107,109,188
	109	217	100,101,102,103
	112	223	13,245

	115	229	31,163
	116	231	28,49
	117	233	17,18,20,113,114
	118	235	221,222
	119	237	164
	120	239	92,213
	122	243	8,12,66
	123	245	158,163,164
	124	247	171
	125	249	149,152,223
	126	251	147,163
	127	253	98
Всего сигналов с Rбмакс = +-20 существует 470			

ПРИЛОЖЕНИЕ Е

Производные системы сигналов (ПСС) на основе нелинейных криптографических сигналов

Криптографические сигналы, отобранные по заданным значениям боковых пиков ПФАК:

1)1 1 1 0 0 0 1 1 1 1 1 0 1 0 0 0 0 1 1 1 1 1 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 1 0 0 0
1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 0 1 0 1 1: 34 0:30
2)1 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0
0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1: 26 0:38
3)0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0
0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 1: 26 0:38
4)0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0
0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 1: 26 0:38
5)0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0
0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 1: 26 0:38
6)0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0
1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1: 26 0:38
7)0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 1 0 1 1 1
0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1: 27 0:37
8)0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 1 0 1 1 1 0
0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 1: 28 0:36
9)0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 1 0 1 1 1 0 0
1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0 1: 28 0:36
10)0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 0 1 0 1 1 1 0 0 1
1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0 0 1: 28 0:36
11)0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0
0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 1: 27 0:37
12)0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0
0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0 1: 27 0:37
13)0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0
1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0 0 1: 27 0:37
14)0 1 0 0 0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 1 1 0 1 1 1 1 1
0 1 1 1 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 1 0 1: 28 0:36

Статистические характеристики и значения пиков ПФАК криптографических сигналов:

1)64 0 -8 -4 -4 0 -8 0 0 4 0 4 4 -8 -4 8 -4 -4 0 4 4 -4 4 -4 0 8 4 4 -4 -8 -4 0 -8 0 -4 -8 -4 4 4 8 0 -4 4 -4 4 4 0 -4 -4 8 -4 -8 4 4 0 4 0 0 -8 0 -4 -4 -8 0 PFAKmin: -4 PFAKmax: -8 MO: -0.09375 |MO|: 0.46875 DISP: 0.5763694553724894 |DISP|: 0.3384787011890674 On start: 1

2)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

3)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

4)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

5)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

6)64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

7)64 4 -8 4 4 0 0 4 -4 4 0 -8 4 0 4 0 4 0 -8 0 0 8 0 0 -8 -4 -4 4 8 4 4 4 -4 4 4 4 4 8 4 -4 -4 -8 0 0 8 0 0 -8 0 4 0 4 0 4 -8 0 4 -4 4 0 0 4 4 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.0703125 |MO|: 0.4296875 DISP: 0.5553298776598447 |DISP|: 0.350712702793093

8)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921 On start: 1

9)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921 On start: 1

10)64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921 On start: 1

11)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8 PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

12)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8 PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

13)64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0 0 4 8 8 4 -4 -8 -8 0 4 8 PFAKmin: 4 PFAKmax: 8 MO: 0.0703125 |MO|: 0.5234375 DISP: 0.6476900319675074 |DISP|: 0.3767205345969094

14)64 8 -4 4 4 0 0 4 -4 -4 4 -4 -8 0 -4 0 8 0 8 -4 -8 -4 -8 8 -8 0 0 4 0 -4 4 4 8 4 4 -4 0 4 0 0 -8 8 -8 -4 -8 -4 8 0 8 0 -4 0 -8 -4 4 -4 -4 4 0 0 4 4 -4 8 PFAKmin: -4 PFAKmax: 8 MO: 0.0 |MO|: 0.5 DISP: 0.6236095697723273 |DISP|: 0.3618734420321171

Отобрано по критерию минимума максимальных боковых пиков ПФАК 14 сигналов.

Матрицы Адамара:

1 1 1 1
1 0 1 0
1 1 0 0
1 0 0 1

1 1 1 1 1 1 1 1
1 0 1 0 1 0 1 0
1 1 0 0 1 1 0 0
1 0 0 1 1 0 0 1
1 1 1 1 0 0 0 0
1 0 1 0 0 1 0 1
1 1 0 0 0 0 1 1
1 0 0 1 0 1 1 0

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0
1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0
1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1
1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1
1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0
1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0
0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1
1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0
0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1
1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1
0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0
0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0
1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1
0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1
1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1
0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1
1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0
0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0
1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1
1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1
1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0
1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1
1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0
1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0
1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0
1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 1 1 0 0
1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 1 0 0 1
1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0

1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1
0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 1 0 1 0
0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0
1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0
0 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0
1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 1 0 0 1
0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1
0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0
1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1
0 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0
1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 1 0
0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1
1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0
1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0
1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 0
1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1
1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 0 0 1 1
1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1
1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 0 1 1 0
1 0 0 1 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1
0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1
0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0
1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1
1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0
1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1
1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1
1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 0 1 1 0
1 0 0 1 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1
0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1
0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0
1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1
1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0
1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 0 0 0 0 1 1 1 0 0 0 1
1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0

1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0
1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1
1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0
1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0
1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0
1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0
1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 1
1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1
1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1
0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0
1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1
1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0
0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1
1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0 0 1
0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
0 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 0
1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
0 0 1 1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0
1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
0 1 1 0 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1
1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0
1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0
1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1
1 0 1 0 1 0 1 0 0 1 0 1 1 0 1 0 0 1
1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1
1 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0 0 0
1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0
1 0 0 1 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0
1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0
1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0
1 0 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1

1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1

1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0

1 1 1 1 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1

1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0

1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0

1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0 1 0 0 1 1 0 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1

0 0 0 1 1 1 0 0 0 0 0 1 0 1 1 1 1 0 0 0 0 0 1 0 0 0 1 1 0 0 1 1 0 0 1 1 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0 1 1 0 1 1 0 0 1 1 0 1 0 1 0 1:30 0:34

Производные системы сигналов на основе криптографических сигналов (значения боковых пиков корреляционных функций (КФ) и статистические характеристики КФ)

64 0 -8 -4 -4 0 -8 0 0 4 0 4 4 -8 -4 8 -4 -4 0 4 4 -4 4 -4 0 8 4 4 -4 -8 -4 0 -8 0 -4 -8 -4 4 4 8 0 -4 4 -4 4 4 0 -4 -4 8 -4 -8 4 4 0 4 0 0 -8 0 -4 -4 -8 0

PFAKmin: -4 PFAKmax: -8 MO: -0.09375 |MO|: 0.46875

DISP: 0.5763694553724894 |DISP|: 0.3384787011890674

0 1 0 0 1 0 0 1 0 1 0 0 0 0 1 0 1 1 0 1 0 1 1 1 0 1 1 0 0 1 1 0 0 1 1 0 1 1 1 1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 1 1 0:30 1:34

64 0 -8 4 -4 0 -8 0 0 -4 0 -4 4 8 -4 -8 -4 4 0 -4 4 4 4 4 0 -8 4 -4 -4 8 -4 0 -8 0 -4 8 -4 -4 4 -8 0 4 4 4 4 -4 0 4 -4 -8 -4 8 4 -4 0 -4 0 0 -8 0 -4 4 -8 0

PFAKmin: 4 PFAKmax: -8 MO: -0.09375 |MO|: 0.46875

DISP: 0.5763694553724894 |DISP|: 0.3384787011890674

0 0 1 0 1 1 1 1 0 0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 1 1 0 1 0 1 1 0 0 0 0 1 1 1 1 0 1 0 1 0 1 0 0 1 1:26 0:38

64 0 8 12 -4 8 8 0 0 -4 0 4 4 8 4 0 -4 20 0 -12 4 -12 -4 4 0 -8 -4 4 -4 8 4 0 -8 0 4 8 -4 4 -4 -8 0 4 -4 -12 4 -12 0 20 -4 0 4 8 4 4 0 -4 0 0 8 8 -4 12 8 0

PFAKmin: -4 PFAKmax: 20 MO: -0.09375 |MO|: 0.625

DISP: 0.8348850862727943 |DISP|: 0.5649747187520014

0 1 1 1 1 0 1 0 0 1 1 1 0 0 0 1 1 1 1 0 0 1 0 0 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 0 0 0 0 1 1 0 1 0 0 1 0 1 1 1 1 1 1 1 1 0 0 1:34 0:30

64 0 8 -12 -4 -8 8 0 0 4 0 -4 4 -8 4 0 -4 -20 0 12 4 12 -4 -4 0 8 -4 -4 -4 -8 4 0 -8 0 4 -8 -4 -4 -4 8 0 -4 -4 12 4 12 0 -20 -4 0 4 -8 4 -4 0 4 0 0 8 -8 -4 -12 8 0

PFAKmin: -4 PFAKmax: -20 MO: -0.09375 |MO|: 0.625 DISP: 0.8444845393105501 |DISP|: 0.5649747187520014
0 0 0 1 0 0 1 1 0 0 0 1 1 0 0 0 1 0 0 0 1 1 0 1 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 1 1 1 0 1 0 1 0 0 0 1 0 0 0 1 0 1 0 0 1 0 1 0 1 1: 28 0:36
 64 -8 0 -12 4 8 0 0 0 4 -8 -4 -4 8 4 8 -4 20 -16 4 -4 12 -4 -4 0 -8 4 -12 4 0 12 0 -8 0 12 0 4 -12 4 -8 0 -4 -4 12 -4 4 -16 20 -4 8 4 8 -4 -4 -8 4 0 0 0 8 4 -12 0 -8
PFAKmin: 4 PFAKmax: 20 MO: -0.09375 |MO|: 0.71875 DISP: 0.9553524941610141 |DISP|: 0.61619541251429
0 1 0 0 0 1 1 0 0 1 0 0 1 1 0 1 1 1 0 1 1 0 0 0 0 1 1 0 1 0 0 1 0 1 1 0 0 0 0 0 1 0 1 1 1 1 1 1 0 1 1 1 0 1 1 1 1 1 0 0 0 0 0 0 1: 32 0:32 +
 64 8 0 12 4 -8 0 0 0 -4 -8 4 -4 -8 4 -8 -4 -20 -16 -4 -4 -12 -4 4 0 8 4 12 4 0 12 0 -8 0 12 0 4 12 4 8 0 4 -4 -12 -4 -4 -16 -20 -4 -8 4 -8 -4 4 -8 -4 0 0 0 -8 4 12 0 8
PFAKmin: 4 PFAKmax: -20 MO: -0.09375 |MO|: 0.71875 DISP: 0.9468776891689071 |DISP|: 0.61619541251429
0 0 1 0 0 0 0 0 0 1 0 1 0 1 1 1 0 1 1 1 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 0 1 1 0 1 1 0 1 1 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 1 0 1 0 0 1 1 0 1: 28 0:36
 64 8 0 4 4 -16 0 0 0 -4 8 -4 -4 -8 -4 0 -4 -4 16 4 -4 4 4 4 0 8 -4 4 4 0 -12 0 -8 0 -12 0 4 4 -4 8 0 4 4 4 -4 4 16 -4 -4 0 -4 -8 -4 -4 8 -4 0 0 0 -16 4 4 0 8
PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.5625 DISP: 0.7715167461315809 |DISP|: 0.5184469164912342
0 1 1 1 0 1 0 1 0 1 1 1 1 1 1 0 1 1 1 0 1 0 1 1 0 1 0 1 1 0 1 0 0 1 0 1 0 0 1 1 1 0 0 0 1 1 0 0 0 1 0 0 0 1 0 0 1 1 1 1 0 0 1 1 1: 36 0:28
 64 -8 0 -4 4 16 0 0 0 4 8 4 -4 8 -4 0 -4 4 16 -4 -4 -4 4 -4 0 -8 -4 -4 4 0 -12 0 -8 0 -12 0 4 -4 -4 -8 0 -4 4 -4 -4 -4 16 4 -4 0 -4 8 -4 4 8 4 0 0 0 16 4 -4 0 -8
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.5625 DISP: 0.7715167461315809 |DISP|: 0.5184469164912342
0 0 0 1 1 1 0 0 1 1 1 0 1 0 0 0 1 0 0 0 0 0 1 0 1 1 0 0 1 1 0 0 0 0 1 1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 1 0 1 1 0 1 0 1 1 0 0 1 0 1 1: 28 0:36
 64 -4 -4 -8 -4 -4 12 -4 0 0 -4 0 4 -4 0 4 -4 8 -4 16 -4 0 0 0 0 4 0 -8 4 -4 8 4 -8 4 8 -4 4 -8 0 4 0 0 0 0 -4 16 -4 8 -4 4 0 -4 4 0 -4 0 0 -4 12 -4 -4 -8 -4 -4
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.5 DISP: 0.6842908520111746 |DISP|: 0.45860381887062823
0 1 0 0 1 0 0 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 1 1 1 0 0 1 1 0 0 1 0 1 1 0 1 1 1 1 0 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 0 0 1 1 0 0 0 0 1: 36 0:28
 64 4 -4 8 -4 4 12 4 0 0 -4 0 4 4 0 -4 -4 -8 -4 -16 -4 0 0 0 0 -4 0 8 4 4 8 -4 -8 -4 8 4 4 8 0 -4 0 0 0 0 -4 -16 -4 -8 -4 -4 0 4 4 0 -4 0 0 4 12 4 -4 8 -4 4
PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.5 DISP: 0.6842908520111746 |DISP|: 0.45860381887062823

0 0 1 0 1 1 1 1 1 1 0 1 1 0 1 1 1 0 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 0 0 0 1 0 0 1 0 0 1 0 1 0 0 1 0 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0 1: 36 0:28
64 4 4 8 -4 4 -12 4 0 0 4 0 4 -4 0 4 -4 8 4 0 -4 8 0 0 0 -4 0 -8 4 -4 -8 -4 -8 -4 -8 -4 4 -8 0 -4 0 0 0 8 -4 0 4 8 -4 4 0 -4 4 0 4 0 0 4 -12 4 -4 8 4 4
PFAKmin: 4 PFAKmax: -12 MO: -0.09375 |MO|: 0.46875
DISP: 0.6107502604049521 |DISP|: 0.38250994890650725
0 1 1 1 1 0 1 0 1 0 0 0 1 1 1 0 1 1 1 0 0 1 0 0 1 0 1 0 1 0 1 0 0 1 0 1 1 1 0 0 0 1 1 1 1 1 0 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1 1: 32 0:32 +
64 -4 4 -8 -4 -4 -12 -4 0 0 4 0 4 4 0 -4 -4 -8 4 0 -4 -8 0 0 0 4 0 8 4 4 -8 4 -8 4 -8 4 4 8 0 4 0 0 0 -8 -4 0 4 -8 -4 -4 0 4 4 0 4 0 0 -4 -12 -4 -4 -8 4 -4
PFAKmin: -4 PFAKmax: -12 MO: -0.09375 |MO|: 0.46875
DISP: 0.5974067715810526 |DISP|: 0.38250994890650725
0 0 0 1 0 0 1 1 1 1 1 0 0 1 1 1 1 0 0 0 1 1 0 1 1 1 0 0 0 0 1 1 0 0 1 1 0 1 0 1 0 0 0 1 0 1 0 1 0 0 1 0 0 0 1 0 0 1 1 0 1 0 1 0 1 0 0: 30 0:34
64 -4 -4 -8 4 -4 -4 4 0 -8 12 0 -4 4 0 12 -4 8 -12 -8 4 -8 0 8 0 -4 -8 16 -4 -4 0 -4 -8 -4 0 -4 -4 16 -8 -4 0 8 0 -8 4 -8 -12 8 -4 12 0 4 -4 0 12 -8 0 4 -4 -4 4 -8 -4 -4
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.65625
DISP: 0.8254744740334078 |DISP|: 0.4961252427805765
0 1 0 0 0 1 1 0 1 0 1 1 0 0 1 0 1 1 0 1 1 0 0 0 1 0 0 1 0 1 1 0 0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 0 0 1 1 1 1 1 1: 30 0:34
64 4 -4 8 4 4 -4 -4 0 8 12 0 -4 -4 0 -12 -4 -8 -12 8 4 8 0 -8 0 4 -8 -16 -4 4 0 4 -8 4 0 4 -4 -16 -8 4 0 -8 0 8 4 8 -12 -8 -4 -12 0 -4 -4 0 12 8 0 -4 -4 4 4 8 -4 4
PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.65625
DISP: 0.8254744740334078 |DISP|: 0.4961252427805765
0 0 1 0 0 0 0 0 1 1 0 1 0 1 0 0 1 0 1 1 1 1 1 0 1 1 1 1 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 1 0 0 1 1 0 0 0 0 1 0 0 0 1 0 1 0 1 1 0 0 1 1: 26 0:38
64 4 4 8 4 4 4 -4 0 8 -12 0 -4 4 0 -4 -4 8 12 -8 4 0 0 -8 0 4 8 0 -4 12 0 4 -8 4 0 12 -4 0 8 4 0 -8 0 0 4 -8 12 8 -4 -4 0 4 -4 0 -12 8 0 -4 4 4 4 8 4 4
PFAKmin: 4 PFAKmax: -12 MO: -0.09375 |MO|: 0.5625
DISP: 0.7117281279799236 |DISP|: 0.45309507336940574
0 1 1 1 0 1 0 1 1 0 0 0 0 0 0 1 1 1 1 0 1 0 1 1 1 0 1 0 0 1 0 1 0 1 0 1 0 0 1 1 0 1 1 1 0 0 1 1 0 1 0 0 0 1 0 0 0 0 0 0 1 1 0 0 1: 30 0:34
64 -4 4 -8 4 -4 4 4 0 -8 -12 0 -4 -4 0 4 -4 -8 12 8 4 0 0 8 0 -4 8 0 -4 -12 0 -4 -8 -4 0 -12 -4 0 8 -4 0 8 0 0 4 8 12 -8 -4 4 0 -4 -4 0 -12 -8 0 4 4 -4 4 -8 4 -4
PFAKmin: -4 PFAKmax: -12 MO: -0.09375 |MO|: 0.5625
DISP: 0.7229647003911237 |DISP|: 0.45309507336940574
0 0 0 1 1 1 0 0 0 0 0 1 0 1 1 1 0 1 1 1 1 1 0 1 1 1 0 0 1 1 0 0 0 0 1 1 1 0 1 0 1 1 1 0 0 1 0 1 1 1 0 1 0 0 1 0 0 1 1 0 0 1 0 1 1: 34 0:30

64 0 -4 -8 4 -8 16 4 -16 0 8 -4 -4 -4 0 -8 4 -4 -4 -8 12 12 -4 0 0 -4 -4 4 -4 -4 8 0 -8 0 8 -4 -4 4 -4 -4 0 0 -4 12 12 -8 -4 -4 4 -8 0 -4 -4 -4 8 0 -16 4 16 -8 4 -8 -4 0
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.65625
DISP: 0.8444845393105501 |DISP|: 0.5271491928066907
0 1 0 0 1 0 0 1 0 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 1 0 1 1 0 1 1 1 1 1 0 1 1 0 0 0 0 1 0 0 0 0 1 1 1 0 0 1 1 0 0 0 0 1: 26 0:38

64 0 -4 8 4 8 16 -4 -16 0 8 4 -4 4 0 8 4 4 -4 8 12 -12 -4 0 0 4 -4 -4 -4 4 8 0 -8 0 8 4 -4 -4 -4 4 0 0 -4 -12 12 8 -4 4 4 8 0 4 -4 4 8 0 -16 -4 16 8 4 8 -4 0
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.65625
DISP: 0.8348850862727943 |DISP|: 0.5271491928066907
0 0 1 0 1 1 1 1 0 0 1 0 0 1 0 0 0 1 0 0 1 1 1 0 1 1 1 1 1 1 1 1 0 0 0 0 1 0 0 1 1 1 0 1 0 1 1 0 1 1 1 0 0 0 0 1 0 1 0 1 0 1 1 0 1: 34 0:30

64 0 4 0 4 0 -16 4 -16 8 -8 -4 -4 -12 0 0 4 -12 4 16 12 4 4 8 0 -4 4 -12 -4 4 -8 0 -8 0 -8 4 -4 -12 4 -4 0 8 4 4 12 16 4 -12 4 0 0 -12 -4 -4 -8 8 -16 4 -16 0 4 0 4 0
PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.71875
DISP: 0.9505947171415781 |DISP|: 0.61619541251429
0 1 1 1 1 0 1 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 1 1 1 0 1 0 1 0 1 0 0 1 0 1 1 1 0 0 1 0 0 0 0 0 1 1 1 0 1 1 0 1 0 0 0 0 0 0 0 0 1 1 1: 30 0:34

64 0 4 0 4 0 -16 -4 -16 -8 -8 4 -4 12 0 0 4 12 4 -16 12 -4 4 -8 0 4 4 12 -4 -4 -8 0 -8 0 -8 -4 -4 12 4 4 0 -8 4 -4 12 -16 4 12 4 0 0 12 -4 4 -8 -8 -16 -4 -16 0 4 0 4 0
PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.71875
DISP: 0.9505947171415781 |DISP|: 0.61619541251429
0 0 0 1 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 1 0 0 1 0 1 1 0 0 0 0 1 1 0 0 1 1 0 1 0 1 1 1 1 0 1 0 1 0 1 1 0 1 1 1 0 1 0 1 1 0 1 1 1 0 1 0 1 1 0 1 0 1 0 1: 32 0:32

64 -8 -4 -8 -4 16 0 12 -16 8 -8 4 4 4 0 -8 4 -12 20 0 -12 -4 -4 8 0 -12 -12 4 4 -4 0 0 -8 0 0 -4 4 4 -12 -12 0 8 -4 -4 -12 0 20 -12 4 -8 0 4 4 4 -8 8 -16 12 0 16 -4 -8 -4 -8
PFAKmin: -4 PFAKmax: 20 MO: -0.09375 |MO|: 0.8125
DISP: 1.0426185963087242 |DISP|: 0.64966224001118
0 1 0 0 0 1 1 0 0 1 0 0 1 1 0 1 0 0 1 0 0 1 1 1 1 0 0 1 0 1 1 0 0 1 1 0 0 0 0 0 1 0 1 1 1 1 1 1 1 0 0 0 1 0 0 0 0 0 1 1 1 1 1 1 1: 32 0:32

64 8 -4 8 -4 -16 0 -12 -16 -8 -8 -4 4 -4 0 8 4 12 20 0 -12 4 -4 -8 0 12 -12 -4 4 4 0 0 -8 0 0 4 4 -4 -12 12 0 -8 -4 4 -12 0 20 12 4 8 0 -4 4 -4 -8 -8 -16 -12 0 -16 -4 8 -4 8
PFAKmin: -4 PFAKmax: 20 MO: -0.09375 |MO|: 0.8125
DISP: 1.0426185963087242 |DISP|: 0.64966224001118
0 0 1 0 0 0 0 0 0 0 1 0 1 0 1 1 0 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1 0 1 1 0 0 1 1 1 1 0 1 1 1 0 0 1 0 1 1 0 0 1: 28 0:36

64 8 4 16 -4 -8 0 -4 -16 0 8 4 4 12 0 0 4 -4 -20 -8 -12 -12 4 0 0 4 12 4 4 4 0 0 -8 0 0 4 4 4 12 4 0 0 4 -12 -12 -8 -20 -4 4 0 0 12 4 4 8 0 -16 -4 0 -8 -4 16 4 8
PFAKmin: 4 PFAKmax: -20 MO: -0.09375 |MO|: 0.71875
DISP: 0.988023505695746 |DISP|: 0.6657243242616421
0 1 1 1 0 1 0 1 0 1 1 1 1 1 1 0 0 0 0 1 0 1 0 0 1 0 1 0 1 0 1 0 0 1 1 1 0 0 0 1 1 0 0 1 0 1 1 1 0 1 1 0 0 0 0 1 1 0 0 1:32 0:32 +
64 -8 4 -16 -4 8 0 4 -16 0 8 -4 4 -12 0 0 4 4 -20 8 -12 12 4 0 0 -4 12 -4 4 -4 0 0 -8 0 0 -4 4 -4 12 -4 0 0 4 12 -12 8 -20 4 4 0 0 -12 4 -4 8 0 -16 4 0 8 -4 -16 4 -8
PFAKmin: 4 PFAKmax: -20 MO: -0.09375 |MO|: 0.71875
DISP: 0.9798313211739514 |DISP|: 0.6657243242616421
0 0 0 1 1 1 0 0 1 1 1 0 1 0 0 0 0 1 1 1 1 1 0 1 0 0 1 1 0 0 1 1 0 0 1 1 1 0 1 0 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1:32 0:32 +
64 -4 -8 -4 -12 4 -12 -8 16 -4 -4 0 -4 16 4 -4 4 0 8 -12 -12 -8 0 4 0 16 8 -8 4 -8 -4 4 -8 4 -4 -8 4 -8 8 16 0 4 0 -8 -12 -12 8 0 4 -4 4 16 -4 0 -4 -4 16 -8 -12 4 -12 -4 -8 -4
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.8125
DISP: 0.9958993160994298 |DISP|: 0.5716842718953874
0 1 0 0 1 0 0 1 1 0 1 1 1 1 0 1 0 0 1 0 1 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 1 1 0 1 0 0 1 1 1 1 1 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 1:36 0:28
64 4 -8 4 -12 -4 -12 8 16 4 -4 0 -4 -16 4 4 4 0 8 12 -12 8 0 -4 0 -16 8 8 4 8 -4 -4 -8 -4 -4 8 4 8 8 -16 0 -4 0 8 -12 12 8 0 4 4 4 -16 -4 0 -4 4 16 8 -12 -4 -12 4 -8 4
PFAKmin: 4 PFAKmax: 16 MO: -0.09375 |MO|: 0.8125
DISP: 1.0039603964605042 |DISP|: 0.5716842718953874
0 0 1 0 1 1 1 1 1 1 0 1 1 0 1 1 0 1 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 1 0 0 1 0 1 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 1:28 0:36
64 4 8 20 -12 12 12 0 16 -4 4 0 -4 8 -4 -4 4 -16 -8 -4 -12 0 0 -12 0 -8 -8 8 4 0 4 -4 -8 -4 4 0 4 8 -8 -8 0 -12 0 0 -12 -4 -8 -16 4 -4 -4 8 -4 0 4 -4 16 0 12 12 -12 20 8 4
PFAKmin: 4 PFAKmax: 20 MO: -0.09375 |MO|: 0.8125
DISP: 1.0503211733667923 |DISP|: 0.64966224001118
0 1 1 1 1 0 1 0 1 0 0 0 1 1 1 0 0 0 0 1 1 0 1 1 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 0 1 1 1 1 1 0 0 1 0 1 1 0 1 0 0 1 1 1 1 1 1 0 0 1:36 0:28
64 -4 8 -20 -12 -12 12 0 16 4 4 0 -4 -8 -4 4 4 16 -8 4 -12 0 0 12 0 8 -8 -8 4 0 4 4 -8 4 4 0 4 -8 -8 8 0 12 0 0 -12 4 -8 16 4 4 -4 -8 -4 0 4 4 16 0 12 -12 -12 -20 8 -4
PFAKmin: -4 PFAKmax: -20 MO: -0.09375 |MO|: 0.8125
DISP: 1.0503211733667923 |DISP|: 0.64966224001118
0 0 0 1 0 0 1 1 1 1 1 0 0 1 1 1 0 1 1 1 0 0 1 0 0 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 0 1 0 1 0 1 1 1 0 1 1 1 0 1 1 0 0 1 0 1 0 1:34 0:30

64 -4 0 -12 12 -12 -4 -8 16 -4 4 0 4 -16 -4 -12 4 -16 8 4 12 0 8 -12 0 0 8 0 -4 0 12 -4 -8 -4 12 0 -4 0 8 0 0 -12 8 0 12 4 8 -16 4 -12 -4 -16 4 0 4 -4 16 -8 -4 -12 12 -12 0 -4

PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.8125 DISP: 1.0459954851647526 |DISP|: 0.64966224001118

0 1 0 0 0 1 1 0 1 0 1 1 0 0 1 0 0 0 1 0 0 1 1 1 0 1 1 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 1 0 0 0 0 0 0 1: 22 0:42

64 4 0 12 12 12 -4 8 16 4 4 0 4 16 -4 12 4 16 8 -4 12 0 8 12 0 0 8 0 -4 0 12 4 -8 4 12 0 -4 0 8 0 0 12 8 0 12 -4 8 16 4 12 -4 16 4 0 4 4 16 8 -4 12 12 12 0 4

PFAKmin: 4 PFAKmax: 16 MO: -0.09375 |MO|: 0.8125 DISP: 0.8116887884695957 |DISP|: 0.64966224001118

0 0 1 0 0 0 0 0 1 1 0 1 0 1 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 1 1 1 0 0 0 0 0 1 1 0 0 0 1 0 0 1 1 0 1 1 1 0 1 1 1 0 1 0 1 0 0 1 1 0 1: 26 0:38

64 4 0 -4 12 -4 4 0 16 -4 -4 0 4 -8 4 4 4 0 -8 12 12 8 -8 4 0 8 -8 0 -4 8 -12 4 -8 4 -12 8 -4 0 -8 8 0 4 -8 8 12 12 -8 0 4 4 4 -8 4 0 -4 -4 16 0 4 -4 12 -4 0 4

PFAKmin: 4 PFAKmax: 16 MO: -0.09375 |MO|: 0.6875 DISP: 0.8536856196133047 |DISP|: 0.5160494704484879

0 1 1 1 0 1 0 1 1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 1 1 0 0 1 1 1 0 1 1 1 0 1 1 1 1 1 1 0 0 1 1 1: 34 0:30

64 -4 0 4 12 4 4 0 16 4 -4 0 4 8 4 -4 4 0 -8 -12 12 -8 -8 -4 0 -8 -8 0 -4 -8 -12 -4 -8 -4 -12 -8 -4 0 -8 -8 0 -4 -8 -8 12 -12 -8 0 4 -4 4 8 4 0 -4 4 16 0 4 4 12 4 0 -4

PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.6875 DISP: 0.8630759914331836 |DISP|: 0.5160494704484879

0 0 0 1 1 1 0 0 0 0 0 1 0 1 1 1 1 0 0 0 0 0 1 0 0 0 1 1 0 0 1 1 1 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 0 1 0 1 1: 28 0:36

64 0 -4 -8 -8 0 4 -4 -12 -4 4 12 8 -8 -4 0 -4 20 8 4 -8 4 0 -4 4 -12 0 -4 8 4 0 0 8 0 0 4 8 -4 0 -12 4 -4 0 4 -8 4 8 20 -4 0 -4 -8 8 12 4 -4 -12 -4 4 0 -8 -8 -4 0

PFAKmin: -4 PFAKmax: 20 MO: -0.09375 |MO|: 0.65625 DISP: 0.8683134450361611 |DISP|: 0.5564461619356259

0 1 0 0 1 0 0 1 0 1 0 0 0 0 1 0 1 1 0 1 0 1 1 1 0 1 1 0 0 1 1 0 1 0 0 1 0 0 0 0 0 1 0 0 1 1 1 1 1 0 0 0 0 1 1 1 0 0 1 1 0 0 0 0 1: 28 0:36

64 0 -4 8 -8 0 4 4 -12 4 4 -12 8 8 -4 0 -4 -20 8 -4 -8 -4 0 4 4 12 0 4 8 -4 0 0 8 0 0 -4 8 4 0 12 4 4 0 -4 -8 -4 8 -20 -4 0 -4 8 8 -12 4 4 -12 4 4 0 -8 8 -4 0

PFAKmin: -4 PFAKmax: -20 MO: -0.09375 |MO|: 0.65625 DISP: 0.8683134450361611 |DISP|: 0.5564461619356259

0 0 1 0 1 1 1 1 0 0 1 0 0 1 0 0 1 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0 0 1 1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 1 1 1 0 0 0 0 1 0 1 0 1 0 1 1 0 1: 28 0:36

64 0 4 0 -8 0 -4 -4 -12 4 -4 4 8 8 4 8 -4 -4 -8 4 -8 4 0 -12 4 4 0 4 8 -4 0 0 8 0 0 -4 8 4 0 4 4 -12 0 4 -8 4 -8 -4 -4 8 4 8 8 4 -4 4 -12 -4 -4 0 -8 0 4 0

PFAKmin: 4 PFAKmax: -12 MO: -0.09375 |MO|: 0.5625 DISP: 0.7071067811865476 |DISP|: 0.4165922475954698
0 1 1 1 1 0 1 0 0 1 1 1 0 0 0 1 1 1 1 0 0 1 0 0 0 1 0 1 0 1 0 1 1 0 1 0 0 0 1 1 0 1 1 1 1 1 0 0 1 0 1 1 0 1 0 0 0 0 0 0 0 0 0 1 1 1: 32 0:32 +
64 0 4 0 -8 0 -4 4 -12 -4 -4 -4 8 -8 4 -8 -4 4 -8 -4 -8 -4 0 12 4 -4 0 -4 8 4 0 0 8 0 0 4 8 -4 0 -4 4 12 0 -4 -8 -4 -8 4 -4 -8 4 -8 8 -4 -4 -4 -12 4 -4 0 -8 0 4 0 PFAKmin: 4 PFAKmax: -12 MO: -0.09375 |MO|: 0.5625 DISP: 0.6956140957069367 |DISP|: 0.4165922475954698
0 0 0 1 0 0 1 1 0 0 0 1 1 0 0 0 1 0 0 0 1 1 0 1 0 0 1 1 1 1 0 0 1 1 0 0 1 0 1 0 0 0 0 1 0 1 0 1 1 1 0 1 1 1 0 1 0 1 0 1 1 0 1 0 1 0 1: 30 0:34
64 -8 -4 -8 8 16 -4 -4 -12 12 4 -12 -8 0 -12 8 -4 4 -8 -4 8 -12 16 -4 4 4 0 4 -8 4 -8 0 8 0 -8 4 -8 4 0 4 4 -4 16 -12 8 -4 -8 4 -4 8 -12 0 -8 -12 4 12 -12 -4 -4 16 8 -8 -4 -8 PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.84375 DISP: 0.9994340427556684 |DISP|: 0.522897698209084
0 1 0 0 0 1 1 0 0 1 0 0 1 1 0 1 1 1 0 1 1 0 0 0 0 1 1 0 1 0 0 1 1 0 0 1 1 1 1 1 1 0 1 0 0 0 0 0 0 1 0 0 0 1 0 0 0 0 0 0 1 1 1 1 1 1 1: 30 0:34
64 8 -4 8 8 -16 -4 4 -12 -12 4 12 -8 0 -12 -8 -4 -4 -8 4 8 12 16 4 4 -4 0 -4 -8 -4 -8 0 8 0 -8 -4 -8 -4 0 -4 4 4 16 12 8 4 -8 -4 -4 -8 -12 0 -8 12 4 -12 -12 4 -4 -16 8 8 -4 8 PFAKmin: -4 PFAKmax: -16 MO: -0.09375 |MO|: 0.84375 DISP: 0.9994340427556684 |DISP|: 0.522897698209084
0 0 1 0 0 0 0 0 0 0 1 0 1 0 1 1 1 0 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 1 1 1 0 0 1 0 0 1 0 0 1 1 0 1 1 1 0 1 1 1 0 0 1 0 1 1 0 0 1 1: 34 0:30
64 8 4 16 8 -16 4 -4 -12 -12 -4 -4 -8 0 12 0 -4 12 8 -4 8 4 -16 -12 4 -12 0 -4 -8 -4 8 0 8 0 8 -4 -8 -4 0 -12 4 -12 -16 4 8 -4 8 12 -4 0 12 0 -8 -4 -4 -12 -12 -4 4 -16 8 16 4 8
PFAKmin: 4 PFAKmax: 16 MO: -0.09375 |MO|: 0.875 DISP: 1.0610620080084232 |DISP|: 0.5873585571306099
0 1 1 1 0 1 0 1 0 1 1 1 1 1 1 0 1 1 1 0 1 0 1 1 0 1 0 1 1 0 1 0 1 0 1 0 1 1 0 0 0 1 1 1 0 0 1 1 1 0 1 1 1 0 1 1 0 0 0 0 1 1 0 0 1: 38 0:26
64 -8 4 -16 8 16 4 4 -12 12 -4 4 -8 0 12 0 -4 -12 8 4 8 -4 -16 12 4 12 0 4 -8 4 8 0 8 0 8 4 -8 4 0 12 4 12 -16 -4 8 4 8 -12 -4 0 12 0 -8 4 -4 12 -12 4 4 16 8 -16 4 -8 PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.875 DISP: 1.0534379692155804 |DISP|: 0.5873585571306099
0 0 0 1 1 1 0 0 1 1 1 0 1 0 0 0 1 0 0 0 0 0 1 0 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 1 1 1 1 0 0 1 0 1 1 1 0 1 0 0 1 0 1 0 0 1 1 0 1 0 1: 30 0:34
64 -4 -8 -4 0 -4 0 0 12 0 -16 -8 8 4 0 -4 -4 8 -4 0 16 0 -12 0 -4 0 -4 8 -8 8 -4 -4 8 -4 -4 8 -8 8 -4 0 -4 0 -12 0 16 0 -4 8 -4 -4 0 4 8 -8 -16 0 12 0 0 -4 0 -4 -8 -4 PFAKmin: -4 PFAKmax: -16 MO: -0.09375 |MO|: 0.625 DISP: 0.8444845393105501 |DISP|: 0.5649747187520014

0 1 0 0 1 0 0 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 1 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 0 0 1 0 1 1 0 0 0 0 1 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 1: 34 0:30

64 4 -8 4 0 4 0 0 12 0 -16 8 8 -4 0 4 -4 -8 -4 0 16 0 -12 0 -4 0 -4 -8 -8 -8 -4 4 8 4 -4 -8 -8 -8 -4 0 -4 0 -12 0 16 0 -4 -8 -4 4 0 -4 8 8 -16 0 12 0 0 4 0 4 -8 4

PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.625 DISP: 0.8444845393105501 |DISP|: 0.5649747187520014

0 0 1 0 1 1 1 1 1 1 0 1 1 0 1 1 1 0 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 0 1 0 1 1 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 1: 42 0:22

64 4 8 20 0 12 0 8 12 0 16 0 8 4 0 12 -4 8 4 0 16 0 12 16 -4 8 4 0 -8 0 4 4 8 4 4 0 -8 0 4 8 -4 16 12 0 16 0 4 8 -4 12 0 4 8 0 16 0 12 8 0 12 0 20 8 4

PFAKmin: 4 PFAKmax: 20 MO: -0.09375 |MO|: 0.78125 DISP: 0.8310142713462031 |DISP|: 0.7107691722756951

0 1 1 1 1 0 1 0 1 0 0 0 1 1 1 0 1 1 1 0 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 0 0 1 1 1 0 0 0 0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 1 1 1 0 0 1: 34 0:30

64 -4 8 -20 0 -12 0 -8 12 0 16 0 8 -4 0 -12 -4 -8 4 0 16 0 12 -16 -4 -8 4 0 -8 0 4 -4 8 -4 4 0 -8 0 4 -8 -4 -16 12 0 16 0 4 -8 -4 -12 0 -4 8 0 16 0 12 -8 0 -12 0 -20 8 -4

PFAKmin: -4 PFAKmax: -20 MO: -0.09375 |MO|: 0.78125 DISP: 1.0610620080084232 |DISP|: 0.7107691722756951

0 0 0 1 0 0 1 1 1 1 1 0 0 1 1 1 1 0 0 0 1 1 0 1 1 1 0 0 0 0 1 1 1 1 0 0 1 0 1 0 1 1 1 0 1 0 1 0 1 1 0 1 1 1 0 1 1 0 0 1 0 1 0 1 1: 36 0:28

64 -4 0 -12 0 -12 0 8 12 -8 8 8 -8 -12 -16 12 -4 16 4 0 -16 8 -4 8 -4 8 4 -8 8 0 -4 4 8 4 -4 0 8 -8 4 8 -4 8 -4 8 -16 0 4 16 -4 12 -16 -12 -8 8 8 -8 12 8 0 -12 0 -12 0 -4

PFAKmin: -4 PFAKmax: -16 MO: -0.09375 |MO|: 0.875 DISP: 1.0653265213428305 |DISP|: 0.5873585571306099

0 1 0 0 0 1 1 0 1 0 1 1 0 0 1 0 1 1 0 1 1 0 0 0 1 0 0 1 0 1 1 0 1 0 0 1 1 1 1 1 1 1 0 1 1 1 1 1 1 1 0 0 0 1 0 0 0 1 1 0 0 0 0 0 0 0 1: 32 0:32 +

64 4 0 12 0 12 0 -8 12 8 8 -8 -8 12 -16 -12 -4 -16 4 0 -16 -8 -4 -8 -4 -8 4 8 8 0 -4 -4 8 -4 -4 0 8 8 4 -8 -4 -8 -4 -8 -16 0 4 -16 -4 -12 -16 12 -8 -8 8 8 12 -8 0 12 0 12 0 4

PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.875 DISP: 1.0577332211964392 |DISP|: 0.5873585571306099

0 0 1 0 0 0 0 0 1 1 0 1 0 1 0 0 1 0 1 1 1 1 1 0 1 1 1 1 0 0 0 0 1 1 1 1 1 0 0 1 1 1 0 1 1 0 0 1 1 1 1 0 1 1 1 0 1 1 1 0 1 0 1 0 0 1 1 0 1: 36 0:28

64 4 0 -4 0 4 0 0 12 8 -8 0 -8 4 16 -4 -4 0 -4 0 -16 -8 4 8 -4 0 -4 0 8 -8 4 -4 8 -4 4 -8 8 0 -4 0 -4 8 4 -8 -16 0 -4 0 -4 -4 16 4 -8 0 -8 8 12 0 0 4 0 -4 0 4

PFAKmin: 4 PFAKmax: 16 MO: -0.09375 |MO|: 0.59375 DISP: 0.8116219250790999 |DISP|: 0.5431384637829754

0 1 1 1 0 1 0 1 1 0 0 0 0 0 0 1 1 1 1 0 1 0 1 1 1 0 1 0 0 1 0 1 1 0 1 0 1 1 0 0 1 0 0 0 1 1 0 0 1 0 1 1 1 0 1 1 1 1 1 1 0 0 1 1 1: 36 0:28

64 -4 0 4 0 -4 0 0 12 -8 -8 0 -8 -4 16 4 -4 0 -4 0 -16 8 4 -8 -4 0 -4 0 8 8 4 4 8 4 4 8 8 0 -4 0 -4 -8 4 8 -16 0 -4 0 -4 4 16 -4 -8 0 -8 -8 12 0 0 -4 0 4 0 -4
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.59375 DISP: 0.8116219250790999 |DISP|: 0.5431384637829754
0 0 0 1 1 1 0 0 0 0 0 1 0 1 1 1 0 1 1 1 1 1 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 0 0 1 0 1 1 0 1 1 0 0 1 1 0 1 0 1 0 1: 32 0:32 +
64 0 -8 -4 8 -8 4 8 -4 8 4 -12 -8 -4 0 0 4 -12 -4 0 -8 -12 0 8 -4 8 0 -4 0 8 -4 0 8 0 -4 8 0 -4 0 8 -4 8 0 -12 -8 0 -4 -12 4 0 0 -4 -8 -12 4 8 -4 8 4 -8 8 -4 -8 0
PFAKmin: -4 PFAKmax: -12 MO: -0.09375 |MO|: 0.625 DISP: 0.7815773087554823 |DISP|: 0.4732423569021264
0 1 0 0 1 0 0 1 0 1 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 1 1 0 0 1 0 0 0 0 0 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 1 1: 28 0:36
64 0 -8 4 8 8 4 -8 -4 -8 4 12 -8 4 0 0 4 12 -4 0 -8 12 0 -8 -4 -8 0 4 0 -8 -4 0 8 0 -4 -8 0 4 0 -8 -4 -8 0 12 -8 0 -4 12 4 0 0 4 -8 12 4 -8 -4 -8 4 8 8 4 -8 0
PFAKmin: 4 PFAKmax: 12 MO: -0.09375 |MO|: 0.625 DISP: 0.7918232879975703 |DISP|: 0.4732423569021264
0 0 1 0 1 1 1 1 0 0 1 0 0 1 0 0 0 1 0 0 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 0 1 1 0 0 0 1 0 1 0 0 1 0 0 0 1 1 1 1 0 1 0 1 0 1 0 0 1 1: 36 0:28
64 0 8 12 8 8 -4 8 -4 0 -4 -4 -8 -12 0 -8 4 -4 4 -8 -8 4 0 0 -4 8 0 4 0 -8 4 0 8 0 4 -8 0 4 0 8 -4 0 0 4 -8 -8 4 -4 4 -8 0 -12 -8 -4 -4 0 -4 8 -4 8 8 12 8 0
PFAKmin: -4 PFAKmax: 12 MO: -0.09375 |MO|: 0.59375 DISP: 0.7506610817856761 |DISP|: 0.4469466258714868
0 1 1 1 1 0 1 0 0 1 1 1 0 0 0 1 0 0 0 1 1 0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0 0 1 1 0 1 1 1 1 1 0 0 1 0 0 1 0 1 1 1 1 1 1 1 0 0 1: 36 0:28
64 0 8 -12 8 -8 -4 -8 -4 0 -4 4 -8 12 0 8 4 4 4 8 -8 -4 0 0 -4 -8 0 -4 0 8 4 0 8 0 4 8 0 -4 0 -8 -4 0 0 -4 -8 8 4 4 4 8 0 12 -8 4 -4 0 -4 -8 -4 -8 8 -12 8 0
PFAKmin: -4 PFAKmax: -12 MO: -0.09375 |MO|: 0.59375 DISP: 0.7506610817856761 |DISP|: 0.4469466258714868
0 0 0 1 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 1 0 0 1 0 1 1 0 0 0 0 1 1 1 1 0 0 1 0 1 0 0 0 0 1 0 1 0 1 0 0 1 0 0 0 1 0 1 0 0 1 0 1 0 1 1: 26 0:38
64 -8 0 -12 -8 8 4 16 -4 0 -20 12 8 12 16 -8 4 -12 4 0 8 4 -8 0 -4 16 8 4 0 0 -4 0 8 0 -4 0 0 4 8 16 -4 0 -8 4 8 0 4 -12 4 -8 16 12 8 12 -20 0 -4 16 4 8 -8 -12 0 -8
PFAKmin: 4 PFAKmax: -20 MO: -0.09375 |MO|: 0.84375 DISP: 1.0831544740676133 |DISP|: 0.6811007134890428
0 1 0 0 0 1 1 0 0 1 0 0 1 1 0 1 0 0 1 0 0 1 1 1 1 0 0 1 0 1 1 0 1 0 0 1 1 1 1 1 0 1 0 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 1 0 0 0 0 0 0 0 1: 30 0:34
64 8 0 12 -8 -8 4 -16 -4 0 -20 -12 8 -12 16 8 4 12 4 0 8 -4 -8 0 -4 -16 8 -4 0 0 -4 0 8 0 -4 0 0 -4 8 -16 -4 0 -8 -4 8 0 4 12 4 8 16 -12 8 -12 -20 0 -4 -16 4 -8 -8 12 0 8

PFAKmin: 4 PFAKmax: -20 MO: -0.09375 |MO|: 0.84375
DISP: 1.0905707884160976 |DISP|: 0.6811007134890428
0 0 1 0 0 0 0 0 0 0 1 0 1 0 1 1 0 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 1 1 1 0 0 1 0 0 1 0
0 1 1 0 0 0 0 1 0 0 0 1 1 0 1 0 0 1 1 0 1: 26 0:38
64 8 0 4 -8 -8 -4 0 -4 8 20 4 8 4 -16 0 4 -4 -4 8 8 4 8 8 -4 0 -8 -4 0 0 4 0 8 0 4 0 0
-4 -8 0 -4 8 8 4 8 8 -4 -4 4 0 -16 4 8 4 20 8 -4 0 -4 -8 -8 4 0 8
PFAKmin: 4 PFAKmax: 20 MO: -0.09375 |MO|: 0.65625
DISP: 0.8536856196133047 |DISP|: 0.5564461619356259
0 1 1 1 0 1 0 1 0 1 1 1 1 1 1 0 0 0 0 1 0 1 0 0 1 0 1 0 0 1 0 1 1 0 1 0 1 1 0 0 0 1 1 1
0 0 1 1 0 1 0 0 0 1 0 0 1 1 1 1 0 0 1 1 1: 34 0:30
64 -8 0 -4 -8 8 -4 0 -4 -8 20 -4 8 -4 -16 0 4 4 -4 -8 8 -4 8 -8 -4 0 -8 4 0 0 4 0 8 0 4
0 0 4 -8 0 -4 -8 8 -4 8 -8 -4 4 4 0 -16 -4 8 -4 20 -8 -4 0 -4 8 -8 -4 0 -8
PFAKmin: -4 PFAKmax: 20 MO: -0.09375 |MO|: 0.65625
DISP: 0.8630759914331836 |DISP|: 0.5564461619356259
0 0 0 1 1 1 0 0 1 1 1 0 1 0 0 0 0 1 1 1 1 1 0 1 0 0 1 1 0 0 1 1 1 1 0 0 0 1 0 1 1 1 1 0
0 1 0 1 0 0 1 0 1 1 0 1 0 1 1 0 0 1 0 1: 34 0:30
64 -4 -4 -8 -16 4 0 -12 4 -4 8 8 -8 8 4 4 4 -16 0 -4 0 8 12 -4 4 -20 -4 8 0 4 0 -4 8 -
4 0 4 0 8 -4 -20 4 -4 12 8 0 -4 0 -16 4 4 4 8 -8 8 8 -4 4 -12 0 4 -16 -8 -4 -4
PFAKmin: -4 PFAKmax: -20 MO: -0.09375 |MO|: 0.75 DISP:
0.9671485646534858 |DISP|: 0.6033964811080853
0 1 0 0 1 0 0 1 1 0 1 1 1 1 0 1 0 0 1 0 1 0 0 0 0 1 1 0 0 1 1 0 1 0 0 1 0 0 0 0 1 0 1 1
0 0 0 0 0 1 1 1 1 0 0 0 0 0 1 1 0 0 0 0: 26 0:38
64 4 -4 8 -16 -4 0 12 4 4 8 -8 -8 -8 4 -4 4 16 0 4 0 -8 12 4 4 20 -4 -8 0 -4 0 4 8 4 0
-4 0 -8 -4 20 4 4 12 -8 0 4 0 16 4 -4 4 -8 -8 -8 8 4 4 12 0 -4 -16 8 -4 4
PFAKmin: 4 PFAKmax: 20 MO: -0.09375 |MO|: 0.75 DISP:
0.9587780328404885 |DISP|: 0.6033964811080853
0 0 1 0 1 1 1 1 1 1 0 1 1 0 1 1 0 1 0 0 1 1 1 0 0 0 0 0 0 0 0 0 0 1 1 1 1 0 1 1 0 1 1 0 1
0 1 1 0 0 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0: 34 0:30
64 4 4 8 -16 4 0 -4 4 -4 -8 0 -8 0 -4 -12 4 0 0 4 0 -8 -12 -4 4 4 4 0 0 4 0 4 8 4 0 4 0
0 4 4 4 -4 -12 -8 0 4 0 0 4 -12 -4 0 -8 0 -8 -4 4 -4 0 4 -16 8 4 4
PFAKmin: 4 PFAKmax: -16 MO: -0.09375 |MO|: 0.53125
DISP: 0.7229647003911237 |DISP|: 0.4904690518944897
0 1 1 1 1 0 1 0 1 0 0 0 1 1 1 0 0 0 0 1 1 0 1 1 0 1 0 1 0 1 0 1 1 0 1 0 0 0 1 1 1 0 0 0
0 0 1 1 0 1 0 0 1 0 1 1 0 0 0 0 0 0 1 1: 30 0:34
64 -4 4 -8 -16 -4 0 4 4 4 -8 0 -8 0 -4 12 4 0 0 -4 0 8 -12 4 4 -4 4 0 0 -4 0 -4 8 -4 0
-4 0 0 4 -4 4 4 -12 8 0 -4 0 0 4 12 -4 0 -8 0 -8 4 4 4 0 -4 -16 -8 4 -4
PFAKmin: -4 PFAKmax: -16 MO: -0.09375 |MO|: 0.53125
DISP: 0.7229647003911237 |DISP|: 0.4904690518944897

0 0 0 1 0 0 1 1 1 1 1 0 0 1 1 1 0 1 1 1 0 0 1 0 0 0 1 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1 1 0 1 0 1 0 0 0 1 0 0 0 1 0 0 1 1 0 1 0 1 0 1: 32 0:32 +
64 -4 -4 -8 16 -4 -8 -12 4 -4 8 -8 8 0 12 -12 4 -8 0 4 0 0 -4 -4 4 -4 -4 -8 0 4 -8 4 8 4 -8 4 0 -8 -4 -4 4 -4 -4 0 0 4 0 -8 4 -12 12 0 8 -8 8 -4 4 -12 -8 -4 16 -8 -4 -4
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.6875
DISP: 0.8402982679518772 |DISP|: 0.4843149917101295
0 1 0 0 0 1 1 0 1 0 1 1 0 0 1 0 0 0 1 0 0 1 1 1 0 1 1 0 1 0 0 1 1 0 0 1 1 1 1 1 1 0 1 1 1 1 1 1 0 1 1 1 0 1 1 1 0 0 1 1 1 1 1 1 1: 40 0:24
64 4 -4 8 16 4 -8 12 4 4 8 8 8 0 12 12 4 8 0 -4 0 0 -4 4 4 4 -4 8 0 -4 -8 -4 8 -4 -8 -4 0 8 -4 4 4 4 -4 0 0 -4 0 8 4 12 12 0 8 8 8 4 4 12 -8 4 16 8 -4 4
PFAKmin: 4 PFAKmax: 16 MO: -0.09375 |MO|: 0.6875
DISP: 0.7596926617339136 |DISP|: 0.4843149917101295
0 0 1 0 0 0 0 0 1 1 0 1 0 1 0 0 0 1 0 0 0 0 0 1 0 0 0 0 1 1 1 1 1 1 1 1 1 0 0 1 1 1 0 1 1 0 0 1 0 0 0 1 0 0 0 1 0 1 0 1 1 0 0 1 1: 28 0:36
64 4 4 8 16 -4 8 -4 4 -4 -8 0 8 -8 -12 4 4 -8 0 -4 0 0 4 -4 4 -12 4 0 0 -12 8 -4 8 -4 8 -12 0 0 4 -12 4 -4 4 0 0 -4 0 -8 4 4 -12 -8 8 0 -8 -4 4 -4 8 -4 16 8 4 4
PFAKmin: 4 PFAKmax: 16 MO: -0.09375 |MO|: 0.65625
DISP: 0.8309489630073106 |DISP|: 0.4961252427805765
0 1 1 1 0 1 0 1 1 0 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 1 1 0 1 0 1 0 1 0 1 1 0 0 1 0 0 0 1 1 0 0 0 1 0 0 0 1 0 0 0 0 0 0 1 1 0 0 1: 24 0:40
64 -4 4 -8 16 4 8 4 4 4 -8 0 8 8 -12 -4 4 8 0 4 0 0 4 4 4 12 4 0 0 12 8 4 8 4 8 12 0 0 4 12 4 4 4 0 0 4 0 8 4 -4 -12 8 8 0 -8 4 4 4 8 4 16 -8 4 -4
PFAKmin: -4 PFAKmax: 16 MO: -0.09375 |MO|: 0.65625
DISP: 0.7385031553341784 |DISP|: 0.4961252427805765

Примеры расчета значений боковых выбросов ПФВК ПСС для пар сигналов (i; j)

i: 0 j: 0 64 8 -4 4 4 0 0 4 -4 -4 4 -4 -8 0 -4 0 8 0 8 -4 -8 -4 -8 8 -8 0 0 4 0 -4 4 4 8 4 4 -4 0 4 0 0 -8 8 -8 -4 -8 -4 8 0 8 0 -4 0 -8 -4 4 -4 -4 4 0 0 4 4 -4 8
i: 0 j: 1 0 8 12 12 4 0 -8 -12 4 -4 -4 -4 -16 -8 12 -16 0 0 0 4 0 12 -8 -8 8 0 -8 -4 8 -12 4 12 16 -12 4 12 8 4 -8 0 8 8 -8 -12 0 -4 0 0 0 16 12 8 -16 4 -4 4 4 12 -8 0 4 -12 12 -8
i: 0 j: 2 0 4 4 -8 20 20 0 8 12 0 -4 -8 0 -4 4 -4 -16 4 0 -8 -8 8 0 12 0 4 0 0 8 0 4 0 0 8 -4 0 8 8 0 4 0 -4 0 0 -8 -16 0 -12 -16 -4 -4 -12 0 8 4 8 12 -8 0 4 20 -16 -4 4
i: 0 j: 3 0 -4 -4 -16 4 -4 0 -8 -12 -8 -4 8 8 12 -4 -4 -8 12 0 -16 0 0 8 -4 0 -4 -16 8 16 0 -4 8 24 0 4 0 16 0 16 4 0 -12 -8 8 0 8 0 4 -8 4 4 -4 8 8 4 0 -12 -8 0 20 4 8 4 4
i: 0 j: 4 0 4 8 0 -12 -12 12 16 -4 8 -8 0 -8 4 16 -4 0 -4 4 8 -8 0 -4 12 8 4 -12 -8 0 8 8 -16 0 8 8 -16 0 0 -12 12 8 4 4 8 8 0 12 -4 0 -4 8 -4 8 8 8 8 -4 8 -4 4 12 -8 8 -12

i: 0 j: 5 0 12 0 0 12 -12 4 16 4 -16 -8 -8 -8 -4 0 -4 8 4 4 8 8 0 12 -4 -8 -4 4 8 0 0 8 8 8 16 0 8 0 0 12 -4 -8 -4 -4 -8 -8 16 4 -4 8 4 0 -4 8 0 0 16 4 -24 -4 -4 -12 -8 8 4
i: 0 j: 6 0 16 -8 4 -4 8 -4 -12 -4 -4 -8 -4 -8 0 8 8 8 0 -12 -12 0 12 4 0 0 -8 12 4 0 -4 8 12 8 12 -8 -12 0 -12 -12 0 0 -8 4 -4 0 4 4 0 8 8 -16 0 8 4 -8 -12 -4 -4 -12 8 4 4 8 16
i: 0 j: 7 0 0 -8 -12 -12 0 -4 4 4 12 0 4 24 0 0 8 0 0 -4 4 0 4 -4 0 0 -8 -12 4 16 -20 0 -12 0 12 -8 -4 -16 -4 4 0 0 -8 -12 -4 0 -4 4 0 0 -8 0 0 -24 4 -8 -4 4 4 -4 -16 12 -4 0 0
i: 0 j: 8 0 -4 0 4 0 -4 -12 -4 -4 8 -8 -4 12 -4 0 -8 16 12 4 -4 -4 0 -4 -8 8 4 -12 -4 -4 0 16 -4 0 0 16 4 -20 0 4 -8 -8 4 -4 -4 -4 -8 4 0 16 4 8 8 12 8 -8 -12 4 0 -4 -8 -8 -8 0 -8
i: 0 j: 9 0 4 8 -12 -16 12 -4 -4 -4 8 0 -4 -4 -4 8 16 24 4 4 12 4 0 -4 8 0 4 -4 -12 -4 0 -8 -4 24 8 -8 12 4 0 -4 8 0 4 -4 4 -4 -16 4 8 24 -4 0 8 4 0 0 12 4 -8 4 8 0 0 8 0
i: 0 j: 10 0 0 0 0 8 0 12 0 4 -12 0 16 4 8 8 4 8 8 4 0 20 12 -4 12 8 -16 -12 16 4 4 0 8 -24 -4 0 -16 -4 4 -4 -4 -8 0 -12 8 12 -4 -4 20 8 8 0 4 12 4 16 0 -4 -4 -4 4 8 4 0 -12
i: 0 j: 11 0 16 0 -16 -8 8 -4 0 -12 -4 0 0 4 -16 -8 -4 0 -8 -4 -16 12 4 4 -4 0 -8 4 -8 4 -4 0 -8 -16 -4 0 -8 4 12 12 12 0 8 -4 0 12 -4 4 -4 0 8 0 -12 4 4 0 8 12 -4 -4 4 0 4 0 -4
i: 0 j: 12 0 0 4 8 8 8 8 8 4 -4 -12 8 12 8 12 4 8 0 -8 0 4 -4 8 12 0 -16 0 -8 -20 4 12 -8 8 -4 -4 0 4 4 16 20 0 -24 0 0 -4 4 0 -4 8 8 12 -4 -12 -4 4 0 -4 -4 -16 -12 0 4 4 4
i: 0 j: 13 0 0 4 0 0 8 0 8 4 4 4 0 4 -8 4 -4 0 16 16 -8 4 -4 8 12 -8 8 0 8 4 -12 4 -8 0 12 12 0 4 -12 -8 4 8 0 -8 0 4 -4 16 -12 0 8 -4 4 4 -12 -4 8 -4 12 0 -4 -16 12 12 -4
i: 0 j: 14 0 4 -4 4 -8 -4 0 -4 12 -8 -12 -4 12 -12 4 0 0 12 0 4 -12 -8 -8 0 0 12 8 -4 -4 -8 -4 4 0 8 -12 -4 -4 8 -8 -8 0 4 0 -4 20 -8 -8 0 0 12 -4 -8 -4 -8 -4 -4 -12 -8 -8 0 8 -16 4 0
i: 0 j: 15 0 -4 -12 -4 0 4 0 12 -4 -8 -4 4 4 -4 4 8 8 4 -16 -4 -12 0 0 -16 -8 -4 -16 -4 4 16 12 4 8 0 -4 -4 -4 16 -8 -8 8 -12 0 12 12 8 16 8 8 4 -12 -16 -4 8 -4 4 4 0 0 -8 -8 0 4 8
i: 0 j: 16 0 8 -4 -8 8 0 8 -8 -8 -4 -4 -4 4 -16 -12 -8 8 0 0 8 -4 -12 0 12 -12 -16 -8 -4 -12 -4 4 4 0 4 4 0 -4 -4 0 -4 4 0 -8 4 4 -4 0 0 -8 8 12 4 -12 4 -4 0 -16 4 8 8 -8 -12 -4 8
i: 0 j: 17 0 0 12 -8 0 8 0 16 8 -12 4 20 -4 -8 12 -8 -8 0 0 -16 -12 4 -8 -4 -12 0 -8 -12 -12 -4 4 4 -8 -4 4 8 -4 4 8 4 -4 8 -8 4 -4 -4 0 0 8 -8 -12 -4 -4 12 -4 -8 -8 -4 -8 -8 0 12 12 0
i: 0 j: 18 0 -4 -4 12 -8 4 8 4 0 -8 -4 -8 -4 4 -4 4 8 -4 8 -12 -12 16 0 -8 -4 -4 -8 -8 4 -8 -4 0 -8 0 4 4 4 0 0 24 4 -4 -8 8 4 -8 8 4 -8 -4 -4 -8 -12 0 4 -12 -16 -16 -8 -4 -16 -8 4 -12
i: 0 j: 19 0 12 4 -4 0 -12 -24 -4 0 8 -4 0 4 4 12 4 -8 4 0 -4 -4 8 0 -8 -20 4 0 16 -12 0 4 0 0 0 -4 -4 4 0 0 0 -4 -4 0 -8 -4 -16 0 4 8 4 12 0 -4 0 12 12 -8 0 0 12 -8 -8 -4 -4

i: 0 j: 20 0 4 8 12 0 -4 -4 -4 0 8 0 8 12 -4 0 4 8 12 12 12 -4 0 -4 -8 -12 -12 -4 8 4 0 0 -16 -8 -8 8 12 4 0 -4 0 12 -4 20 8 -4 8 12 -4 -8 4 8 -8 4 8 -24 4 0 -8 -12 4 16 0 -16 4
i: 0 j: 21 0 4 0 4 0 4 4 4 0 8 16 -8 -4 4 8 -12 8 4 4 -4 -4 0 -12 8 4 -20 4 8 -4 0 -16 0 16 8 0 -4 12 8 -12 -8 -12 -4 12 0 12 -8 -4 -4 -8 -4 8 -8 -12 0 -8 -4 -8 -8 -4 -4 0 8 0 -4
i: 0 j: 22 0 -8 16 0 8 0 -4 -8 -8 -12 -8 4 12 0 -8 0 -8 8 12 8 -4 12 -4 -12 -4 0 4 4 -4 12 8 -4 0 4 0 0 4 -12 -20 -4 -4 -8 -4 -4 4 4 -12 -16 8 8 0 -4 -4 4 0 -8 0 -12 12 8 0 4 8 0
i: 0 j: 23 0 0 0 8 8 0 -20 16 8 -4 0 4 -4 -16 -8 0 -8 -8 -4 -8 -4 4 -4 4 -4 0 20 4 20 4 0 -4 8 12 16 0 -4 4 -4 4 4 0 -4 4 4 -4 -4 0 8 8 8 12 -4 4 -8 0 -8 -4 12 0 0 4 0 -8
i: 0 j: 24 0 4 0 8 4 -12 -4 -8 16 8 8 -4 8 12 0 -8 8 4 -20 0 16 0 -12 -4 4 4 4 -4 0 16 8 12 -8 8 0 8 8 0 4 12 12 -4 4 4 -8 -8 4 -8 -8 4 -8 -12 -8 -8 0 -8 -8 0 12 -8 -4 8 8 8
i: 0 j: 25 0 4 -8 0 -4 -4 4 0 8 0 0 4 8 12 0 0 -8 -4 4 0 -24 0 -4 -4 -4 4 4 -12 8 8 0 4 0 -8 -8 -8 8 -8 12 4 12 4 4 4 24 0 -4 0 8 -4 -8 20 0 -16 0 16 8 -8 -4 -8 -4 8 0 -8
i: 0 j: 26 0 0 -8 -12 12 -8 -12 4 16 -4 8 0 16 0 8 4 8 -8 -4 4 0 -4 12 8 4 8 4 0 0 12 0 -8 0 -4 -8 4 -8 -12 -4 8 4 16 4 0 8 20 12 12 -8 0 0 0 -16 4 0 -4 0 4 -4 4 4 12 0 -12
i: 0 j: 27 0 8 -8 12 4 -8 4 12 8 -4 8 -8 0 8 0 -4 -8 8 -4 -12 -8 -12 -4 -8 -4 -16 -4 -8 -8 -4 0 0 -8 4 -8 20 8 -12 -4 0 20 0 -4 -16 8 4 -4 4 8 0 -8 0 8 4 8 -12 0 4 20 4 4 4 0 4
i: 0 j: 28 0 -8 -12 4 20 8 8 -4 0 12 4 0 0 -16 4 4 -8 -8 0 -4 -8 4 8 8 12 0 -16 0 0 -4 -4 8 0 4 -4 -4 8 12 8 0 12 16 8 -16 -16 -4 8 4 8 -8 -4 0 0 4 4 12 0 -4 0 -4 -12 -4 -12 4
i: 0 j: 29 0 -16 4 4 4 0 16 4 8 12 4 0 -8 0 4 12 -8 -8 0 -12 8 4 0 -8 -12 8 -8 0 0 4 -12 0 8 -4 -4 4 0 -12 16 -8 -4 16 0 8 8 4 0 -4 8 8 4 -8 0 -4 4 -12 0 -4 -24 4 -4 -4 -4 4

i: 1 j: 0 0 -8 12 -12 4 0 -8 12 4 4 -4 4 -16 8 12 16 0 0 0 -4 0 -12 -8 8 8 0 -8 4 8 12 4 -12 16 12 4 -12 8 -4 -8 0 8 -8 -8 12 0 4 0 0 0 -16 12 -8 -16 -4 -4 -4 4 -12 -8 0 4 12 12 8
i: 1 j: 1 64 -8 -4 -4 4 0 0 -4 -4 4 4 4 -8 0 -4 0 8 0 8 4 -8 4 -8 -8 -8 0 0 -4 0 4 4 -4 8 -4 4 4 0 -4 0 0 -8 -8 -8 4 -8 4 8 0 8 0 -4 0 -8 4 4 4 -4 -4 0 0 4 -4 -4 -8
i: 1 j: 2 0 4 -4 16 4 4 0 8 -12 8 -4 -8 8 -12 -4 4 -8 -12 0 16 0 0 8 4 0 4 -16 -8 16 0 -4 -8 24 0 4 0 16 0 16 -4 0 12 -8 -8 0 -8 0 -4 -8 -4 4 4 8 -8 4 0 -12 8 0 -20 4 -8 4 -4
i: 1 j: 3 0 -4 4 8 20 -20 0 -8 12 0 -4 8 0 4 4 4 -16 -4 0 8 -8 -8 0 -12 0 -4 0 0 8 0 4 0 0 -8 -4 0 8 -8 0 -4 0 4 0 0 -8 16 0 12 -16 4 -4 12 0 -8 4 -8 12 8 0 -4 20 16 -4 -4
i: 1 j: 4 0 -12 0 0 12 12 4 -16 4 16 -8 8 -8 4 0 4 8 -4 4 -8 8 0 12 4 -8 4 4 -8 0 0 8 -8 8 -16 0 -8 0 0 12 4 -8 4 -4 8 -8 -16 4 4 8 -4 0 4 8 0 0 -16 4 24 -4 4 -12 8 8 -4
i: 1 j: 5 0 -4 8 0 -12 12 12 -16 -4 -8 -8 0 -8 -4 16 4 0 4 4 -8 -8 0 -4 -12 8 -4 -12 8 0 -8 8 16 0 -8 8 16 0 0 -12 -12 8 -4 4 -8 8 0 12 4 0 4 8 4 8 -8 8 -8 -4 -8 -4 -4 12 8 8 12

i: 1 j: 6 0 0 -8 12 -12 0 -4 -4 4 -12 0 -4 24 0 0 -8 0 0 -4 -4 0 -4 -4 0 0 8 -12 -4 16 20 0 12 0 -12 -8 4 -16 4 4 0 0 8 -12 4 0 4 4 0 0 8 0 0 -24 -4 -8 4 4 -4 -4 16 12 4 0 0
i: 1 j: 7 0 -16 -8 -4 -4 -8 -4 12 -4 4 -8 4 -8 0 8 -8 8 0 -12 12 0 -12 4 0 0 8 12 -4 0 4 8 -12 8 -12 -8 12 0 12 -12 0 0 8 4 4 0 -4 4 0 8 -8 -16 0 8 -4 -8 12 -4 4 -12 -8 4 -4 8 -16
i: 1 j: 8 0 -4 8 12 -16 -12 -4 4 -4 -8 0 4 -4 4 8 -16 24 -4 4 -12 4 0 -4 -8 0 -4 -4 12 -4 0 -8 4 24 -8 -8 -12 4 0 -4 -8 0 -4 -4 -4 -4 16 4 -8 24 4 0 -8 4 0 0 -12 4 8 4 -8 0 0 8 0
i: 1 j: 9 0 4 0 -4 0 4 -12 4 -4 -8 -8 4 12 4 0 8 16 -12 4 4 -4 0 -4 8 8 -4 -12 4 -4 0 16 4 0 0 16 -4 -20 0 4 8 -8 -4 -4 4 -4 8 4 0 16 -4 8 -8 12 -8 -8 12 4 0 -4 8 -8 8 0 8
i: 1 j: 10 0 -16 0 16 -8 -8 -4 0 -12 4 0 0 4 16 -8 4 0 8 -4 16 12 -4 4 4 0 8 4 8 4 4 0 8 -16 4 0 8 4 -12 12 -12 0 -8 -4 0 12 4 4 4 0 -8 0 12 4 -4 0 -8 12 4 -4 -4 0 -4 0 4
i: 1 j: 11 0 0 0 0 8 0 12 0 4 12 0 -16 4 -8 8 -4 8 -8 4 0 20 -12 -4 -12 8 16 -12 -16 4 -4 0 -8 -24 4 0 16 -4 -4 -4 4 -8 0 -12 -8 12 4 -4 -20 8 -8 0 -4 12 -4 16 0 -4 4 -4 -4 8 -4 0 12
i: 1 j: 12 0 0 4 0 0 -8 0 -8 4 -4 4 0 4 8 4 4 0 -16 16 8 4 4 8 -12 -8 -8 0 -8 4 12 4 8 0 -12 12 0 4 12 -8 -4 8 0 -8 0 4 4 16 12 0 -8 -4 -4 4 12 -4 -8 -4 -12 0 4 -16 -12 12 4
i: 1 j: 13 0 0 4 -8 8 -8 8 -8 4 4 -12 -8 12 -8 12 -4 8 0 -8 0 4 4 8 -12 0 16 0 8 -20 -4 12 8 8 4 -4 0 4 -4 16 -20 0 24 0 0 -4 -4 0 4 8 -8 12 4 -12 4 4 0 -4 4 -16 12 0 -4 4 -4
i: 1 j: 14 0 4 -12 4 0 -4 0 -12 -4 8 -4 -4 4 4 4 -8 8 -4 -16 4 -12 0 0 16 -8 4 -16 4 4 -16 12 -4 8 0 -4 4 -4 -16 -8 8 8 12 0 -12 12 -8 16 -8 8 -4 -12 16 -4 -8 -4 -4 4 0 0 8 -8 0 4 -8
i: 1 j: 15 0 -4 -4 -4 -8 4 0 4 12 8 -12 4 12 12 4 0 0 -12 0 -4 -12 8 -8 0 0 -12 8 4 -4 8 -4 -4 0 -8 -12 4 -4 -8 -8 8 0 -4 0 4 20 8 -8 0 0 -12 -4 8 -4 8 -4 4 -12 8 -8 0 8 16 4 0
i: 1 j: 16 0 0 12 8 0 -8 0 -16 8 12 4 -20 -4 8 12 8 -8 0 0 16 -12 -4 -8 4 -12 0 -8 12 -12 4 4 -4 -8 4 4 -8 -4 -4 8 -4 -4 -8 -8 -4 -4 4 0 0 8 8 -12 4 -4 -12 -4 8 -8 4 -8 8 0 -12 12 0
i: 1 j: 17 0 -8 -4 8 8 0 8 8 -8 4 -4 4 4 16 -12 8 8 0 0 -8 -4 12 0 -12 -12 16 -8 4 -12 4 4 -4 0 -4 4 0 -4 4 0 4 4 0 -8 -4 4 4 0 0 -8 -8 12 -4 -12 -4 -4 0 -16 -4 8 -8 -8 12 -4 -8
i: 1 j: 18 0 -12 4 4 0 12 -24 4 0 -8 -4 0 4 -4 12 -4 -8 -4 0 4 -4 -8 0 8 -20 -4 0 -16 -12 0 4 0 0 0 -4 4 4 0 0 0 -4 4 0 8 -4 16 0 -4 8 -4 12 0 -4 0 12 -12 -8 0 0 -12 -8 8 -4 4
i: 1 j: 19 0 4 -4 -12 -8 -4 8 -4 0 8 -4 8 -4 -4 -4 -4 8 4 8 12 -12 -16 0 8 -4 4 -8 8 4 8 -4 0 -8 0 4 -4 4 0 0 -24 4 4 -8 -8 4 8 8 -4 -8 4 -4 8 -12 0 4 12 -16 16 -8 4 -16 8 4 12
i: 1 j: 20 0 -4 0 -4 0 -4 4 -4 0 -8 16 8 -4 -4 8 12 8 -4 4 4 -4 0 -12 -8 4 20 4 -8 -4 0 -16 0 16 -8 0 4 12 -8 -12 8 -12 4 12 0 12 8 -4 4 -8 4 8 8 -12 0 -8 4 -8 8 -4 4 0 -8 0 4
i: 1 j: 21 0 -4 8 -12 0 4 -4 4 0 -8 0 -8 12 4 0 -4 8 -12 12 -12 -4 0 -4 8 -12 12 -4 -8 4 0 0 16 -8 8 8 -12 4 0 -4 0 12 4 20 -8 -4 -8 12 4 -8 -4 8 8 4 -8 -24 -4 0 8 -12 -4 16 0 -16 -4

i: 1 j: 22 0 0 0 -8 8 0 -20 -16 8 4 0 -4 -4 16 -8 0 -8 8 -4 8 -4 -4 -4 -4 -4 0 20 -4 20 -4 0 4 8 -12 16 0 -4 -4 -4 -4 4 0 -4 -4 4 4 -4 0 8 -8 8 -12 -4 -4 -8 0 -8 4 12 0 0 -4 0 8
i: 1 j: 23 0 8 16 0 8 0 -4 8 -8 12 -8 -4 12 0 -8 0 -8 -8 12 -8 -4 -12 -4 12 -4 0 4 -4 -4 -12 8 4 0 -4 0 0 4 12 -20 4 -4 8 -4 4 4 -4 -12 16 8 -8 0 4 -4 -4 0 8 0 12 12 -8 0 -4 8 0
i: 1 j: 24 0 -4 -8 0 -4 4 4 0 8 0 0 -4 8 -12 0 0 -8 4 4 0 -24 0 -4 4 -4 -4 4 12 8 -8 0 -4 0 8 -8 8 8 8 12 -4 12 -4 4 -4 24 0 -4 0 8 4 -8 -20 0 16 0 -16 8 8 -4 8 -4 -8 0 8
i: 1 j: 25 0 -4 0 -8 4 12 -4 8 16 -8 8 4 8 -12 0 8 8 -4 -20 0 16 0 -12 4 4 -4 4 4 0 -16 8 -12 -8 -8 0 -8 8 0 4 -12 12 4 4 -4 -8 8 4 8 -8 -4 -8 12 -8 8 0 8 -8 0 12 8 -4 -8 8 -8
i: 1 j: 26 0 -8 -8 -12 4 8 4 -12 8 4 8 8 0 -8 0 4 -8 -8 -4 12 -8 12 -4 8 -4 16 -4 8 -8 4 0 0 -8 -4 -8 -20 8 12 -4 0 20 0 -4 16 8 -4 -4 -4 8 0 -8 0 8 -4 8 12 0 -4 20 -4 4 -4 0 -4
i: 1 j: 27 0 0 -8 12 12 8 -12 -4 16 4 8 0 16 0 8 -4 8 8 -4 -4 0 4 12 -8 4 -8 4 0 0 -12 0 8 0 4 -8 -4 -8 12 -4 -8 4 -16 4 0 8 -20 12 -12 -8 0 0 0 -16 -4 0 4 0 -4 -4 -4 4 -12 0 12
i: 1 j: 28 0 16 4 -4 4 0 16 -4 8 -12 4 0 -8 0 4 -12 -8 8 0 12 8 -4 0 8 -12 -8 -8 0 0 -4 -12 0 8 4 -4 -4 0 12 16 8 -4 -16 0 -8 8 -4 0 4 8 -8 4 8 0 4 4 12 0 4 -24 -4 -4 4 -4 -4
i: 1 j: 29 0 8 -12 -4 20 -8 8 4 0 -12 4 0 0 16 4 -4 -8 8 0 4 -8 -4 8 -8 12 0 -16 0 0 4 -4 -8 0 -4 -4 4 8 -12 8 0 12 -16 8 16 -16 4 8 -4 8 8 -4 0 0 -4 4 -12 0 4 0 4 -12 4 -12 -4

i: 2 j: 0 0 4 -4 -16 20 4 0 -8 12 8 4 8 0 -12 -4 -4 -16 -12 0 -16 -8 0 0 -4 0 4 0 8 8 0 -4 8 0 0 4 0 8 0 0 4 0 12 0 8 -8 -8 0 4 -16 -4 4 -4 0 -8 -4 0 12 8 0 20 20 -8 4 4
i: 2 j: 1 0 -4 4 -8 4 -20 0 8 -12 0 4 -8 8 4 4 -4 -8 -4 0 -8 0 -8 -8 12 0 -4 16 0 16 0 4 0 24 -8 -4 0 16 -8 -16 4 0 4 8 0 0 16 0 -12 -8 4 -4 -12 8 -8 -4 8 -12 8 0 4 4 16 -4 4
i: 2 j: 2 64 -8 4 12 4 0 0 -12 -4 4 -4 -4 -8 8 4 -16 8 0 -8 4 -8 -12 8 -8 -8 0 0 -4 0 12 -4 12 8 12 -4 12 0 -4 0 0 -8 -8 8 -12 -8 4 -8 0 8 -16 4 8 -8 -4 -4 4 -4 -12 0 0 4 12 4 -8
i: 2 j: 3 0 -8 -12 4 4 0 8 4 4 4 4 -4 -16 0 -12 0 0 0 0 -4 0 4 8 8 8 0 8 4 8 4 -4 4 16 -4 -4 -4 8 -4 8 0 8 -8 8 -4 0 4 0 0 0 0 -12 0 -16 4 4 -4 4 -4 8 0 4 -4 -12 8
i: 2 j: 4 0 0 8 -12 -4 0 4 4 -4 -12 8 4 -8 0 -8 8 8 0 12 4 0 -4 -4 0 0 8 -12 4 0 20 -8 -12 8 -12 8 -4 0 4 12 0 0 8 -4 -4 0 4 -4 0 8 8 16 0 8 -4 8 -4 -4 -4 12 -16 4 4 -8 0
i: 2 j: 5 0 -16 8 4 -12 -8 4 -12 4 4 0 -4 24 0 0 8 0 0 4 -12 0 -12 4 0 0 8 12 4 16 4 0 12 0 -12 8 -12 -16 12 -4 0 0 8 12 -4 0 -4 -4 0 0 -8 0 0 -24 -4 8 -12 4 4 4 8 12 -4 0 16
i: 2 j: 6 0 -12 -8 0 -12 12 -12 16 -4 16 8 -8 -8 4 -16 -4 0 -4 -4 8 -8 0 4 -4 8 4 12 8 0 0 -8 8 0 -16 -8 8 0 0 12 -4 8 4 -4 -8 8 -16 -12 -4 0 -4 -8 -4 8 0 -8 16 -4 24 4 -4 12 8 -8 4
i: 2 j: 7 0 -4 0 0 12 12 -4 16 4 -8 8 0 -8 -4 0 -4 8 4 -4 8 8 0 -12 12 -8 -4 -4 -8 0 -8 -8 -16 8 -8 0 -16 0 0 -12 12 -8 -4 4 8 -8 0 -4 -4 8 4 0 -4 8 -8 0 8 4 -8 4 4 -12 8 -8 -12

i: 2 j: 8 0 -16 0 -16 8 -8 -12 0 4 4 0 0 4 16 -8 -4 8 8 -4 -16 20 -4 4 -4 8 8 12 -8 4 4 0 -8 -24 4 0 -8 -4 -12 4 12 -8 -8 12 0 12 4 4 -4 8 -8 0 -12 12 -4 -16 8 -4 4 4 4 8 -4 0 -4
i: 2 j: 9 0 0 0 0 -8 0 4 0 -12 12 0 16 4 -8 8 4 0 -8 4 0 12 -12 -4 12 0 16 -4 16 4 -4 0 8 -16 4 0 -16 4 -4 -12 -4 0 0 4 8 12 4 -4 20 0 -8 0 4 4 -4 0 0 12 4 4 4 0 -4 0 -12
i: 2 j: 10 0 -4 0 -12 0 -12 12 -4 -4 -8 8 -4 12 4 0 16 16 -4 -4 12 -4 0 4 8 8 -4 12 -12 -4 0 -16 -4 0 -8 -16 12 -20 0 -4 8 -8 -4 4 4 -4 16 -4 8 16 4 -8 8 12 0 8 12 4 8 4 8 -8 0 0 0
i: 2 j: 11 0 4 -8 4 -16 4 4 -4 -4 -8 0 -4 -4 4 -8 -8 24 -12 -4 -4 4 0 4 -8 0 -4 4 -4 -4 0 8 -4 24 0 8 4 4 0 4 -8 0 -4 4 -4 -4 8 -4 0 24 -4 0 8 4 -8 0 -12 4 0 -4 -8 0 8 -8 -8
i: 2 j: 12 0 4 4 -4 -8 -4 0 12 12 8 12 4 12 4 -4 8 0 -4 0 -4 -12 0 8 -16 0 4 -8 -4 -4 -16 4 4 0 0 12 -4 -4 -16 8 -8 0 12 0 12 20 -8 8 8 0 -4 4 -16 -4 -8 4 4 -12 0 8 -8 8 0 -4 8
i: 2 j: 13 0 -4 12 4 0 4 0 -4 -4 8 4 -4 4 12 -4 0 8 -12 16 4 -12 8 0 0 -8 -12 16 -4 4 8 -12 4 8 -8 4 -4 -4 -8 8 -8 8 -4 0 -4 12 8 -16 0 8 -12 12 -8 -4 8 4 -4 4 8 0 0 -8 16 -4 0
i: 2 j: 14 0 0 -4 0 8 -8 -8 8 4 -4 12 0 12 8 -12 -4 8 -16 8 -8 4 4 -8 12 0 -8 0 8 -20 12 -12 -8 8 -12 4 0 4 12 -16 4 0 0 0 0 -4 4 0 -12 8 -8 -12 4 -12 12 -4 8 -4 -12 16 -4 0 -12 -4 -4
i: 2 j: 15 0 0 -4 8 0 -8 0 8 4 4 -4 8 4 -8 -4 4 0 0 -16 0 4 4 -8 12 -8 16 0 -8 4 -4 -4 -8 0 4 -12 0 4 -4 8 20 8 24 8 0 4 -4 -16 -4 0 -8 4 -4 4 4 4 0 -4 4 0 -12 -16 -4 -12 4
i: 2 j: 16 0 -12 4 -4 -8 12 -8 -4 0 -8 4 0 -4 -4 4 4 8 -4 -8 -4 -12 -8 0 -8 -4 -4 8 16 4 0 4 0 -8 0 -4 -4 4 0 0 0 4 4 8 -8 4 16 -8 4 -8 -4 4 0 -12 0 -4 12 -16 0 8 12 -16 8 -4 -4
i: 2 j: 17 0 4 -4 12 0 -4 24 4 0 8 4 -8 4 -4 -12 4 -8 4 0 -12 -4 -16 0 -8 -20 4 0 -8 -12 8 -4 0 0 0 4 4 4 0 0 24 -4 4 0 8 -4 8 0 4 8 4 -12 -8 -4 0 -12 -12 -8 16 0 -4 -8 8 4 -12
i: 2 j: 18 0 0 4 -8 8 -8 -8 16 -8 12 4 20 4 8 12 -8 8 0 0 -16 -4 -4 0 -4 -12 0 8 -12 -12 4 -4 4 0 4 -4 8 -4 -4 0 4 4 -8 8 4 4 4 0 0 -8 8 -12 -4 -12 -12 4 -8 -16 4 -8 -8 -8 -12 4 0
i: 2 j: 19 0 -8 -12 -8 0 0 0 -8 8 4 -4 -4 -4 16 -12 -8 -8 0 0 8 -12 12 8 12 -12 16 8 -4 -12 4 -4 4 -8 -4 -4 0 -4 4 -8 -4 -4 0 8 4 -4 4 0 0 8 -8 12 4 -4 -4 4 0 -8 -4 8 8 0 12 -12 8
i: 2 j: 20 0 0 -16 8 8 0 4 16 -8 4 8 4 12 16 8 0 -8 8 -12 -8 -4 -4 4 4 -4 0 -4 4 -4 -4 -8 -4 0 -12 0 0 4 -4 20 4 -4 0 4 4 4 4 12 0 8 -8 0 12 -4 -4 0 0 0 4 -12 0 0 -4 -8 -8
i: 2 j: 21 0 8 0 0 8 0 20 -8 8 12 0 4 -4 0 8 0 -8 -8 4 8 -4 -12 4 -12 -4 0 -20 4 20 -12 0 -4 8 -4 -16 0 -4 12 4 -4 4 8 4 -4 4 -4 4 -16 8 -8 -8 -4 -4 -4 8 -8 -8 12 -12 8 0 -4 0 0
i: 2 j: 22 0 -4 -8 4 0 -4 4 4 0 -8 0 -8 12 -4 0 -12 8 -4 -12 -4 -4 0 4 8 -12 20 4 8 4 0 0 0 -8 -8 -8 -4 4 -8 4 -8 12 4 -20 0 -4 8 -12 -4 -8 4 -8 -8 4 0 24 -4 0 8 12 -4 16 -8 16 -4

i: 2 j: 23 0 -4 0 12 0 4 -4 -4 0 -8 -16 8 -4 4 -8 4 8 -12 -4 12 -4 0 12 -8 4 12 -4 8 -4 0 16 -16 16 8 0 12 12 0 12 0 -12 4 -12 8 12 -8 4 -4 -8 -4 -8 -8 -12 -8 8 4 -8 8 4 4 0 0 0 4
i: 2 j: 24 0 -8 8 12 12 8 12 12 16 4 -8 -8 16 -8 -8 -4 8 -8 4 -12 0 12 -12 -8 4 16 -4 -8 0 4 0 0 0 -4 8 20 -8 12 4 0 4 0 -4 -16 8 -4 -12 4 -8 0 0 0 -16 -4 0 -12 0 -4 4 4 4 -4 0 4
i: 2 j: 25 0 0 8 -12 4 8 -4 4 8 4 -8 0 0 0 0 4 -8 8 4 4 -8 4 4 8 -4 -8 4 0 -8 -12 0 -8 -8 4 8 4 8 12 4 8 20 -16 4 0 8 -20 4 12 8 0 8 0 8 -4 -8 -4 0 -4 -20 4 4 -12 0 -12
i: 2 j: 26 0 -4 0 0 4 4 4 0 16 0 -8 4 8 -12 0 0 8 4 20 0 16 0 12 -4 4 -4 -4 -12 0 -8 -8 4 -8 8 0 -8 8 8 -4 4 12 -4 -4 4 -8 0 -4 0 -8 4 8 20 -8 16 0 16 -8 8 -12 -8 -4 -8 -8 -8
i: 2 j: 27 0 -4 8 8 -4 12 -4 -8 8 -8 0 -4 8 -12 0 -8 -8 -4 -4 0 -24 0 4 -4 -4 -4 -4 -4 8 -16 0 12 0 -8 8 8 8 0 -12 12 12 4 -4 4 24 8 4 -8 8 -4 8 -12 0 8 0 -8 8 0 4 -8 -4 -8 0 8
i: 2 j: 28 0 12 -4 0 4 4 -16 0 0 -8 20 -12 0 4 4 8 8 -4 8 8 0 -8 -16 4 -4 -4 -8 4 -8 8 -4 -4 24 8 4 0 0 0 0 -12 4 4 0 4 -8 8 16 0 -8 4 4 4 0 -16 -4 -8 -8 -8 -8 0 4 -8 4 16
i: 2 j: 29 0 -4 4 0 4 4 0 8 8 -16 12 4 -8 12 12 0 8 4 0 0 0 0 -16 -12 4 -4 -8 4 -8 -8 -4 4 -16 8 -4 -8 24 0 0 12 4 -4 16 -4 0 8 0 8 -8 12 4 -20 0 0 -12 0 8 -16 8 -8 -4 0 -12 0
i: 3 j: 0 0 4 4 8 4 20 0 -8 -12 0 4 8 8 -4 4 4 -8 4 0 8 0 8 -8 -12 0 4 16 0 16 0 4 0 24 8 -4 0 16 8 -16 -4 0 -4 8 0 0 -16 0 12 -8 -4 -4 12 8 8 -4 -8 -12 -8 0 -4 4 -16 -4 -4
i: 3 j: 1 0 -4 -4 16 20 -4 0 8 12 -8 4 -8 0 12 -4 4 -16 12 0 16 -8 0 0 4 0 -4 0 -8 8 0 -4 -8 0 0 4 0 8 0 0 -4 0 -12 0 -8 -8 8 0 -4 -16 4 4 4 0 8 -4 0 12 -8 0 -20 20 8 4 -4
i: 3 j: 2 0 8 -12 -4 4 0 8 -4 4 -4 4 4 -16 0 -12 0 0 0 0 4 0 -4 8 -8 8 0 8 -4 8 -4 -4 -4 16 4 -4 4 8 4 8 0 8 8 8 4 0 -4 0 0 0 0 -12 0 -16 -4 4 4 4 4 8 0 4 4 -12 -8
i: 3 j: 3 64 8 4 -12 4 0 0 12 -4 -4 -4 4 -8 -8 4 16 8 0 -8 -4 -8 12 8 8 -8 0 0 4 0 -12 -4 -12 8 -12 -4 -12 0 4 0 0 -8 8 8 12 -8 -4 -8 0 8 16 4 -8 -8 4 -4 -4 -4 12 0 0 4 -12 4 8
i: 3 j: 4 0 16 8 -4 -12 8 4 12 4 -4 0 4 24 0 0 -8 0 0 4 12 0 12 4 0 0 -8 12 -4 16 -4 0 -12 0 12 8 12 -16 -12 -4 0 0 -8 12 4 0 4 -4 0 0 8 0 0 -24 4 8 12 4 -4 4 -8 12 4 0 -16
i: 3 j: 5 0 0 8 12 -4 0 4 -4 -4 12 8 -4 -8 0 -8 -8 8 0 12 -4 0 4 -4 0 0 -8 -12 -4 0 -20 -8 12 8 12 8 4 0 -4 12 0 0 -8 -4 4 0 -4 -4 0 8 -8 16 0 8 4 8 4 -4 4 12 16 4 -4 -8 0
i: 3 j: 6 0 4 0 0 12 -12 -4 -16 4 8 8 0 -8 4 0 4 8 -4 -4 -8 8 0 -12 -12 -8 4 -4 8 0 8 -8 16 8 8 0 16 0 0 -12 -12 -8 4 4 -8 -8 0 -4 4 8 -4 0 4 8 8 0 -8 4 8 4 -4 -12 -8 -8 12
i: 3 j: 7 0 12 -8 0 -12 -12 -12 -16 -4 -16 8 8 -8 -4 -16 4 0 4 -4 -8 -8 0 4 4 8 -4 12 -8 0 0 -8 -8 0 16 -8 -8 0 0 12 4 8 -4 -4 8 8 16 -12 4 0 4 -8 4 8 0 -8 -16 -4 -24 4 4 12 -8 -8 -4
i: 3 j: 8 0 0 0 0 -8 0 4 0 -12 -12 0 -16 4 8 8 -4 0 8 4 0 12 12 -4 -12 0 -16 -4 -16 4 4 0 -8 -16 -4 0 16 4 4 -12 4 0 0 4 -8 12 -4 -4 -20 0 8 0 -4 4 4 0 0 12 -4 4 -4 0 4 0 12
i: 3 j: 9 0 16 0 16 8 8 -12 0 4 -4 0 0 4 -16 -8 4 8 -8 -4 16 20 4 4 4 8 -8 12 8 4 -4 0 8 -24 -4 0 8 -4 12 4 -12 -8 8 12 0 12 -4 4 4 8 8 0 12 12 4 -16 -8 -4 -4 4 -4 8 4 0 4
i: 3 j: 10 0 -4 -8 -4 -16 -4 4 4 -4 8 0 4 -4 -4 -8 8 24 12 -4 4 4 0 4 8 0 4 4 4 -4 0 8 4 24 0 8 -4 4 0 4 8 0 4 4 4 -4 -8 -4 0 24 4 0 -8 4 8 0 12 4 0 -4 8 0 -8 -8 8

i: 3 j: 11 0 4 0 12 0 12 12 4 -4 8 8 4 12 -4 0 -16 16 4 -4 -12 -4 0 4 -8 8 4 12 12 -4 0 -16 4 0 8 -16 -12 -20 0 -4 -8 -8 4 4 -4 -4 -16 -4 -8 16 -4 -8 -8 12 0 8 -12 4 -8 4 -8 -8 0 0 0
i: 3 j: 12 0 4 12 -4 0 -4 0 4 -4 -8 4 4 4 -12 -4 0 8 12 16 -4 -12 -8 0 0 -8 12 16 4 4 -8 -12 -4 8 8 4 4 -4 8 8 8 8 4 0 4 12 -8 -16 0 8 12 12 8 -4 -8 4 4 4 -8 0 0 -8 -16 -4 0
i: 3 j: 13 0 -4 4 4 -8 4 0 -12 12 -8 12 -4 12 -4 -4 -8 0 4 0 4 -12 0 8 16 0 -4 -8 4 -4 16 4 -4 0 0 12 4 -4 16 8 8 0 -12 0 -12 20 8 8 -8 0 4 4 16 -4 8 4 -4 -12 0 8 8 8 0 -4 -8
i: 3 j: 14 0 0 -4 -8 0 8 0 -8 4 -4 -4 -8 4 8 -4 -4 0 0 -16 0 4 -4 -8 -12 -8 -16 0 8 4 4 -4 8 0 -4 -12 0 4 4 8 -20 8 -24 8 0 4 4 -16 4 0 8 4 4 4 -4 4 0 -4 -4 0 12 -16 4 -12 -4
i: 3 j: 15 0 0 -4 0 8 8 -8 -8 4 4 12 0 12 -8 -12 4 8 16 8 8 4 -4 -8 -12 0 8 0 -8 -20 -12 -12 8 8 12 4 0 4 -12 -16 -4 0 0 0 0 -4 -4 0 12 8 8 -12 -4 -12 -12 -4 -8 -4 12 16 4 0 12 -4 4
i: 3 j: 16 0 -4 -4 -12 0 4 24 -4 0 -8 4 8 4 4 -12 -4 -8 -4 0 12 -4 16 0 8 -20 -4 0 8 -12 -8 -4 0 0 0 4 -4 4 0 0 -24 -4 -4 0 -8 -4 -8 0 -4 8 -4 -12 8 -4 0 -12 12 -8 -16 0 4 -8 -8 4 12
i: 3 j: 17 0 12 4 4 -8 -12 -8 4 0 8 4 0 -4 4 4 -4 8 4 -8 4 -12 8 0 8 -4 4 8 -16 4 0 4 0 -8 0 -4 4 4 0 0 0 4 -4 8 8 4 -16 -8 -4 -8 4 4 0 -12 0 -4 -12 -16 0 8 -12 -16 -8 -4 4
i: 3 j: 18 0 8 -12 8 0 0 0 8 8 -4 -4 4 -4 -16 -12 8 -8 0 0 -8 -12 -12 8 -12 -12 -16 8 4 -12 -4 -4 -4 -8 4 -4 0 -4 -4 -8 4 -4 0 8 -4 -4 -4 0 0 8 8 12 -4 -4 4 4 0 -8 4 8 -8 0 -12 -12 -8
i: 3 j: 19 0 0 4 8 8 8 -8 -16 -8 -12 4 -20 4 -8 12 8 8 0 0 16 -4 4 0 4 -12 0 8 12 -12 -4 -4 -4 0 -4 -4 -8 -4 4 0 -4 4 8 8 -4 4 -4 0 0 -8 -8 -12 4 -12 12 4 8 -16 -4 -8 8 -8 12 4 0
i: 3 j: 20 0 -8 0 0 8 0 20 8 8 -12 0 -4 -4 0 8 0 -8 8 4 -8 -4 12 4 12 -4 0 -20 -4 20 12 0 4 8 4 -16 0 -4 -12 4 4 4 -8 4 4 4 4 4 16 8 8 -8 4 -4 4 8 8 -8 -12 -12 -8 0 4 0 0
i: 3 j: 21 0 0 -16 -8 8 0 4 -16 -8 -4 8 -4 12 -16 8 0 -8 -8 -12 8 -4 4 4 -4 -4 0 -4 -4 -4 4 -8 4 0 12 0 0 4 4 20 -4 -4 0 4 -4 4 -4 12 0 8 8 0 -12 -4 4 0 0 0 -4 -12 0 0 4 -8 8
i: 3 j: 22 0 4 0 -12 0 -4 -4 4 0 8 -16 -8 -4 -4 -8 -4 8 12 -4 -12 -4 0 12 8 4 -12 -4 -8 -4 0 16 16 16 -8 0 -12 12 0 12 0 -12 -4 -12 -8 12 8 4 4 -8 4 -8 8 -12 8 8 -4 -8 -8 4 -4 0 0 0 -4
i: 3 j: 23 0 4 -8 -4 0 4 4 -4 0 8 0 8 12 4 0 12 8 4 -12 4 -4 0 4 -8 -12 -20 4 -8 4 0 0 0 -8 8 -8 4 4 8 4 8 12 -4 -20 0 -4 -8 -12 4 -8 -4 -8 8 4 0 24 4 0 -8 12 4 16 8 16 4
i: 3 j: 24 0 0 8 12 4 -8 -4 -4 8 -4 -8 0 0 0 0 -4 -8 -8 4 -4 -8 -4 4 -8 -4 8 4 0 -8 12 0 8 -8 -4 8 -4 8 -12 4 -8 20 16 4 0 8 20 4 -12 8 0 8 0 8 4 -8 4 0 4 -20 -4 4 12 0 12
i: 3 j: 25 0 8 8 -12 12 -8 12 -12 16 -4 -8 8 16 8 -8 4 8 8 4 12 0 -12 -12 8 4 -16 -4 8 0 -4 0 0 0 4 8 -20 -8 -12 4 0 4 0 -4 16 8 4 -12 -4 -8 0 0 0 -16 4 0 12 0 4 4 -4 4 4 0 -4
i: 3 j: 26 0 4 8 -8 -4 -12 -4 8 8 8 0 4 8 12 0 8 -8 4 -4 0 -24 0 4 4 -4 4 -4 4 8 16 0 -12 0 8 8 -8 8 0 -12 -12 12 -4 -4 -4 24 -8 4 8 8 4 8 12 0 -8 0 8 8 0 4 8 -4 8 0 -8

i: 3 j: 27 0 4 0 0 4 -4 4 0 16 0 -8 -4 8 12 0 0 8 -4 20 0 16 0 12 4 4 4 -4 12 0 8 -8 -4 -8 -8 0 8 8 -8 -4 -4 12 4 -4 -4 -8 0 -4 0 -8 -4 8 -20 -8 -16 0 -16 -8 -8 -12 8 -4 8 -8 8
i: 3 j: 28 0 4 4 0 4 -4 0 -8 8 16 12 -4 -8 -12 12 0 8 -4 0 0 0 0 -16 12 4 4 -8 -4 -8 8 -4 -4 -16 -8 -4 8 24 0 0 -12 4 4 16 4 0 -8 0 -8 -8 -12 4 20 0 0 -12 0 8 16 8 8 -4 0 -12 0
i: 3 j: 29 0 -12 -4 0 4 -4 -16 0 0 8 20 12 0 -4 4 -8 8 4 8 -8 0 8 -16 -4 -4 4 -8 -4 -8 -8 -4 4 24 -8 4 0 0 0 0 12 4 -4 0 -4 -8 -8 16 0 -8 -4 4 -4 0 16 -4 8 -8 8 -8 0 4 8 4 -16

ПРИЛОЖЕНИЕ Ж

ЗАТВЕРДЖУЮ

ТВО директора ІПРІ НАН України,
д.т.н., професор
_____ Додонов О.Г.
«__» _____ 2015 р.

АКТ

використання наукових результатів докторської дисертаційної роботи

ЗАМУЛИ ОЛЕКСАНДРА АНДРІЙОВИЧА

Комісія у складі:

Голова комісії:
Завідувач відділом ІПРІ НАН України, д.т.н., професор — Матов О.Я.

Члени комісії:
Старший науковий співробітник, к.в.н., доцент — Руденко М.П.
Старший науковий співробітник, к.т.н. — Сенченко В.Р.

склала цей акт про те, що на протязі 2013 -2015 р.р. результати докторської дисертаційної роботи Замули Олександра Андрійовича "Моделі і методи синтезу складних сигналів з необхідними властивостями для захищених телекомунікаційних систем" використані Інститутом проблем реєстрації інформації НАН України при виконанні наступних НДР та ДКР:

Назва НД та ДКР	Форма впровадження	Ефективність від впровадження
1. Побудова моделюючого комплексу для управління функціонуванням корабельного з'єднання	1. Метод синтезу нелінійних дискретних сигналів, що використовує випадкові (псевдовипадкові) процеси, і дозволяє створювати сигнали з необхідними ансамблевими, структурними та кореляційними властивостями	Дозволяє покращити показники завадозахищеності та інформаційної безпеки телекомунікаційної системи корабельного з'єднання в умовах зовнішніх і внутрішніх впливів

Назва НД та ДКР	Форма впровадження	Ефективність від впровадження
	2. Метод інформаційного обміну даними, в якому, застосовується зміна, за визначеним правилом, відповідності біт повідомлення складний сигнал, і в якості складних сигналів застосовуються сигнали з необхідними ансамблевими, структурними та кореляційними властивостями	
2. Дослідити та розробити методи забезпечення живучості комп'ютерних інформаційних мереж для високотехнологічних об'єктів» (шифр – «КІМ-2013»	3. Метод синтезу системи нелінійних дискретних сигналів, в якому, використовується процедура зчитування та запису (за визначеним правилом) символів послідовності сигналу для формування всієї множини сигналів, що відноситься до цієї системи сигналів	Дозволяє покращити такі показники функціонування телекомунікаційної системи, як завадозахищеність та інформаційна безпека мереж для високотехнологічних об'єктів

Голова комісії Матов О.Я.

Члени комісії Руденко М.П.

Сенченко В.Р.

ДЕРЖАВНИЙ КОНЦЕРН "УКРОБОРОНПРОМ"
ДЕРЖАВНЕ ПІДПРИЄМСТВО
"ЦЕНТРАЛЬНЕ КОНСТРУКТОРСЬКЕ БЮРО "ПРОТОН"
ДП «ЦКБ «ПРОТОН»

Майдан Повстання, буд 7/8 , м. Харків, 61001 Телефон: (057) 732-15-48. Телефакс: (057) 732-25-44
код ЄДРПОУ 14309408

"ЗАТВЕРДЖУЮ"

Проректор Харківського національного університету імені В.Н. Каразіна

д.т.н., професор _____ В.О. Катрич

"___" _____ 2015р.

"ЗАТВЕРДЖУЮ"

Директор ДП«ЦКБ « Протон »

к.т.н. _____ О.І. Вотяков

"___" _____ 2015р.

23.09.2015 № 632/02

АКТ

реалізації результатів дисертаційних досліджень

Замули Олександра Андрійовича

Комісія ДП «ЦКБ«Протон» в складі: голови – головного наукового співробітника кандидата технічних доцента наук Петрова Вадима Лук'яновича, і членів комісії – головного наукового співробітника кандидата технічних наук Голобородько Юрія Миколайовича, головного наукового співробітника кандидата технічних наук старшого наукового співробітника Писарьонка Георгія Георгійовича, головного конструктора ДКР Повтарєва Валєрія Івановича, склала дійсний акт в тім, що в ДП «ЦКБ«Протон» при виконанні науково-дослідних робіт, щодо розробки перспективних засобів зв'язку та визначення шляхів модернізації «Малогабаритної завадозахищеної КХ радіостанції малої

ппотужності» яка розроблена та вироблена у ЦКБ, використані наступні результати наукових досліджень Замули О.А.:

- метод синтезу нелінійних криптографічних дискретних сигналів, щодозволяє завадостійкість прийому сигналів в умовах впливу різноманітних перешкод.

- удосконалений метод синтезу нелінейних дискретних сигналів із заданими ансамблевими, кореляційними і структурними властивостями, що дозволяє підвищити продуктивність синтезу системи сигналів;

Це дозволяє стверджувати, що використання перерахованих результатів наукових досліджень О.А. Замули, отриманих при роботі над дисертацією, дозволить підвищити скритність функціонювання та завадостійкість прийому сигналів розробляємих засобів зв'язку і передачі даних.

Акт розглянуто та схвалено на засіданні НТР ДП «ЦКБ «Протон», протокол № 14 від 22.09.2015 р.

Голова комісії:
головний науковий співробітник к.т.н. доцент Петров В. Л.

Члени комісії:
головний науковий співробітник к.т.н. Голобородько Ю.М

головний науковий співробітник к.т.н. с.н.с. Писарьонок Г.Г.

головний конструктор ДКР Повтарєв В.І.

С.Г. Рассомахін

«Затверджую»
Перший проректор з наукової роботи
Харківського національного
університету імені В. Н. Каразіна

_____ В.О. Катрич
24. 09. 2015 р.

АКТ
використання результатів докторської дисертаційної роботи
Замули Олександра Андрійовича

Комісія у складі зав. кафедри безпеки інформаційних систем і технологій (БІСТ) Рассомахіна Сергія Генадійовича, професора кафедри БІСТ Громико Ігоря Олексійовича та доцента кафедри БІСТ Сватовського Ігоря Івановича склала цей акт про використання наукових результатів докторської дисертації Замули О.А. в навчальному процесі.

При викладанні дисциплін "Управління інформаційною безпекою", "Комплексні системи захисту інформації: проектування, впровадження, супровід", "Нормативно-правове забезпечення інформаційної безпеки" використано такі наукові результати дисертаційної роботи:

1. Концепція і політика забезпечення інформаційної безпеки в телекомунікаційних системах. Принципи забезпечення безпеки інформації в телекомунікаційних системах.

2. Критерії і показники захищеності інформації в телекомунікаційних системах.

3. Моделі загроз інформаційної безпеки в телекомунікаційних системах. Методи захисту інформації в телекомунікаційних системах.

Зав. кафедри БІСТ, д.т.н., доцент. С.Г. Рассомахін

професор кафедри БІСТ к.т.н., доцент І.О. Громико

доцент кафедри БІСТ к.т.н., доцент І.І. Сватовський

"ЗАТВЕРДЖУЮ"
Проректор Харківського національного університету імені В.Н. Каразіна

д.т.н., професор _____ В.О. Катрич

"25" 09 2015р.

"ЗАТВЕРДЖУЮ"
Виконавчий директор Приватного акціонерного товариства "Інститут інформаційних технологій"

_____ В.Д. Кравченко

"28" 09 2015р.

АКТ

використання наукових результатів докторської дисертаційної роботи

ЗАМУЛИ ОЛЕКСАНДРА АНДРІЙОВИЧА

Комісія у складі: голови – доктора технічних наук, професора Потія О.В. та членів комісії: доктора технічних наук, професора Олійникова Р.В., кандидата технічних наук, професора Качко О.Г., склала цей акт про використання наукових результатів докторської дисертаційної роботи, що отримані доцентом кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна Замулою Олександром Андрійовичем в Приватному акціонерному товаристві "Інститут інформаційних технологій" (згідно договору № 0003/01-15 від 01.09.15). Комісія з'ясувала наступне.

1. Фахівцями Приватного акціонерного товариства "Інститут інформаційних технологій" використані такі наукові результати дисертаційної роботи Замули Олександра Андрійовича:

- Метод синтезу нелінійних криптографічних дискретних сигналів, який використовує випадкові і псевдовипадкові процеси, і створює послідовності символів (сигналів) певного алфавіту, які задовольняють вимогам незворотності, нерозрізненості, непередбачуваності і володіють необхідними ансамблевими та кореляційними властивостями, що дозволяє поліпшити завадозахищеність, імітостійкість, скритність телекомунікаційної системи, а також завадостійкість прийому сигналів в умовах впливу структурних, загороджувальних, ретрансльованих та інших видів перешкод.
- Удосконалений метод синтезу нелінійних дискретних сигналів із заданими ансамблевими, кореляційними і структурними властивостями, що задовольняють вимогам незворотності, нерозрізненості, непередбачуваності, і відрізняється від відомого методу тим, що використовує механізм спрямованого (обмеженого) перебору, для відбору сигналів із заданими властивостями, що дозволяє підвищити продуктивність синтезу системи сигналів.

• Удосконалений метод синтезу ансамблю сигналів, який відрізняється від відомого тим, що використовує залежність індексів і елементів кінцевого поля, що підвищує швидкодію процесу синтезу сигналів і, таким чином дозволяє здійснювати синтез сигналів в реальному часі при реалізації динамічного режиму передачі даних користувачів телекомунікаційної системи.

• Методи табличної реалізації модульних операцій в медулярній системі числення (МСС) з використанням спеціального коду табличного представлення операндів, які дозволяють, залежно від величини l-байтового (l = 1,4, 8) машинного слова, наприклад, при виконанні операції модульного множення від 64 до 4096 разів скоротити час виконання операцій, в порівнянні з використанням суматорних методів в позиційній системі числення.

• Алгоритми для реалізації розроблених і вдосконалених методів синтезу систем НС, швидкої реалізації модульних операцій, відповідно до яких синтезований клас апаратних засобів формування і обробки сигналів в телекомунікаційних системах, на які отримано 12 патентів України, що підтверджує світову новизну і практичну значимість отриманих наукових результатів роботи.

• Комплекс програмних засобів, що дозволяє реалізувати методи синтезу та дослідження властивостей нових класів нелінійних сигналів. Такий комплекс дозволяє: генерувати криптографічні послідовності символів практично будь-якої тривалості; отримувати значення мінімальних і максимальних пелюстків функції кореляції; порівнювати отримані значення з відомими межами «щільної упаковки»; зчитувати відібрані сигнали, що задовольняють границям для відповідних кореляційних функцій; надавати обраним послідовностям унікальні ідентифікатори; досліджувати ансамблеві, статистичні та кореляційних властивостей синтезованих сигналів.

2. Зазначені наукові результати розглянуті та подані для використання при побудові телекомунікаційних систем. Отримані наукові результати докторської дисертаційної роботи є певним розвитком теорії та практики систем складних сигналів, криптографічного захисту інформації на рівні джерела складних сигналів. Використання наукових результатів докторської дисертації Замули О.А. дозволить забезпечити необхідний рівень завадозахищеності та інформаційної безпеки телекомунікаційних систем.

Голова комісії, доктор технічних наук, професор О.В. Потій

Члени комісії:
доктор технічних наук, професор Р.В. Олійников

кандидат технічних наук, професор О.Г. Качко