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 суматорного 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. Карази-на 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 ефективности 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.

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, R. 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.// I-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 телеко- мунікаційної 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 по- токов [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. Заму-

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.