*На правах рукописи*

СУЛИМОВ АМИР ИЛЬДАРОВИЧ

# ПРОСТРАНСТВЕННО-РАЗНЕСЕННАЯ ГЕНЕРАЦИЯ СОГЛАСОВАННЫХ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ФИЗИЧЕСКИХ СВОЙСТВ РАДИОКАНАЛОВ

Специальность: 05.12.04 – Радиотехника,
в том числе системы и устройства телевидения

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Казань – 2016

Работа выполнена на кафедре радиофизики Института физики
Федерального государственного автономного
образовательного учреждения высшего образования
«Казанский (Приволжский) федеральный университет»

**Научный руководитель:**

доктор физико-математических наук, доцент;
ФГАОУ ВО «Казанский (Приволжский) федеральный университет»,
заведующий кафедрой радиофизики
**Шерстюков Олег Николаевич**

**Официальные оппоненты:**

доктор физико-математических наук, профессор;
ФГБОУ ВО «Марийский государственный университет»,
проректор по научной работе и инновационной деятельности
**Леухин Анатолий Николаевич**

доктор физико-математических наук, профессор;
ФГБОУ ВО «Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ»,
заведующий кафедрой радиоэлектронных и телекоммуникационных систем
**Надеев Адель Фирадович**

**Ведущая организация:**

ФГАОУ ВО «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского», г. Нижний Новгород

Защита диссертации состоится «20» декабря 2016 г. в 14 часов 30 минут на заседании диссертационного совета Д 212.081.18 в ФГАОУ ВО «Казанский (Приволжский) федеральный университет». По адресу: 420111, г. Казань, ул. Кремлевская, д. 16а, Институт физики.

С диссертаций можно ознакомиться в научной библиотеке ФГАОУ ВО «Казанский (Приволжский) федеральный университет».

Автореферат разослан «____» _____ 2016 г.

Ученый секретарь
диссертационного совета Д 212.081.18,
к.ф.-м.н., доцент А.Д. Акчурин

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования**

Пространственно-разнесённая генерация согласованных случайных последовательностей может найти широкое применение в различных областях современной науки и техники, в частности, для решения задач по защите информации в информационно-телекоммуникационных системах. К настоящему времени наиболее эффективным методом её защиты является шифрование [1]. К сожалению, активно используемые асимметричные шифры с открытым ключом обеспечивают лишь ограниченную стойкость к взлому, поскольку вскрываются за конечное время при наличии достаточной вычислительной мощности. Значительный прогресс в совершенствовании вычислительных средств, наблюдающийся на протяжении последних десятилетий, неуклонно снижает целесообразность их применения.

С другой стороны, К. Шенноном доказана [2] возможность создания *абсолютно стойких* систем шифрования на базе симметричных шифров с секретным ключом. Для этого достаточно, чтобы каждое передаваемое сообщение шифровалось одноразовым секретным ключом, длина которого должна быть не меньше длины сообщения. Таким образом, создание систем шифрования с абсолютной стойкостью сопряжено с необходимостью непрерывной генерации и безопасного распределения новых секретных ключей. Техническое решение данной задачи возможно путём пространственно-разнесённой генерации согласованных случайных последовательностей, используемых в качестве ключей шифрования.

Исторически первой системой пространственно-разнесённой генерации общей для двух корреспондентов случайной последовательности можно считать систему квантового распределения ключей (КРК) [3]. Проблематикой данных систем занимается бурно развивающееся направление – «квантовая криптография». Несмотря на очевидные успехи, достигнутые в данной области, отмечаются [4] и существующие недостатки этого метода, снижающие достижимую на практике безопасность распределения ключей. К техническим недостаткам систем КРК следует отнести и относительно невысокую дальность действия, достигающую 307 *км* при условии использования высококачественной оптико-волоконной линии связи [5]. Техника систем КРК всё ещё остаётся достаточно дорогостоящей и сложной в её техническом сопровождении. Кроме того, существуют значительные технические затруднения при реализации квантового распределения ключей, например, в мобильных системах связи.

Указанные недостатки систем КРК делают актуальным разработку и обоснование альтернативных способов пространственно-разнесённой генерации согласованных случайных последовательностей. В качестве таковых могут выступать беспроводные *радиотехнические* способы, основанные на физических свойствах стохастических радиоканалов со случайной траекторией распространения сигнала. Необходимые физические свойства проявляются, например, в системах метеорной радиосвязи, а также в системах связи в условиях многолучевой среды городской застройки. При этом физические свойства метеорного распространения радиоволн могут обеспечить возможность генерации в двух пунктах связи общей случайной последовательности при их разнесении на расстояния до 1500 *км*. Физические свойства многолучевого распространения радиоволн в условиях городской застройки могут позволить решать эти задачи в мобильных приложениях.

**Объектом исследования** являются физические свойства радиоканалов со стохастическими характеристиками, обладающими хотя бы приближённой взаимностью, а также различные аспекты их применения для осуществления пространственно-разнесённой генерации согласованных случайных последовательностей.

**Цель работы:** разработка теоретических основ радиотехнических систем пространственно-разнесённой генерации согласованных случайных последовательностей, основанных на случайности параметров принимаемого сигнала, распространяющегося через взаимный радиоканал со стохастическими характеристиками; а также теоретическое обоснование систем пространственно-разнесённой генерации случайных последовательностей, основанных на физических свойствах метеорного распространения радиоволн и многолучевого распространения в урбанизированной среде городской застройки.

Достижение заявленной цели потребовало решения следующих **задач:**

1. Разработка методов и процедур обработки сигналов и преобразования измеренных данных для синхронной генерации в двух пунктах связи общей случайной последовательности;
2. Разработка математической модели радиотехнических систем пространственно-разнесённой генерации согласованных случайных последовательностей (систем ПРГССП);
3. Разработка и реализация имитационных моделей исследуемых радиоканалов, обеспечивающих имитацию процессов пространственно-разнесённой генерации в двух и более пунктах связи согласованных случайных последовательностей, включая имитацию вариаций амплитудно-фазовых характеристик сигнала при его прохождении через стохастическую среду распространения с учётом невзаимности и нестационарности канала, а также в условиях разнесённого радиоприёма;
4. Теоретическое обоснование реализуемости систем радиометеорной ПРГССП;
5. Теоретическое обоснование реализуемости фазовых систем ПРГССП, основанных на случайности траектории распространения сигнала в многолучевых средах.

**Научная новизна** работы заключается в предлагаемых способах использования физических свойств радиоканалов для решения задач пространственно-разнесённой генерации согласованных случайных последовательностей и определяется следующими положениями:

1. Обобщена методика пространственно-разнесённой генерации согласованных случайных последовательностей на основе физических свойств взаимных радиоканалов, что позволило добиться её универсальности по отношению к физической природе используемого радиоканала;

2. Впервые разработана единая методологическая основа для оценки базовых функциональных характеристик и оптимизации параметров радиотехнических систем ПРГССП, учитывающая нестационарность и неабсолютную взаимность используемых стохастических радиоканалов. Предложена математическая модель радиотехнических систем ПРГССП, формализующая разработанную методологию;

3. Впервые реализована имитационная модель метеорного радиоканала, учитывающая полный комплекс явлений, обусловливающих невзаимность и нестационарность канала, в том числе при организации разнесённого приёма. Впервые реализована имитационная модель локально стационарного многолучевого радиоканала, позволяющая имитировать процессы синхронной ПРГССП при перемещении устройств связи в условиях городской застройки, в том числе при организации на обеих сторонах радиоканала разнесённого приёма;

4. Впервые на единой методологической основе исследована проблема пространственно-разнесённой генерации согласованных случайных последовательностей на основе фазово-временных характеристик метеорных радиоотражений. В результате, установлено влияние основных физических факторов стохастичности метеорного радиоканала на коррелированность фазово-временных характеристик и задержек на время распространения сигнала двух последовательно регистрируемых метеорных радиоотражений. Впервые произведена оценка статистических характеристик генерируемой радиометеорным способом общей (для двух заданных пунктов связи) случайной последовательности, а также оценка производительности системы радиометеорной ПРГССП с учётом нестабильности и невзаимности метеорного радиоканала;

5. Впервые на единой методологической основе исследована проблема пространственно-разнесённой генерации согласованных случайных последовательностей на основе фазово-временных характеристик многолучевых радиоканалов. В результате, установлены закономерности, отражающие влияние основных технических характеристик связной аппаратуры, физических характеристик городской среды распространения, характера относительного перемещения устройств связи и процедуры обработки измеренных данных на функциональные характеристики систем ПРГССП, использующих стохастичность многолучевого распространения. Впервые произведена оценка статистических характеристик общей (для двух заданных пунктов связи) случайной последовательности, генерируемой на основе фазово-временной характеристики многолучевого радиоканала.

**<u>На защиту выносятся следующие положения:</u>**

1. Методы и процедуры пространственно-разнесённой генерации согласованных случайных последовательностей (ПРГССП), основанные на измерении случайных параметров сигнала, зондирующего взаимный радиоканал со стохастическими характеристиками;

2. Математическая модель радиотехнической системы ПРГССП;

3. Имитационные модели исследованных радиоканалов: *а*) усовершенствованная имитационная модель метеорного радиоканала, учитывающая полный комплекс явлений, обусловливающих невзаимность и нестационарность канала, в том числе при организации разнесённого приёма; *б*) имитационная модель локально стационарного многолучевого радиоканала, позволяющая имитировать процессы синхронной ПРГССП при перемещении устройств связи в условиях городской застройки, в том числе при организации на обеих сторонах радиоканала разнесённого приёма;

4. Теоретическое обоснование реализуемости систем радиометеорной ПРГССП, включая оценки основных её функциональных характеристик;

5. Теоретическое обоснование реализуемости фазовых систем ПРГССП, опирающейся на случайность траектории распространения сигнала в многолучевых средах, обладающих свойством хотя бы приближённой взаимности, включая оценки их основных функциональных характеристик.

**Достоверность результатов** работы подтверждается их логической непротиворечивостью, сравнением с аналогичными результатами, полученными другими исследователями, экспериментальной проверкой разработанной теории и методов, проверкой работоспособности разработанных методов с помощью теоретических расчётов и имитационного моделирования, проверкой адекватности разработанных имитационных моделей путём сопоставления результатов моделирования с результатами натурных экспериментов, применением современных и надёжных методик обработки данных, проведением корректных математических расчётов и анализа.

**Теоретическая и практическая значимость** результатов работы определяется возможностью создания систем шифрования с близкой к совершенной по Шеннону стойкостью [2]. Реализация генерации и распределения ключей шифрования на основе физических свойств радиоканалов принципиально решает проблему распределения ключей в системах симметричного шифрования [1]. В результате, открывается возможность создания систем симметричного шифрования с непредсказуемо изменяющимся во времени ключом, превосходящих по своей стойкости современные системы с фиксацией ключа шифрования на длительном интервале работы.

Работа носит теоретический характер, однако разработанные в её рамках теоретические положения могут служить в качестве технических рекомендаций при проектировании радиотехнических систем ПРГССП, а также закладывают основы по реализации аппаратуры для данных систем.

По результатам диссертационного исследования автором получено 3 патента Российской Федерации на изобретение.

**Апробация работы.** Основные положения и результаты работы докладывались и обсуждались на следующих семинарах и конференциях: XI Международная конференция по информационной безопасности и криптографии «SECRYPT-2014» (Вена, Австрия, 2014), XII Международная конференция по информационной безопасности и криптографии «SECRYPT-2015» (Кольмар, Франция, 2015), X Международная IEEE Сибирская конференция по управлению и связи «SIBCON-2013» (Красноярск, Россия, 2013), XI Международная IEEE Сибирская конференция по управлению и связи «SIBCON-2015» (Омск, Россия, 2015), XXIII Всероссийская научная конференция по распространению радиоволн (Йошкар-Ола, 2011), XXIV Всероссийская научная конференция по распространению радиоволн (Иркутск, 2014), III Международная научно-практическая конференция «Научно-техническое творчество молодежи» (Москва, 2011), Международная научно-практическая конференция «Роль неправительственных научно-общественных организаций в решении проблем, связанных с разработкой и внедрением инновационных технологий во все сферы человеческой деятельности» (Казань, 2009), Слёт изобретателей и рационализаторов Республики Татарстан (Казань, 2011), Ежегодная итоговая научная конференция Казанского (Приволжского) федерального университета (Казань, 2010, 2011, 2012, 2013, 2014, 2015).

**Публикации.** По теме диссертации опубликовано 19 работ, включая 3 статьи, 7 работ по итогам международных конференций, 6 тезисов докладов конференций, 3 патента РФ на изобретение. Из них 2 работы опубликованы в журналах из перечня ВАК РФ, 6 работ проиндексированы в международных реферативных базах данных Scopus и Web of Science.

**Личный вклад автора.** Основные результаты диссертационной работы получены автором лично. Автору принадлежат найденные решения поставленных задач и их реализация. В публикациях, подготовленных в соавторстве, автору диссертации принадлежат следующие результаты: разработка теоретических основ систем радиотехнической ПРГССП, включая методы и алгоритмы обработки измеренных данных и генерации случайных последовательностей, методика оценки характеристик систем ПРГССП, разработка и реализация компьютерных имитационных моделей радиоканалов, разработка и реализация блока электродинамических расчётов, алгоритмов пассивной фазовой пеленгации при разнесённом приёме сигналов, анализ физических свойств радиоканалов и процессов распространения радиоволн в средах, анализ и обработка экспериментальных данных, проведение численных оценок. Автор принимал активное участие в планировании работ и интерпретации результатов экспериментов по реализации пространственно-разнесённой генерации согласованных случайных последовательностей, основанной на физических свойствах многолучевого распространения радиоволн.

**Структура и объём работы.** Диссертация состоит из введения, 4-х глав, заключения, 6-ти приложений, списка сокращений, списка литературы. В работе содержатся 243 страницы печатного текста, 91 рисунок, 13 таблиц, список литературы, содержащий 155 библиографических наименований.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрена актуальность темы диссертационной работы, сформулирована цель работы и задачи исследования; приведены положения, выносимые на защиту; показаны научная новизна и практическая значимость, обоснована достоверность полученных результатов; а также описана структура диссертационной работы.

### Первая глава

Первая глава посвящена обзору уровня современных исследований в области физических и радиотехнических способов пространственно-разнесённой генерации согласованных случайных последовательностей. Подчёркивается актуальность разработки и внедрения систем ПРГССП для повышения стойкости симметричных систем шифрования.

### Вторая глава

Во второй главе излагается обобщенная математическая модель системы ПРГССП, основанной на физических свойствах радиоканала. В данной главе рассматривается общая методика передачи, приёма и обработки зондирующих сигналов для формирования у заданной пары пунктов связи двух экземпляров общей случайной последовательности (ОСП), излагаются методы оптимизации параметров процедуры ПРГССП.

Методика формирования двух экземпляров ОСП у заданной пары абонентов представлена блок-схемой на рис. 1. Пункты связи обмениваются серией зондирующих сигналов (ЗС), в качестве которых могут быть использованы радиоимпульсы большой длительности. Передатчик (пункт $A$) излучает полностью детерминированный радиосигнал, информационный параметр $X$ (например, фаза или задержка по времени) которого принимает известное значение $x_0$. На выходе взаимного радиоканала со случайными физическими характеристиками (например, со случайной траекторией распространения) параметр $X$ становится случайной величиной с распределением вероятностей $w(x)$, определяемым физическими свойствами радиоканала. Иными словами, канал осуществляет стохастическую модуляцию параметра зондирующего сигнала $X$. При этом взаимность канала понимается здесь как его обратимость, подразумевающая инвариантность параметров принятого сигнала относительно направления передачи.

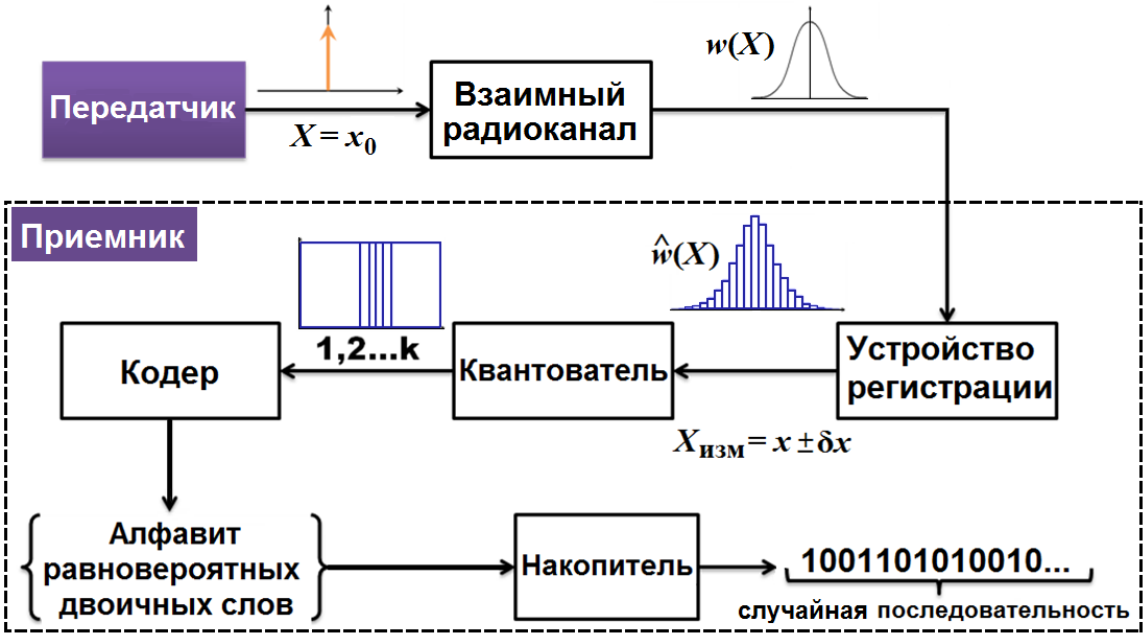



Рис. 1 – Блок-схема формирования общей случайной последовательности

Измерения $\{x_B\}$ случайной величины $X$ на приёмном конце (в пункте $B$) представляют собой природный источник случайности, используемый для формирования одного экземпляра ОСП. Второй экземпляр формируется в пункте $A$ в силу взаимности радиоканала, обеспечивающей равенство измерений параметра $\{x_B\}$ и $\{x_A\}$ с точностью до разрешающей способности $\delta x$. Для формирования из измеренных данных $\{x_B\}$ и $\{x_A\}$ двух идентичных экземпляров ОСП пункты $A$ и $B$ регулярно посылают друг другу ЗС во встречных направлениях, подвергая их одинаковой обработке при приёме.

Устройство регистрации сигналов искажает исходную форму распределения $w(x)$ из-за наличия порога регистрации $U_0$ и ограниченной разрешающей способности $\delta x$ по параметру $X$. В пределах заданной разрешающей способности пункты $A$ и $B$ регистрируют одинаковые отсчёты наблюдаемого параметра $X$: $\delta x = | x_A - x_B |$. Основными причинами её ограничения являются: инструментальные погрешности измерительной аппаратуры $\delta x_{инстр}$ (например, погрешность синхронизации), шумовые погрешности $\delta x_ш$ и невзаимность среды распространения $\delta x_{НВ}$. В силу статистической

независимости указанных причин, суммарное рассогласование измерений $x_A$ и $x_B$ записывается в форме:

$$\delta x = \sqrt{\delta x_{инстр}^2 + \delta x_{ш}^2 + \delta x_{нв}^2} \ . \qquad (1)$$

На выходе устройства регистрации наблюдается гистограмма $\hat{w}(x)$ распределения параметра $X$, образующаяся путем дискретизации исходного распределения $w(x)$ с шагом $\Delta x = 2\max(\delta x)$. В общем случае, гистограмма $\hat{w}(x)$ неравномерна. Непосредственное применение измеренной выборки к формированию ОСП приводит к неудовлетворительным статистическим характеристикам последней. Воизбежание этого, выборку предварительно подвергают неравномерному квантованию с компенсирующей сеткой уровней квантования (рандомизируют), чем обеспечивают равномерность гистограммы распределения параметра $X$ на выходе квантователя.

Таким путём, на выходе квантователя образуется гистограмма с $k$ одинаковыми по высоте, но неравными по ширине столбцами. При этом попадание результата $x$ очередного измерения параметра $X$ в любой из $k$ интервалов равновероятно. Кодер сопоставляет каждому интервалу уникальный двоичный код $\mathrm{W}_j$, $(j = \overline{1,k})$, образуя на выходе ансамбль из $k$ равновероятных двоичных слов. Математическими преобразованиями совокупности двоичных эквивалентов измерений $X$ формируют экземпляр общей случайной последовательности $K$ необходимой длины.

Может быть рекомендована следующая последовательность операций при обработке накопленной выборки параметра $\{X\}$ и формировании ОСП:

1) отсеивание измерений по признакам невзаимности;
2) декорреляция выборки;
3) равномерное квантование измерений;
4) неравномерное квантование измерений (рандомизация выборки);
5) кодирование измерений.

С теоретико-информационной точки зрения, предельная скорость генерации ОСП определяется формулой:

$$R_K = I(X_A; X_B) \cdot F, \qquad (2)$$

где $I(X_A; X_B) = H(X) - H(X_A \mid X_B)$ есть количество взаимной информации между измерениями сторон, а $F$ [*Гц*] – предельная частота снятия измерений параметра $X$. Частота $F$ может ограничиваться сверху, например, взаимной корреляцией последовательных измерений (имеет место в многолучевых средах) или прерывистым характером канала (имеет место при метеорном распространении радиоволн). Энтропия параметра $H(X)$ также определяется физическими свойствами радиоканала. Условная энтропия $H(X_A \mid X_B)$ отражает влияние ограниченной разрешающей способности $\delta x$ и факторов рассогласования измерений пунктов $A$ и $B$ на производительность системы ПРГССП.

Вследствие наличия уклонения $\delta x$ измерений параметра $X$, выполняемых пунктами $A$ и $B$, возможно возникновение битовых ошибок при пространственно-разнесённой генерации экземпляров ОСП. Для их устранения необходимо ввести процедуру сверки симметричности экземпляров ОСП $K_A$ и $K_B$, генерируемых

сторонами. Сверка экземпляров влечёт за собой некоторые потери в скорости генерации ОСП по причине отбраковки фрагментов последовательности, содержащих асимметричные биты. Таким образом, введение сверки экземпляров снижает эффективность η преобразования измеренных данных в двоичную ОСП. С учётом этого, фактическая скорость генерации ОСП может быть определена следующим образом:

$$R_K = \frac{\eta \cdot m \cdot N}{n_0 \cdot T}, \qquad (3)$$

где $N$ – объём накопленной за время $T$ выборки измерений наблюдаемого параметра сигнала $X$, $n_0$ – шаг декорреляции выборки и $m$ – разрядность кодирования измерений. Сравнивая формулы (2) и (3) можно заметить, что $F = N/(n_0 \cdot T)$ и $I(X_A; X_B) = \eta m$. Эффективность η($m$) является функцией разрядности $m$, поэтому возможна оптимизация параметров процедуры генерации ОСП путём подбора оптимальной разрядности кодера: $m = m^*$.

В рамках разработанной математической модели систем ПРГССП введены критерии и предложены соответствующие целевые функции для поиска оптимальной разрядности кодирования измерений $m^*$. Также предложены методы оптимизации шага декорреляции выборки $n_0$ и формулы для расчёта эффективности η. Показана работоспособность разработанных методов оптимизации на примере обработки измерений случайной фазы несущей ЗС.

**Третья глава**

В третьей главе излагаются теоретические основы и результаты оценок основных функциональных характеристик радиометеорной системы ПРГССП, опирающейся на использование случайности траектории распространения сигнала в метеорном радиоканале (МРК). В этой главе описываются принципиальные (для целей ПРГССП) физические свойства метеорного радиоканала, излагается теоретическая основа воспроизводящей их имитационной модели МРК, анализируются статистические характеристики генерируемой ОСП, производятся оценки её скорости генерации, а также исследуется влияние базовых физических характеристик МРК на производительность систем радиометеорной ПРГССП.

Имитационное моделирование характеристик регистрируемых метеорных радиоотражений (МРО) производилось на основе численного решения строгой задачи дифракции радиоволн на метеорном следе [6]. Учитывался полный комплекс поляризационных явлений при метеорном распространении радиоволн, включая случайную ориентацию метеорного следа в пространстве, вращение плоскости поляризации радиоволн за счёт эффекта Фарадея в магнитоактивной плазме ионосферы Земли, а также поляризационные характеристики антенн и электрические свойства подстилающей поверхности.

При оценке скорости генерации ОСП предполагалось, что в МРК действуют два основных физических фактора, ограничивающих достижимую величину $R_K$: неабсолютная взаимность канала и ограниченная интенсивность регистрации МРО. Оценка интенсивности регистрации МРО производилась с помощью компьютерной имитационной модели «КАМЕТ» [7]. В качестве тестовой использовалась типичная метеорная радиолиния (Москва-Казань) протяжённостью 720 *км* со следующими параметрами:

- эпоха моделирования: июнь, 6:00 по местному времени;
- несущая частота: $f = 50$ *МГц*;
- мощность передатчика: $P_T = 5000$ *Вт*;
- порог регистрации: $U_0 = 0{,}5$ *мкВ* (минус 185 *дБ*);
- тип антенн: пятиэлементный «волновой канал»;
- поляризация антенн: горизонтальная;
- требуемое отношение (сигнал/шум): $SNR = 20$ *дБ*;
- минимальная генерируемая масса метеороидов: $m_0 = 3 \cdot 10^{-5}$ *г*;
- СКО турбулентной составляющей скорости ветра: $\sigma_V = 25$ *м/с*;
- объём выборки: $N = 20000$ метеорных радиоотражений.

На рис. 2 представлены зависимости средней скорости генерации ОСП фазовым методом от разрядности кодирования измерений $m$, смоделированные для тестовой радиолинии при трёх уровнях (сигнал/шум). Средняя часовая численность регистрируемых МРО составила $N_Ч = 417$. Вследствие высокой невзаимности канала оптимальная разрядность кодирования $m^*$ не превышала 1-2 *бит/изм*.

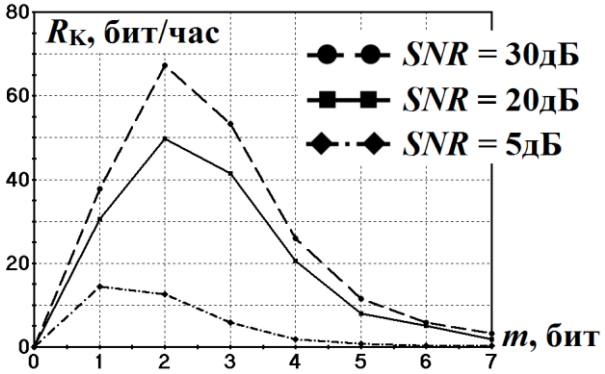
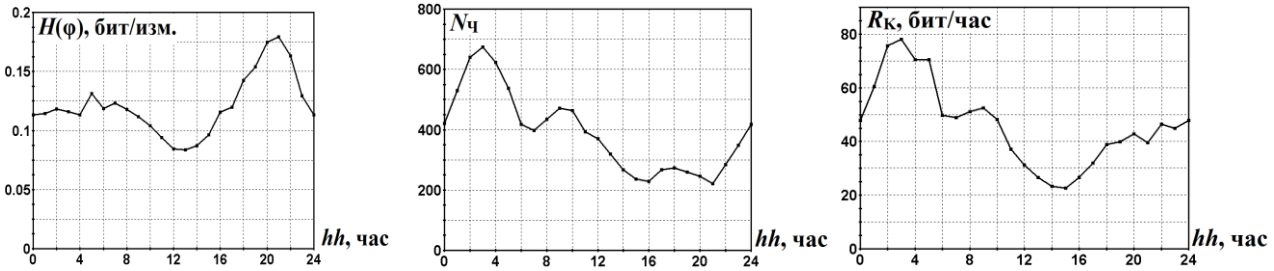



Рис. 2 – Скорость радиометеорной генерации общей случайной последовательности

С ростом рассогласования измерений сторон оптимальная разрядность кодирования $m^*$ смещается в область малых значений. Попытка установить разрядность кодирования выше $m^*$ приводит к резкому росту доли асимметричных битов в генерируемых сторонами экземплярах ОСП, что существенно снижает эффективность $\eta(m)$. Доля асимметричных битов составила: $p_e = 7{,}9$ % ($SNR = 30$ *дБ*, $m^* = 2$), $p_e = 8{,}6$ % ($SNR = 20$ *дБ*, $m^* = 2$) и $p_e = 8{,}0$ % ($SNR = 5$ *дБ*, $m^* = 1$). Для их устранения производилась сверка экземпляров ОСП циклическими избыточными кодами стандарта *CRC*-16-*CCITT*. Высокая доля асимметричных битов привела к низкой эффективности генерации ОСП: $\eta < 10$ %, что приводило к «потере» свыше 90 % выборки на этапе сверки симметрии экземпляров ОСП. Исходя из этого, достигнутая скорость $R_K$ генерации ОСП не превосходила 70 *бит*/*час*.

Спецификой МРК, обусловленной его астрономической природой, является глубокий суточный ход характеристик канала. Результаты моделирования суточных зависимостей, полученные при $SNR = 20$ *дБ*, представлены на рис. 3. На рис. 3*а* представлена суточная зависимость удельной информационной ёмкости (энтропии) одного измерения фазы несущей сигнала: $H(\varphi) = \eta(m^*) \cdot m^*$, обусловленная суточными колебаниями уровня невзаимности канала. На рис. 3*б* представлена суточная зависимость часовой численности регистрируемых МРО. Из рис. 3 очевидно, что скорость генерации ОСП в подавляющей степени определяется




*а*) *б*) *в*)

Рис. 3. – Суточная зависимость скорости генерации ОСП

регистрируемой численностью МРО, то есть энергетическим потенциалом радиолинии.

Скорость генерации ОСП варьировалась в пределах от 22,7 *бит/час* (15 часов по м.в.) до 78,1 *бит/час* (3 часа по м.в.) при среднесуточном значении 46,2 *бит/час*. Максимальная суточная выработка общей случайной последовательности для тестовой радиолинии (Москва-Казань) составила 1154 *бит/сутки*. Оценка остаточной вероятности битовой ошибки $p_b$ (после сверки экземпляров ОСП) не превосходила $2{,}8 \cdot 10^{-6}$, что согласуется с теоретическими оценками надёжности циклических избыточных кодов.

**Четвёртая глава**

В четвёртой главе излагаются теоретические основы и результаты оценок основных функциональных характеристик систем ПРГССП, опирающихся на использование случайности траектории распространения сигнала в многолучевых средах, обладающих свойством хотя бы приближённой взаимности. В этой главе описываются принципиальные (для целей ПРГССП) физические свойства локально стационарного многолучевого канала, излагается теоретическая основа воспроизводящей их имитационной модели, рассматривается влияние физических характеристик канала на скорость генерации ОСП, а также анализируются статистические характеристики ОСП, генерируемой фазовым методом.

При разработке имитационной модели многолучевого радиоканала в условиях городской застройки за основу была принята геометрическая модель Пономарёва-Куликова-Тельпуховского [8]. Разработанная модель имитирует двустороннюю передачу зондирующих сигналов между стационарным пунктом (БС – базовой станцией) и мобильным терминалом (МТ), хаотически перемещающимся в пределах городской застройки. Модель имеет динамический характер в том смысле, что имитирует изменения фазы, амплитуды, многолучевой структуры сигнала и характеристик радиоканала в «реальном масштабе» времени наблюдения по мере перемещения МТ. При этом имитируется комплексная картина замираний сигнала, процессы возникновения и исчезновения рассеивателей, порождающих относительно точки приёма ЗС парциальные волны.

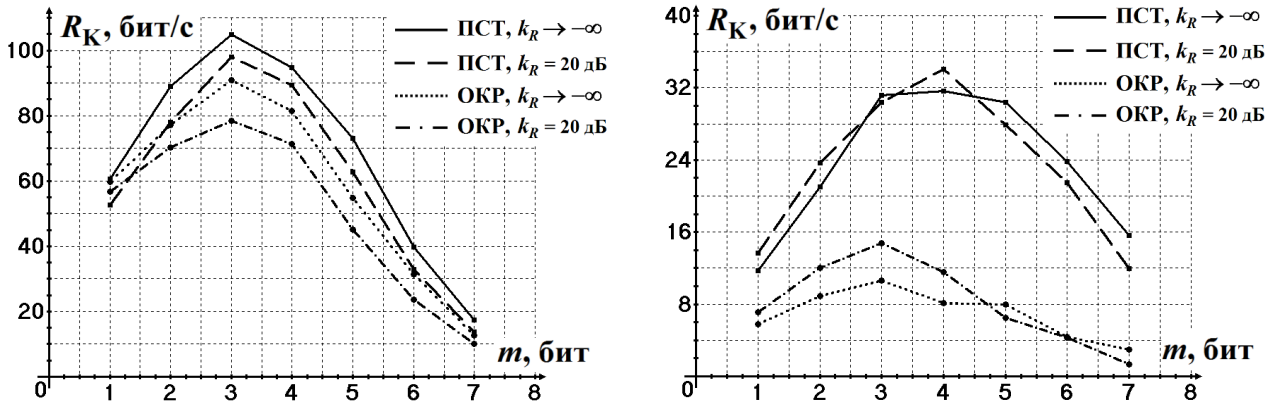
При оценке скорости генерации ОСП в качестве тестовой использовалась радиолиния с типичными для городской среды параметрами:

- частота несущей: $f = 1000$ *МГц*;
- мощность передатчика БС: $P_T = 2$ *Вт*;
- мощность передатчика МТ: $P_{T\_обр} = 0{,}25$ *Вт*;
- начальная длина радиолинии: $D = 350$ *м*;
- требуемое отношение (с/ш): $SNR = 20$ *дБ*;

- логарифмический порог регистрации сигналов: $U_0$ = -50 *дБ*;
- среднее количество парциальных лучей: $\overline{n} = 12$;
- средняя плотность городской застройки: ν = 90 *зданий*/*км*$^2$;
- высота подвеса антенны БС: $z_1$ = 30 *м*;
- высота подвеса антенны МТ: $z_2$ = 1,5 *м*;
- средний уровень крыш: <*h*> = 20 *м*.

В ходе генерации ОСП на этапе 2 «декорреляция измерений» устанавливалась допустимая корреляция последовательных измерений $R_{1\,\text{пор}} = 0.3$, после чего находилось соответствующее ему значение шага декорреляции $n_0$. Вследствие неабсолютной симметрии фазовых измерений сторон, производилась сверка экземпляров ОСП с помощью циклических избыточных кодов стандарта *CRC*-16-*CCITT*.

Результаты проведённого моделирования представлены на рис. 4. Моделирование производилось для различных комбинаций из следующих множеств значений параметров канала: 1) скорость перемещения МТ – $V$ = {10 *м/с*; 1,4 *м/с*}; 2) интенсивность сигнала прямой видимости, характеризуемая коэффициентом Райса – $k_R$ = {-∞; 20 *дБ*}, 3) тип перемещения МТ: движение вокруг БС (на рисунках отмечено сокращением «ОКР») и перемещение по случайной траектории (на рисунках отмечено сокращением «ПСТ»).




*а*) $V$ = 10 *м/с* *б*) $V$ = 1,4 *м/с*

Рис. 4 – Скорость генерации ОСП при отношении (сигнал/шум): *SNR* = 20 *дБ*

Анализ результатов показал, что главным физическим фактором, ограничивающим скорость генерации ОСП, является канальный шум. Перемещение МТ по случайной траектории вызывает более высокую вариативность состояния канала, чем перемещение с сохранением протяжённости радиолинии. Возникновение интенсивной прямой волны снижает энтропию параметров многолучевого сигнала, что приводит к снижению скорости $R_K$. Оценки остаточной вероятности битовой ошибки при распределении экземпляров ОСП показали, что при указанных выше скоростях генерации ОСП она поддерживалась на уровне не более $1{,}0 \cdot 10^{-6}$.

В **заключении** диссертационной работы сформулированы основные научные результаты, полученные в ходе её выполнения.

В **приложениях** представлен материал вспомогательного характера.

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

В рамках данного диссертационного исследования были получены следующие результаты:

1. Разработаны методы и процедуры синхронной генерации в двух пунктах связи общей случайной последовательности (ОСП), универсальные по отношению к физической природе используемого радиоканала. Впервые сформулирован перечень физических свойств, которыми должен обладать радиоканал, для возможности реализации на его основе систем пространственно-разнесённой генерации согласованных случайных последовательностей (систем ПРГССП);

2. Разработана математическая модель радиотехнических систем ПРГССП, на основе которой получены следующие результаты:

• показано, что принципиальные ограничения на производительность систем ПРГССП накладывает неабсолютная взаимность используемого радиоканала;

• предложены сеансовые протоколы дуплексной и полудуплексной передачи зондирующих сигналов, регламентирующие порядок активности сторон, что имеет непосредственное практическое значение;

• предложены методы оптимизации процедуры обработки измерений и формирования ОСП. Продемонстрирована работоспособность предложенных методов оптимизации на примере радиоканалов с неабсолютной взаимностью и нестационарностью;

• для ряда наиболее широко распространённых аналитических моделей автокорреляционной функции наблюдаемого параметра сигнала определён оптимальный шаг декорреляции выборки;

• рассмотрено применение метода циклических избыточных кодов для контроля симметричности экземпляров ОСП, генерируемых заданной парой пунктов связи. Найдена оптимальная длина сверяемого фрагмента ОСП;

• показано, что внедрение процедуры сверки симметричности экземпляров ОСП снижает скорость её генерации;

• установлена взаимосвязь четырёх основных характеристик согласованности экземпляров ОСП для случая равномерного распределения наблюдаемого стохастического параметра сигнала. Это даёт возможность проведения на практике оперативной селекции измеренных данных для более эффективной генерации ОСП;

• разработаны следующие *технические рекомендации* при практической реализации систем ПРГССП: 1) использовать рандомизацию выборки в качестве обязательного этапа формирования ОСП; 2) периодически обновлять сведения о вероятностных свойствах уклонения накапливаемых сторонами выборок измерений наблюдаемого параметра сигнала путём обмена серией тестовых сигналов;

3. Усовершенствована и реализована имитационная модель метеорного радиоканала, учитывающая полный комплекс явлений, обуславливающих невзаимность и нестационарность канала, в том числе при организации разнесённого приёма. Разработана и реализована имитационная модель локально стационарного многолучевого радиоканала, позволяющая имитировать процессы синхронной ПРГССП при перемещении устройств связи в условиях городской застройки, в том числе при организации на обеих сторонах радиоканала разнесённого приёма;

4. Теоретически обоснована реализуемость систем радиометеорной ПРГССП. В частности, получены следующие результаты:

• определено и формализовано понятие «невзаимного метеорного радиоотражения»;

• по результатам моделирования типичной метеорной радиолинии (Москва-Казань), технические характеристики которой представлены на с. 11, доля метеорных радиоотражений невзаимного типа варьировалась в пределах от 4,5 % до 11 % со средним значением 8 %. При этом среднеквадратическое отклонение остаточной фазовой невзаимности канала (при отбраковке всех радиоотражений невзаимного типа) варьировалась в пределах от 16° до 23°, что согласуется с результатами экспериментальных исследований [9];

• систематизирован перечень известных методов оперативного выявления и отбраковки невзаимных метеорных радиоотражений;

• доказана статистическая независимость выборочных отсчётов фазы несущей (а также времени метеорного распространения сигнала), измеренных для двух последовательно регистрируемых метеорных радиоотражений;

• показано, что сверка симметрии экземпляров ОСП при радиометеорной ПРГССП может привести к потере свыше 90 % от её исходного объёма;

• произведены оценки основных функциональных характеристик радиометеорной системы ПРГССП. Для тестовой радиолинии (Москва-Казань) оценка средней скорости генерации ОСП фазовым методом составила 1154 *бит/сутки* при вероятности битовой ошибки менее $2{,}8 \cdot 10^{-6}$. Пиковая скорость генерации ОСП составила порядка 80 *бит/час*;

• разработаны следующие *технические рекомендации* при практической реализации радиометеорных систем ПРГССП: 1) для оперативного выявления невзаимных метеорных радиоотражений отслеживать поляризацию принятой радиоволны; 2) для оценки момента наименьшей невзаимности канала отслеживать динамику его фазовой нестабильности; 3) отбраковывать метеорные радиоотражения с высокой фазовой нестабильностью; 4) исключить этап декорреляции выборки из процедуры формирования ОСП; 5) преимущественно использовать радиоотражения от недоуплотнённых метеорных следов; 6) производить подстройку параметров системы с учётом суточно-сезонных вариаций характеристик канала; 7) использовать частоты в диапазоне от 30 до 50 *МГц*; 8) при выборе мощности передатчика учитывать резко насыщающийся характер зависимости достигаемой скорости генерации ОСП.

Полученные оценки свидетельствуют о возможности использования систем радиометеорной ПРГССП для целей генерации и распределения ключей симметричного шифрования в заданной паре пунктов связи, разнесённых на расстояния до 1500 *км*;

5. Теоретически обоснована реализуемость фазовых систем ПРГССП, опирающихся на случайность траектории распространения сигнала в многолучевых средах. В частности, получены следующие результаты:

• показана неприменимость модели рэлеевского (в общем случае, райсовского) радиоканала к анализу процессов ПРГССП в средах со слабой (менее шести парциальных волн) многолучевостью;

• установлены закономерности изменения статистических характеристик генерируемой случайной последовательности и производительности системы

ПРГССП при вариации основных технических параметров многолучевого радиоканала (несущей частоты, скорости и траектории перемещения мобильных средств связи, амплитудного порога регистрации, отношения (сигнал/шум)) и физических характеристик многолучевой среды городской застройки (количества парциальных волн, интенсивности сигнала прямой видимости, плотности городской застройки);

• установлено, что зависимость временного интервала корреляции фазовых измерений $\Delta\tau_\varphi$ от допплеровой частоты $f_Д$ хорошо аппроксимируется гиперболой $\Delta\tau_\varphi(f_Д) = C(R_0) / f_Д$, где $C(R_0)$ – коэффициент, зависящий от заданной допустимой корреляции последовательных измерений $R_0$;

• повышение скорости генерации ОСП без ухудшения её статистических свойств возможно в условиях высокой ($f_Д > 25$ *Гц*) нестационарности канала;

• повышение (сигнал/шум) свыше 30 *дБ* нецелесообразно, поскольку не приводит к существенному снижению вероятности возникновения асимметричных битов. Нижняя граница вероятности битовой ошибки определяется степенью нестационарности (допплеровой частотой) радиоканала;

• установлено, что наличие интенсивного сигнала прямой видимости снижает скорость генерации ОСП;

• предложена процедура предварительной обработки накопленной выборки фазовых измерений, основанная на исключении резких скачков фазово-временной характеристики канала. Реализация данной процедуры позволяет примерно на 30 % повысить скорость генерации ОСП;

• для типичной тестовой радиолинии, характеристики которой представлены на с. 12, оценка скорости генерации ОСП в многолучевой среде демонстрировала пиковое значение порядка 157 *бит/с* (при отношении (сигнал/шум) равном 30 *дБ*) при вероятности битовой ошибки не более $1{,}0 \cdot 10^{-6}$;

• разработаны следующие *технические рекомендации* при практической реализации систем ПРГССП: 1) включить декорреляцию накопленной выборки измерений в перечень обязательных этапов формирования ОСП, использовать допустимую корреляцию соседних измерений фазы несущей сигнала не более 0,25; 2) не устанавливать амплитудный порог регистрации сигнала выше минус 15 *дБ* относительно медианного уровня; 3) использовать частоты в диапазоне от 500 до 3000 *МГц*, в указанном диапазоне увеличение частоты приводит к насыщающемуся повышению производительности системы ПРГССП; 4) подавлять сигнал прямой видимости либо обеспечивать случайность траектории перемещения средств связи и рассеивающих объектов в многолучевой среде; 5) повышение (сигнал/шум) свыше 30 *дБ* нецелесообразно; 6) исключать из выборки фрагменты фазово-временной характеристики канала, содержащие резкие скачки (например, свыше 20° по модулю); 7) при работе в средах со слабой многолучевостью (менее 10 парциальных волн) статистические характеристики генерируемой случайной последовательности резко ухудшаются.

Полученные оценки свидетельствуют о возможности использования систем многолучевой ПРГССП для целей генерации и распределения ключей симметричного шифрования между заданной парой устройств связи, например, в системах мобильной радиосвязи.

## ПУБЛИКАЦИИ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

*Публикации в рецензируемых источниках, рекомендованных ВАК РФ*

1. Сидоров, В.В. Метеорная генерация секретных ключей шифрования для защиты открытых каналов связи [Текст] / В.В. Сидоров, А.В. Карпов, **А.И. Сулимов** // Информационные технологии и вычислительные системы. – 2008. – №3. – с. 45-54.
2. **Сулимов, А.И.** Моделирование синхронной генерации криптографических ключей в метеорном радиоканале [Текст] / А.И. Сулимов, А.В. Карпов, О.Н. Шерстюков, В.В. Сидоров, Р.Г. Хузяшев // Ученые записки Казанского университета. Серия Физико-математические науки. – 2011. – Т. 153, кн. 4. – с. 167-175.
3. **Sulimov, A.I.** Simulation of encryption key distribution process based on a multipath radio propagation / A.I. Sulimov, O.N. Sherstyukov, A.V. Karpov, A.D. Smolyakov // Proceedings of X International IEEE Siberian Conference on Control and Communications (SIBCON-2013), Krasnoyarsk, Russia. – 2013. – pp. 1-4. (Web of Science, Scopus)
4. Smolyakov, A.D. Experimental verification of possibility of secret encryption keys distribution with a phase method in a multipath environment / A.D. Smolyakov, **A.I. Sulimov**, A.V. Karpov, O.N. Sherstyukov // Proceedings of X International IEEE Siberian Conference on Control and Communications (SIBCON-2013), Krasnoyarsk, Russia. – 2013. – pp. 1-5. (Web of Science, Scopus)
5. **Sulimov, A.I.** Experimental study of performance and security constraints on wireless key distribution using random phase of multipath radio signal / A.I. Sulimov, A.D. Smolyakov, A.V. Karpov, O.N. Sherstyukov // Proceedings of the 11th International Conference on Security and Cryptography (SECRYPT-2014), Vienna, Austria. – 2014. – pp. 411-416. (Scopus)
6. **Sulimov, A.** Secure key distribution based on meteor burst communications / A. Sulimov, A. Karpov // Proceedings of the 11th International Conference on Security and Cryptography (SECRYPT-2014), Vienna, Austria. – 2014. – pp. 445-450. (Scopus)
7. Smolyakov, A.D. Experimental extraction of shared secret key from fluctuations of multipath channel at moving a mobile transceiver in an urban environment / A.D. Smolyakov, **A.I. Sulimov**, A.V. Karpov, A.A. Galiev // Proceedings of the 12th International Conference on Security and Cryptography (SECRYPT-2015), Colmar, France. – 2015. – pp. 355-360. (Scopus)
8. **Sulimov, A.I.** Performance evaluation of meteor key distribution / A.I. Sulimov, A.V. Karpov // Proceedings of the 12th International Conference on Security and Cryptography (SECRYPT-2015), Colmar, France. – 2015. – pp. 392-397. (Scopus)

*Патентные документы*

1. Пат. 2370898 Российская Федерация, МПК H 04 L 9/20 (2006.01). Способ защиты информации [текст] / Сидоров В.В., Карпов А.В., **Сулимов А.И.**; заявитель и патентообладатель ФГАОУ ВО «Казанский (Приволжский) федеральный университет». – № 2007134624/09; заявл. 05.09.2007; опубл. 20.10.2009, Бюл. № 29. – 11 с.: ил.

2. Пат. 2423800 Российская Федерация, МПК H 04 L 9/18 (2006.01). Способ защиты информации [текст] / Сидоров В.В., Шерстюков О.Н., **Сулимов А.И.**; заявители и патентообладатели: ФГАОУ ВО «Казанский (Приволжский) федеральный университет», Сидоров В.В., Шерстюков О.Н, Сулимов А.И. – № 2008152523/09; заявл. 29.12.2008; опубл. 10.07.2011, Бюл. № 19. – 9 с.
3. Пат. 2527734 Российская Федерация, МПК H 04 L 9/00 (2006.01). Способ защиты информации [текст] / **Сулимов А.И.**, Шерстюков О.Н., Карпов А.В., Каюмов И.Р., Смоляков А.Д.; заявитель и патентообладатель ООО «НПП «СэйвТелеком». – № 2012112893/08; заявл. 04.04.2012; опубл. 10.09.2014 Бюл. № 25. – 11 с.: ил.

*Прочие публикации*

1. Сидоров, В.В. Современные тенденции в области защиты информации в телекоммуникационных системах. / В.В. Сидоров, А.В. Карпов, **А.И. Сулимов** [Текст] // Материалы международной научно-практической конференции «Роль неправительственных научно-общественных организаций в решении проблем, связанных с разработкой и внедрением инновационных технологий во все сферы человеческой деятельности». Вестник академии информатизации Республики Татарстан, Казань, Россия. – 2009. – с. 47-54.
2. **Сулимов, А.И.** Особо надежная защита информации [Текст] / А.И. Сулимов // Научно-техническое творчество молодежи – путь к обществу, основанному на знаниях: сборник докладов III Международной научно-практической конференции, Москва, Россия. – 2011. – с. 235-236.
3. **Сулимов, А.И.** Генерация и распределение ключей симметричного шифрования на основе физических свойств радиометеорного распространения [Текст] / А.И. Сулимов, А.В. Карпов, В.В. Сидоров, О.Н. Шерстюков // Сборник докладов XXIII Всероссийской научной конференции «Распространение радиоволн», Йошкар-Ола, Россия. – 2011. – Т.1. – с. 421-425.
4. **Сулимов, А.И.** Динамическая модель многолучевого радиоканала [Текст] / А.И. Сулимов, О.Н. Шерстюков, А.Д. Смоляков, А.В. Карпов, В.В. Сидоров // Сборник докладов XXIII Всероссийской научной конференции «Распространение радиоволн», Йошкар-Ола, Россия. – 2011. – Т.2. – с. 72-76.
5. Карпов, А.В. Экспериментальное исследование пространственной декорреляции сигналов в многолучевом радиоканале [Текст] / А.В. Карпов, А.Д. Смоляков, **А.И. Сулимов** // Сборник докладов XXIV Всероссийской научной конференции по распространению радиоволн, Иркутск, Россия. – 2014. – Т. 2. – с. 88-91.
6. Карпов, А.В. Моделирование условий невзаимности в метеорном радиоканале [Текст] / А.В. Карпов, Д.В. Любимов, **А.И. Сулимов** // Сборник докладов XXIV Всероссийской научной конференции по распространению радиоволн, Иркутск, Россия. – 2014. – с. 105-108.
7. Карпов, А. Современные физические методы в криптографии [Электронный ресурс] / А. Карпов, А. Смоляков, **А. Сулимов**, О. Шерстюков // Радиоэлектронные технологии. – 2015. – №4. – с. 86-89. Режим доступа: http://hi-tech.media/42015.html.
8. Karpov, A.V. Study of phase non-reciprocity of meteor burst channel / A.V. Karpov, **A.I. Sulimov**, S.N. Tereshin // Proceedings of XI International IEEE Siberian Conference on Control and Communications (SIBCON-2015), Omsk, Russia. – 2015. – pp. 1-5.

## СПИСОК ЦИТИРУЕМОЙ ЛИТЕРАТУРЫ


1. Смарт, Н. Криптография [Текст] / Н. Смарт. – М.: Техносфера, 2005. – 528 с.
2. Шеннон, К.Э. Работы по теории информации и кибернетике [Текст] / Клод Элвуд Шеннон. – М.: Изд-во иностранной литературы, 1963. – 827 с.
3. Bennett, C.H. Quantum Cryptography: Public key distribution and coin tossing / C.H. Bennett, G. Brassard // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India. – 1984. – pp. 175-179.
4. Qi, Bing. Time-shift attack in practical quantum cryptosystems / Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, Xiongfeng Ma // Quantum information computation. – 2005. – Vol.7. – iss.1-2. – pp. 1-10.
5. Korzh, B. Provably secure and practical quantum key distribution over 307 km of optical fibre / B. Korzh, C. Ci Wen Lim, R. Houlmann et el. // Nature Photonics. – 2015. – vol. 9. – pp. 163-168.
6. Хузяшев, Р.Г. Анализ дифракции на метеорном следе наклонно падающих радиоволн строгим и приближенным методами [Текст]: дис. … кан. физ.-мат. наук: 01.04.03/ Хузяшев Рустем Газизович. – Казань, 1986. – 158 с.
7. Карпов, А.В. Компьютерная модель метеорного радиоканала [Текст]: дис. на соиск. уч. степ. док. физ.-мат. наук: 05.12.01/ Карпов Аркадий Васильевич. – Казань, 1998. – 414 с.
8. Пономарев, Г.А. Распространение УКВ в городе [Текст] / Г.А. Пономарев, А.М. Куликов, Е.Д. Тельпуховский. – Томск: МП «Раско», 1991. – 223 с.
9. Использование метеорного радиоканала для высокоточной синхронизации разнесённых хранителей времени: Отчет о НИР по теме «Шкала» / Казанский государственный университет (КГУ). – Казань, 1991. – 109 с.