ОТЗЫВ

официального оппонента на диссертационную работу Махорина Дмитрия Алексеевича “Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи”, представленной на соискание ученой степени кандидата технических наук по специальности 05.11.07 – “Оптические и оптико-электронные приборы и комплексы”

Актуальность

В последнее время существенное развитие получили системы и технологии квантового распределенного ключа по волоконно-оптическим линиям связи. Наблюдается заметный рост как зарубежных, так и отечественных работ. Это связано как с бурным развитием средств передачи и приема сигналов, так и с необходимостью дальнейшего развития технологий квантовой криптографии для усиления защищенности передаваемой информации. Рассматриваемое в диссертации временное кодирование является перспективным направлением развития способов кодирования информации. Основными преимуществами такого кодирования являются возможность передачи сигнала на значительные расстояния и защищенность от перехвата и других действий нелегитимного пользователя. Вместе с тем в рамках рассматриваемой темы остается много нерешенных проблем. Всё вышесказанное доказывает актуальность рассматриваемой темы диссертации.

Содержание диссертации по главам

Первая глава диссертации носит обзорный характер. В ней рассматриваются такие вопросы как используемые в диссертации принципы квантовой механики, проблема приготовления состояний квантовых частиц, технология приготовления кубитов, способы и протоколы кодирования, обоснование использования временного кодирования, принципы работы передающего и принимающего оптического модуля. Все указанные разделы сопровождаются ссылками на авторов предшествующих исследований. Материал главы полностью обосновывает актуальность диссертационного исследования и решаемые задачи.

Вторая глава диссертации посвящена таким вопросам как оценка помехоустойчивости лавинного фотодиода в различных режимах работы, обоснование возможности реализации приемной системы на базе лавинного фотодиода, структурная схема предлагаемого в диссертации высоковольтного источника питания, предлагаемые функциональные схемы приемной системы, расчетные формулы трансформации квантовых состояний одиночных фотонов и кубитов в последовательности интерферометров Маха-Цендера. Материал главы доказывает возможность реализации предлагаемого приемного оптического модуля и импульсного источника питания.

Третья глава диссертации посвящена исследованию предлагаемых систем квантового распределенного ключа с временным кодированием. В ней рассматриваются такие вопросы как структура системы квантового распределенного ключа с временным кодированием, схемы устройств для формирования посылаемых сигналов, дешифрации кодовых состояний, оценка шумов, оценка безопасных от атак нелегитимного пользователя границ значений скорости генерации ключа и длины квантового канала, процедуры статистического и интерферометрического контроля, программная реализация симуляции приемо-передающей системы. Материал этой главы обосновывает предложенные в диссертации схемы и доказывает, что использование интерферометрического и статистического контроля значительно увеличивает защищенность системы.

Четвертая глава диссертации посвящена предлагаемой системе кодирования с использованием tb- кубитов. В ней рассматриваются такие вопросы как возможные состояния tb- кубитов в системе, предлагаемая схема кодирования, структурная схема системы, основанная на tb- кубитах. Материал главы обосновывает то, что использование таких систем позволяет усилить защищенность канала.

Степень обоснованности и достоверность научных положений

Диссертационная работа содержит подробный анализ предшествующих исследований, что обосновывает необходимость решения поставленных задач. Достоверность научных положений обосновывается путем применения аппарата квантовой механики, теоретических расчетов, построением программных симуляций разработанных макетов систем квантового распределенного ключа в волоконно-оптических линиях связи.

Обоснованность выносимых на защиту защищаемых положений не вызывает сомнений.

Соответствие диссертации представленной специальности

Область исследований диссертации связана с разработкой, совершенствованием и исследованием характеристик систем передачи, приема, обработки информации, передаваемой с использованием электромагнитного излучения по волоконно-оптическому каналу. Что в полной мере соответствует специальности 05.11.07 – "Оптические и оптико-электронные приборы и комплексы".

Научная новизна

Основными научными результатами, обладающими новизной, на мой взгляд, являются следующие:

1. предложенная система интерференционного и статистического контроля одноуровневых состояний в системах КРК с временным кодированием.
2. предложенная система передачи квантового распределенного ключа с использование tb- кубитов.
3. предложенная процедура обнаружения нелегитимного пользователя в канале связи, основанная на данных о состоянии tb- кубита на выходе канала.
4. разработанные макеты систем волоконно-оптической связи содержащей в себе звенья, реализующие предлагаемые протоколы кодирования и контроля.

Новизна этих результатов подтверждается сравнением с ранее опубликованными работами. Достоверность подтверждается с использованием аппарата квантовой механики, теоретическим анализом источников ошибок в канале и ее оценкой, программной симуляцией канала связи.

Опубликованность результатов.

По основным результатам диссертационной работы опубликовано 8 публикаций в изданиях рекомендованных ВАК России. Анализ публикаций показывает, что основные результаты достаточно полно опубликованы в статьях в журналах рекомендуемых ВАК России. Следует отметить хорошую структурированность публикаций и логическую последовательность. Первые публикации диссертанта посвящены проблемам приготовления квантовых состояний и генерации посылаемого в волоконно-оптический канал квантового ключа, далее идут работы о системе приема передаваемых сигналов и специфике создания таких систем. Далее о проблемах кодирования-декодирования, оценке ошибок канала. Затем о проблеме поиска нелегитимного пользователя. А наиболее свежие работы посвящены разработке систем с использованием tb- кубитов и путях усиления защищенности канала связи с использованием tb- кубитов.

Практическая значимость результатов работы

Разработанные в диссертации протоколы и системы квантового распределенного ключа с временным кодированием позволяют оптимизировать существующие системы квантового распределенного ключа с симметричным шифрованием. Внедрение предложенных модификаций позволит значительно увеличить защищенность каналов волоконно-оптической связи. Содержащиеся в диссертации подробные схемы таких систем сведут к минимуму время, необходимое для аппаратурной реализации систем.

Практическая значимость результатов также подтверждается приведенной в диссертации копии акта внедрения (использования) результатов диссертационной работы. В этом акте подтверждается использование “модели системы квантового распределения ключей с временным кодированием по протоколу M04 с подсистемами интерферометрического и статистического контроля целостности передаваемых данных”, указывается, что “результаты представляют практический интерес ПАО «Ростелеком» в связи с развитием корпоративной политики по внедрению перспективных систем защищенной связи”.

Вопросы и замечания:

1) На страницах 6,7 при упоминании вклада Wootters W.K., Zurek W.H., …, Boucher W. считаю необходимым указать ссылки на работы этих исследователей.

2) В разделе научная новизна пункт 2 указывается, что "Показано, что использование статистического и интерферометрического контроля… позволяет усилить защищенность системы". Насколько процентов снижается вероятность перехвата информации нелегитимным пользователем?

3) На странице 10 указывается, что достоверность полученных результатов обеспечивается, в том числе верификацией полученных результатов с имеющимися экспериментальными данными. Но, на мой взгляд, в диссертации проверке достоверности результатов путем сопоставления с экспериментальными данными уделено недостаточно внимания.

4) На странице 30 упоминается :".. однако это возможно только при определенной критической длине квантового канала, которая зависит от доли двух- и более фотонных импульсов в передаваемых информационных посылках". В тексте диссертации следовало указать формулы для оценки этой критической длины квантового канала и привести пример конкретного расчета.

5) На странице 35 указывается, что "существенным фактором, препятствующим применению ОВ для поляризационного кодирования, является поляризационная дисперсия волокна, приводящая к декогеренции ПК в ОВ, т.е. быстрому разрушению когерентных состояний. Поэтому использование ПК в ОВ нежелательно". В диссертации следовало указать длину ОВ, при которой влияние поляризационной дисперсии становится критическим.

6) На странице 51 упоминается, что используется аппроксимация вида (2.2) для получения (2.6), но какова погрешность использования этой стандартной, но все же приближенной формулы?

7) Пункт 2.2 диссертации посвящен оценке помехоустойчивости. Пункт завершается формулой (2.8), но оценки величин F_{ap} и F_{dcr} не приводятся. Считаю необходимым указать значения F_{ap} и F_{dcr} по порядку величин.

8) Считаю, что в диссертации доказано, что меры, которые предлагаются необходимы. Но являются ли они достаточными? Можно ли

это доказать. Каковы направления развития или есть ли пути обхода предлагаемых мер?

9) В работе не указана предельная длина ОВ, при которой возможна работа предлагаемой системы.

10) Замечания по оформлению:

- В разделе практическая значимость пункты 4 и 5 повторяют друг друга.
- В диссертации нет расшифровки аббревиатуры КЧ.
- В списке статей диссертанта в изданиях, рекомендованных ВАК России. опечатки: №6 - правильно Т.34, №3 – 2014 г., №8 – Т. 59. Эти опечатки затрудняют поиск этих статей.
- На странице 17 в формуле для $|\langle x | s \rangle|^2$ после знака равно опечатка.
- На странице 43 две формулы (1.15).
- На странице 43 в тексте “Сравнивая формулы (1.11) и (1.14)” неверно указаны ссылки на формулы.
- На странице 51 отсутствует рисунок 2.4, но на него есть ссылка в тексте.
- На страницах 65-66 упоминается рисунок 2.20, но в тексте его нет.
- Рисунки 2.21 и 2.22 абсолютно одинаковые (кроме подписи к ним). Подпись к рисунку 2.21 не соответствует действительности. Однако в тексте автореферата данный рисунок приведен верно (рис. 4).
- Не совсем качественно выполнена схема 3.3
- На станице 81 указывается “Сформированный сырой ключ представлен на рис. 3.13” неверная ссылка правильно 3.12.
- Рисунок 3.13 не полностью отображает то, что описано
- На странице 97 неверная ссылка на формулу (3).
- Приложение Б крайне некачественно оформлено: название на странице приложения А, в тексте присутствуют посторонние знаки.

Высказанные замечания не снижают общую положительную оценку диссертации.

В целом считаю, что диссертационная работа Махорина Д.А. посвящена новой, актуальной и перспективной теме построения защищенных систем квантового распределенного ключа с временным кодированием в линиях волоконно-оптической связи. Работа написано основательно, содержит в себе достаточное количество новых и перспективных с точки зрения практических приложений результатов. Текст диссертации оставляет

исключительно приятное впечатление. Автореферат диссертации соответствует тексту диссертации и ее основным положениям.

Заключение

Диссертационная работа Махорина Д.А. является законченным научным исследованием, соответствует всем критериям, предъявляемых к кандидатским диссертациям, установленных Положением о порядке присуждения ученых степеней, а соискатель Махорин Д.А. заслуживает присвоения ему ученой степени кандидата технических наук по специальности 05.11.07 – "Оптические и оптико-электронные приборы и комплексы".

Официальный оппонент, к.ф.-м.н.,
старший научный сотрудник Лаборатории
распространения оптических сигналов
Федерального государственного бюджетного
учреждения науки Института оптики атмосферы
им. В.Е. Зуева Сибирского отделения
Российской академии наук (ИОА СО РАН) Тарасенков М.В.

Подпись официального оппонента заверяю:
ученый секретарь ИОА СО РАН,
к.ф.-м.н. Тихомирова О.В.

«10» июня 2016 г.

Контактная информация:
Адрес: Российская Федерация, 634055, г. Томск, площадь Академика Зуева, д.1 тел. (3822) 491-081, e- mail: TMV@iao.ru