«УТВЕРЖДАЮ»
Проректор по
научной работе и
инновациям
д.т.н., профессор
_____Мещеряков Р.В.
«10» марта 2016 г.

ЗАКЛЮЧЕНИЕ

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Томский государственный университет систем управления и радиоэлектроники» (ТУСУР).

Диссертация «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи» выполнена в ТУСУРе на кафедре радиоэлектроники и защиты информации (РЗИ).

Соискатель Махорин Дмитрий Алексеевич в 2011 г. окончил ТУСУР по специальности «Средства связи с подвижными объектами».

Удостоверение о сдаче кандидатских экзаменов выдано в 2016 г. ТУСУРом.

Научный руководитель – доктор технических наук Задорин Анатолий Семенович, профессор, заведующий кафедрой РЗИ ТУСУРа.

По итогам обсуждения принято следующее заключение:

Оценка выполненной соискателем работы.

Диссертация Махорина Дмитрия Алексеевича является научно-квалифицированной работой, в которой содержится решение важных и актуальных задач:

1. разработка расчетной и программной моделей оценки помехоустойчивости приемного оптического модуля (ПрОМ) и предельной скорости генерации ключа системы КРК;
2. разработка источника питания лавинного фотодиода (ЛФД) в линейном режиме и контроллера ЛФД в гейгеровском режиме:
3. разработка схемы и модели приготовления многоуровневых временных состояний квантовых частиц;
4. разработка модели подсистем интерферометрического и статистического контроля, а также модели системы КРК с временным кодированием одноуровневых состояний одиночных фотонов по протоколу BB84;
5. разработка и исследование метода временного кодирования двухуровневых состояний системы КРК.

Актуальность темы диссертации. Для организации конфиденциальных каналов передачи данных широкое распространение получили методы шифрования с открытым ключом (асимметричное шифрование), пришедшие на смену симметричному шифрованию, которое обладает существенным

недостатком – необходимостью надежного распределения секретного ключа для передающей и приемной стороны.

Защищенность систем с использованием асимметричного шифрования ограничена, как известно, вычислительными возможностями аппаратуры нелегитимного пользователя. В этой связи подобные криптографические алгоритмы принято считать условно защищенными.

Однако перспективы создания принципиально новых вычислительных машин, так называемых квантовых компьютеров, позволит существенно увеличить скорость вычислений, что существенно снизит криптостойкость систем с открытым ключом, поэтому актуальной задачей является поиск альтернативных методов шифрования.

Развитие науки и техники, практическое применение идей квантовой механики в области квантовых вычислений в последние десятилетия позволило разработать системы квантового распределения ключа (КРК), использующие симметричное шифрование. Технология КРК основывается на применении для связи между легитимными пользователями квантовых частиц – фотонов, свойства которых используются для формирования ключевой последовательности $\mathbf{k}_{АБ}$.

Системы КРК обладают существенным преимуществом перед существующими методами шифрования, так как их защищенность от перехвата данных являются безусловной и основана на физических законах, в том числе на теореме о запрете клонирования.

Личный вклад автора. Все представленные в диссертации результаты исследований получены лично автором либо при его непосредственном участии. В работах, опубликованных в соавторстве, автором получены существенные теоретические и практические результаты.

Достоверность полученных результатов диссертационного исследования обеспечивается обоснованностью предлагаемых моделей, решений и выводов, верификацией полученных результатов с имеющимися теоретическими и экспериментальными данными, результатами симуляции на ЭВМ.

Научная новизна:

1. Показано, что регулировка порога срабатывания решающего устройства в ПрОМ системы КРК по сравнению с существующими цифровыми системами связи позволяет лимитировать вероятность ложных сигналов за счет снижения средней битовой скорости формирования ключа.
2. Показано, что использование статистического и интерферометрического контроля одноуровневых состояний в системах КРК с временным кодированием по сравнению с известными аналогами позволяет усилить защищенность системы.
3. Разработан оригинальный способ построения системы КРК с временным кодированием tb-кубитов, передаваемых по ККС.
4. Предложено использование данных о состоянии кубитов на выходе ККС не прошедших процедуру согласования базисов в рамках протокола BB84 для детектирования перехвата данных

5. Предложен оригинальный способ обнаружения атак на систему КРК, заключающийся в обработке временного статистического распределения сигналов на выходе ПрОМ по тайм-слотам (минимальным временным интервалам, в пределах которых может быть детектирован фотон, ТС) в пределах тактового интервала.

Практическая значимость:

1. Предложена модель оценки помехоустойчивости ПрОМ с ЛФД, работающем в линейном режиме. Установлена зависимость уровней вероятности ложного сигнала P_f и пропуска сигнала P_l, а также средней битовой скорости генерации ключа от вариации порога срабатывания решающего устройства.

2. Предложена и исследована схема контроллера ЛФД ПрОМ для высоковольтных диодов в линейном и гейгеровском режиме с активным гашением лавины в виде формирователя импульсов перенапряжения с разрядной линией.

3. Разработаны и исследованы модели подсистем интерферометрического и статистического контроля, а также модель системы КРК с временным кодированием одноуровневых состояний одиночных фотонов по протоколу BB84.

4. Предложена модель описания способа приготовления tb-кубитов в системе из нескольких разбалансированных интерферометров Маха-Цендера (ИМЦ).

5. Предложена модель описания способа приготовления tb-кубитов в системе из нескольких разбалансированных интерферометров Маха-Цендера (ИМЦ).

6. Предложено использование дополнительного оптического волокна, соединяющего свободные порты ИМЦ-А, Б при контроле интерференции амплитуд вероятности КЧ в квантовом канале, позволяющего увеличить системный битрейт в два раза по сравнению с аналогичными оптоволоконными системами КРК с фазовым кодированием.

Полнота изложенных материалов в печатных работах, опубликованных автором. По результатам исследований опубликованы 13 печатных работ, из которых в рекомендованных ВАК РФ периодических изданиях – 8. Получено свидетельство о государственной регистрации программы для ЭВМ:

1. Задорин А.С., Максимов А.В., Махорин Д.А. и др. Скорость генерации кода в системе квантового распределения ключей // Доклады ТУСУРа. – 2011. – № 2 (24). – С. 139-141

2. Задорин А.С., Максимов А.В., Махорин Д.А. Режимы работы фотоприемного устройства системы квантовой криптографии // Доклады ТУСУРа. – 2012. - №2(26). – С. 63-66

3. Махорин Д.А., Галиев А.Б., Задорин А.С. Возможность реализации линейного режима счета фотонов на лавинном фотодиоде S8664-05K при комнатной температуре // Доклады ТУСУРа. – 2013. – №1(31). – С. 65-68

4. Задорин А.С., Махорин Д.А. Модель системы квантового распределения ключей с временным кодированием // Доклады ТУСУРа. – 2014. – №3 (33). – С. 85-89.

5. Задорин А.С., Махорин Д.А. Статистическая обработка сигналов в системах квантового распределения ключей // Доклады ТУСУРа. – 2014. – №3 (33). – С. 90-93.

6. Задорин А.С., Махорин Д.А. Интерферометрический контроль целостности данных в системе квантового распределения ключей с временным кодированием // Доклады ТУСУРа. – 2014. – №4 (33). – С. 85-89.

7. Задорин А.С., Махорин Д.А. Матричное описание трансформации квантовых состояний одиночных фотонов в последовательности разбалансированных интерферометров Маха-Цендера // Доклады ТУСУРа. – 2015. – №3 (37). – С. 145-149.

8. Махорин Д.А. Особенности гейгеровского режима работы фотоприемного устройства системы КРК // Материалы докладов XVII Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР – 2012», г. Томск, 16-18 мая 2012г.

9. Авдоченко Б.И., Задорин А.С., Максимов А.В., Махорин Д.А. Контроллер лавинного фотодиода системы квантовой криптографии // Материалы докладов VIII Международной научно-практической конференции «Электронные средства и системы управления - 2012» – Томск, 8-10 ноября 2012г. часть 2. – С. 105-109.

10. Махорин Д. А., Задорин А. С., Альбрехт Р. С., Исатаев А. Н. Усиление защищенности системы квантового распределения ключа с временным кодированием по оптическому волокну // Международная конференция «СВЧ-техника и телекоммуникационные технологии» (КрыМиКо'2015), материалы 25-й международ. конф. – Севастополь, 2015. том 1 – С. 1019-1021.

11. Задорин А.С., Махорин Д.А. Временное кодирование состояний фотонов в системе квантового распределения ключей с временным кодированием ТВ-кубитов // Материалы докладов XI Международной научно-практической конференции «Электронные средства и системы управления - 2014», г. Томск, 25-27 ноября 2015г. Часть. 1. С. 265-269.

12. Махорин Д.А., Задорин А.С., Решетников С.Ю. Статистический контроль распределения числа фотонов в информационных сообщениях в системе квантового распределения ключа с временным кодированием // Материалы докладов XI Международной научно-практической конференции «Электронные средства и системы управления - 2014», г. Томск, 25-27 ноября 2015г. Часть. 1. С. 270-273.

13. Задорин А.С., Махорин Д.А. Принцип квантового распределения ключей по оптическому волокну на основе временных сдвигов ТВ-кубитов // Изв. вузов. Физика. 2016, №3.

14. Свид. о гос. Регистрации программы для ЭВМ №2015617171 Махорин Д.А., Задорин А.С. Quantum key distribution system. Зарег. в Реестре программ для ЭВМ 2 июля 2015г.

Ценность научных работ соискателя. Научные работы соискателя имеют высокую ценность. Она подтверждается многочисленными публикациями их результатов в рецензируемых журналах и материалах конференций.

В диссертационной работе Махориным Д.А. разработана программная модель системы квантового распределения ключа с временным кодированием по протоколу M04, а также подсистемы интерферометрического и статистического контроля целостности передаваемых данных для указанной модели.

Данные результаты использованы в Томском филиале ПАО «Ростелеком», а также в учебном процессе каф. РЗИ в течение зимних и весенних семестров 2014-2016 гг. при подготовке студентов в рамках основных образовательных программ кафедры: бакалаврские программы 10.03.01 «Информационная безопасность» и 10.03.02 «Инфокоммуникационные технологии и системы связи», профиль «Защищенные системы и сети связи», а также в магистерской программе "Системы и устройства передачи, приема и обработки сигналов" направления 11.04.01 «Радиотехника».

Специальность, которой соответствует диссертация

Диссертационная работа Махорина Дмитрия Алексеевича по своему содержанию соответствует специальности 05.11.07 - «Оптические и оптико-электронные приборы и комплексы» в области исследования и разработки новых методов и процессов, которые могут быть положены в основу создания оптических и оптико-электронных приборов, систем и комплексов различного назначения.

Диссертация «Модель системы квантового распределения ключа с временным кодированием по волоконно-оптической линии связи» Махорина Дмитрия Алексеевича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.11.07 – «Оптические и оптико-электронные приборы и комплексы».

Заключение принято на заседании кафедры РЗИ.

Присутствовало на заседании чел. Результаты голосования: «за» – 21 чел., «против» – 0., «воздержалось» – 0 чел., протокол № 6 от «10» марта 2016 г.

Председатель,
д.ф.-м.н., профессор _____Задорин А.С.

Секретарь,
старший преподаватель _____Зеленецкая Ю.В.