Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 621.391; 621.383.92

Толкачева
Виолетта Сергеевна

Разработка высокоскоростного устройства передачи защищенной от несанкционированного доступа информации

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 – Методы и системы защиты информации, информационная безопасность

Научный руководитель
Тимофеев Александр Михайлович
кандидат технических наук, доцент

Минск 2015

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время информационная безопасность – одно из приоритетных направлений развития современных средств связи, в которых данные передаются по волоконно-оптическим линиям связи. Обеспечить защиту информации от несанкционированного доступа можно с помощью квантовых систем, использующих для передачи каждого бита информации оптические сигналы, содержащие от одного до десятка фотонов. Защита информации от несанкционированного доступа в квантовых системах связи базируется на использовании фундаментальных законов квантовой механики и связана с невозможностью копирования заранее неизвестного состояния отдельного квантового объекта и невозможностью получения любой информации о квантовых состояниях этого объекта без их изменения.

Известные квантовые системы передачи защищенной от несанкционированного доступа информации обеспечивают низкую скорость передачи информации, так как данные передаются последовательно друг за другом. Также существующие устройства передачи данных для кодирования передаваемой информации используют неортогональные состояния фотонов, что приводит к появлению дополнительных ошибок при передаче данных, обусловленных поворотом поляризации фотонов на 45º. В связи с этим целью данной работы являлась разработка устройства передачи защищенной от несанкционированного доступа информации, позволяющего увеличить скорость передачи информации путем одновременной передачи четырех двоичных символов и использования для кодирования передаваемой информации двух состояний фотонов, а также устранить ошибки при передаче данных за счет кодирования передаваемой информации взаимно ортогональными состояниями фотонов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Целью настоящей диссертационной работы является разработка устройства передачи защищенной от несанкционированного доступа информации, позволяющего увеличить скорость передачи информации путем одновременной передачи четырех двоичных символов и использования для кодирования передаваемой информации двух состояний фотонов.

Для достижения поставленной цели потребовалось решение следующих взаимосвязанных задач:

1. Рассмотреть основные криптографические методы защиты информации.

2. Провести аналитических обзор существующей элементной базы и видов систем квантовой криптографии.

3. На основе выполненного обзора предложить устройство передачи данных, которое повысить увеличить скорость передачи информации путем одновременной передачи четырех двоичных символов и использования для кодирования передаваемой информации двух состояний фотонов.

4. Предложить математическую модель волоконно-оптического канала связи при передаче данных сигналами малой мощности, учитывающую вероятность образования темновых импульсов и квантовую эффективность регистрации приемного модуля канала связи.

5. Экспериментально исследовать влияние длительности импульсов стробирования и времени передачи одного бита информации на пропускную способность канала связи.

В качестве объекта исследования использовался волоконно-оптический канал связи, в котором приемным модулем служит счетчик фотонов на базе кремниевого лавинного фотодиода ФД-115Л.

Предметом исследований являлось установить, какое влияние оказывают длительность импульсов стробирования и время передачи одного бита информации на пропускную способность канала связи.

Личный вклад соискателя

Содержание диссертации отражает личный вклад соискателя. В работах, выполненных в соавторстве автор принимал участие в определении целей, задач исследований, а также в проведении самих исследований и обработке полученных результатов.

Апробация и опубликованность результатов

Основные полученные результаты диссертационной работы докладывались и обсуждались на Международной научно-технической конференции, приуроченной к 50-летию МРТИ – БГУИР (Минск, Республика Беларусь, 2014 г.) и XII Белорусско-российской научно-технической конференции «Технические средства защиты информации» (Минск, Республика Беларусь, 2014 г.). Опубликовано два тезиса докладов.

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения и библиографического списка.

В первой главе приведена классификация криптографических методов защиты информации и рассмотрены типовые структуры квантовых систем распределения ключа.

Во второй главе рассмотрена основная элементная база для систем квантовой криптографии.

Третья глава содержит методику и результаты экспериментальных исследований пропускной способности защищенного от несанкционированного доступа канала однофотонной связи, а также принципы передачи защищенной от несанкционированного доступа информации для разработанного устройства, заключающиеся в одновременной передаче четырех двоичных символов и использовании для кодирования передаваемой информации двух состояний фотонов, что позволило устранить ошибки при передаче данных.

Полный объем диссертации составляет 54 страницы машинописного текста. Диссертация содержит 13 рисунков на 7 страницах. Библиографический список занимает 7 страниц и состоит из 81 наименования использованных источников и списка собственных публикаций соискателя из двух наименований на одной странице.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** определены основные направления исследований, обоснована актуальность темы диссертации, показана необходимость разработки устройства передачи защищенной от несанкционированного доступа информации.

В **первой главе** приведены результаты анализа литературы, где рассмотрены известные типовые структуры квантовых систем распределения ключа. Показано, что при создании высокоскоростных криптосистем следует использовать симметричные схемы, скорость шифрования которых по сравнению с асимметричными на несколько порядков выше. Установлено, что шифрование информации является наиболее эффективным методом защиты информации, в сравнении с другими. Причем комплексное использование методов стеганографии и шифрования многократно повышает сложность раскрытия информации несанкционированным пользователем.

Во **второй главе** дано описание основных характеристик источников, оптических волокон и детекторов, применяемых в качестве элементной базы для систем квантовой криптографии. На основе рассмотренных способов получения источников одиночных фотонов установлено, что использование процесса параметрической генерации коррелированных пар фотонов требует наличия дорогостоящих искусственных кристаллов и лазеров и характеризуется низким коэффициентом преобразования фотонов накачки в пару коррелированных фотонов ($10^{-7} \div 10^{-11}$). Трудность получения источников фотонов на одиночных квантовых излучателях связана, в частности, с необходимостью поддержания ультравысокого вакуума и экстремально низких температур (менее 1 К). Источники одиночных фотонов, полученные на ослаблении оптических импульсов, свободны от этих недостатков и позволяют получить направленный поток фотонов практически на любой длине волны, что определяет целесообразность применения таких источников для высокоскоростных систем передачи защищенной от несанкционированного доступа информации. Сопоставительный анализ фотоприемников квантовых систем показал, что в качестве фотоприемников высокоскоростных устройств передачи защищенной от несанкционированного доступа информации целесообразно использовать лавинные фотодиоды, которые имеют высокий квантовый выход, низкие напряжения питания, обладают высоким коэффициентом умножения (10^6 и более). При этом кремниевые лавинные фотодиоды позволяют реализовать режим счета фотонов при комнатных температурах и,

в сравнении с фотоэлектронными умножителями, обладают лучшей пороговой чувствительностью.

В **третьей главе** дано описание принципов передачи защищенной от несанкционированного доступа информации для разработанного устройства. Предложенное устройство позволяет в 4 раза увеличить скорость передачи информации за счет одновременной передачи четырех двоичных символов и использования для кодирования передаваемой информации двух состояний фотонов, что позволяет устранить ошибки при передаче данных за счет кодирования передаваемой информации взаимноортогональными состояниями фотонов. Получено выражение для расчета пропускной способности канала связи, учитывающее вероятность образования темновых импульсов, квантовую эффективность регистрации фотоприемника и длительность передачи одного бита (символа). Предложена многоканальная квантовая система связи, которая, в сравнении с одноканальными, позволяет увеличить СПИ квантовых систем связи в i раз (где i − число каналов) за счет того, что все биты передаваемого кодового слова транслируются по одному оптическому волокну на разных длинах волн оптического излучения.

ЗАКЛЮЧЕНИЕ

На основании выполненного аналитического обзора литературных источников определены способы получения источников одиночных фотонов. Установлено, что для высокоскоростных систем передачи защищенной от несанкционированного доступа информации целесообразно применение источников одиночных фотонов, полученных на ослаблении оптических импульсов, что обусловлено простотой реализации, низкой стоимостью и возможностью получения направленного потока фотонов практически на любой длине волны.

При построении систем передачи защищенной от несанкционированного доступа информации необходимо использовать квантовые каналы для передачи состояния фотонов, построенные на базе оптических волокон, компенсирующих влияние хроматической дисперсии и поляризационных эффектов.

Целесообразность использования ЛФД в качестве фотоприемников систем, обеспечивающих передачу защищенной от несанкционированного доступа информации, обусловлена тем, что такие фотоприемники имеют высокий квантовый выход, низкие напряжения питания, обладают высоким коэффициентом умножения. При этом кремниевые ЛФД позволяют реализовать режим счета фотонов при комнатных температурах и, в сравнении с ФЭУ, обладают лучшей пороговой чувствительностью.

Предложено устройство передачи информации с кодированием взаимно ортогональными состояниями фотонов, позволяющее в четыре раза увеличить скорость передачи информации за счет одновременной передачи четырех двоичных символов и использования для кодирования передаваемой информации двух состояний фотонов, а также устранить ошибки при передаче данных за счет кодирования передаваемой информации взаимно ортогональными состояниями фотонов.

На основании созданной математической модели канала однофотонной связи получено выражение для расчета пропускной способности, учитывающее среднее время передачи одного бита информации, вероятность образования темновых импульсов и квантовую эффективность регистрации счетчика фотонов.

Экспериментально установлено, что квантовая эффективность регистрации счетчика фотонов, вероятность образования темновых импульсов и пропускная способность защищенного от несанкционированного доступа канала однофотонной связи зависит как от

длительности импульсов стробирования, так и от времени передачи одного бита информации.

Предложена многоканальная квантовая система связи, которая, в сравнении с одноканальными, позволяет увеличить СПИ квантовых систем связи в i раз (где i − число каналов) за счет того, что все биты передаваемого кодового слова транслируются по одному оптическому волокну на разных длинах волн оптического излучения.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1 Зеневич, А.О. Многоканальная квантовая система связи для передачи конфиденциальной информации / А.О. Зеневич, А.М. Тимофеев, А.Г. Косари, А.А. Липай, Е.В. Мороз, В.С. Толкачева // Междунар. науч.-техн. конф., приуроченная к 50-летию МРТИ–БГУИР: материалы докладов в 2 ч., Минск, 18-19 марта 2014 г. / Белорус. гос. ун-т информатики и радиоэлектроники; редкол.: А.А. Кураев [и др.]. – Минск: БГУИР, 2014. – ч.1. – С. 426–427.

2 Зеневич, А.О. Одноквантовая система передачи конфиденциальной информации по волоконно-оптической линии связи / А.О. Зеневич, А.М. Тимофеев, А.Ю. Косари, А.Ю. Зябликов, А.А. Липай, В.С. Толкачева // Технические средства защиты информации: Тезисы докладов XII Белорусско-российской научно-технической конференции, 28–29 мая 2014 г., Минск – Минск: БГУИР, 2014. – С. 26