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

УДК 004.056.53

Зябликов
Александр Юрьевич

Математическая модель защищенного от несанкционированного доступа канала однофотонной связи

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 связаны с невозможностью копирования заранее неизвестного состояния отдельного квантового объекта и невозможностью получения любой информации о квантовых состояниях этого объекта без их изменения.

Однако современные квантово-криптографические системы обладают следующими недостатками: низкой скоростью передачи информации (до 50 кбит/с); малой дальностью передачи (до 200 км).

Учитывая малую скорость передачи информации в квантово-криптографических системах ее стремятся повысить. Для этого целесообразно установить влияние основных характеристик канала однофотонной связи на скорость передачи информации, используя соответствующую математическую модель канала связи. До настоящего времени математические модели канала связи, в котором данные передаются отдельными фотонами, отсутствуют.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Целью настоящей диссертационной работы является создание математической модели канала связи, в котором данные передаются отдельными фотонами.

Для достижения поставленной цели потребовалось решение следующих взаимосвязанных задач:

1. Рассмотреть виды каналов связи и провести обзор существующих принципов моделирования каналов и систем связи.

2. Рассмотреть основные угрозы для телекоммуникационных систем и криптографические методы защиты информации в них.

3. Провести сравнительный обзор квантово-криптографических средств защиты информации.

4. Разработать устройство передачи защищенных от несанкционированного доступа данных с автоматическим контролем вероятности ошибки регистрации.

5. Предложить математическую модель одноквантового канала связи, учитывающую квантовую эффективность регистрации приемного модуля канала связи, статистическое распределение импульсов на выходе счетчика при воздействии на него оптического излучения и статистическое распределение темновых импульсов.

В качестве объекта исследований использовался волоконно-оптический канал связи с приемником на основе счетчика фотонов.

Предметом исследований являлось установить, какое влияние оказывают пороговый уровень зарегистрированного числа фотонов, мощность оптического излучения, 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, заключения и библиографического списка.

В первой главе рассмотрены математические модели дискретных каналов связи, приведена классификация угроз для телекоммуникационных систем и рассмотрены криптографические методы защиты информации.

Во второй главе приведен обзор типовых структур квантово криптографических систем защиты информации и предложено устройство передачи данных по оптическому каналу связи с временным кодированием состояний фотонов.

Третья глава содержит результаты математического моделирования и экспериментальных исследований пропускной способности защищенного от несанкционированного доступа канала однофотонной связи.

Полный объем диссертации составляет 56 страницы машинописного текста. Диссертация содержит 14 рисунков на 12 страницах. Библиографический список занимает 5 страниц и состоит из 47 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 математического моделирования защищенного от несанкционированного доступа канала однофотонной связи.

В **первой главе** приведены результаты анализа литературы, где рассмотрены известные математические модели дискретных каналов связи. 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** приведен обзор типовых структур квантово криптографических систем защиты информации, основное преимущество которых состоит в их безусловной защищенности, которая зависит от вычислительных ресурсов злоумышленника. Кроме того, использование квантовой криптографии решает основную проблему симметричного шифрования – генерацию двух идентичных ключевых последовательностей у двух удаленных пользователей. Определено, что в системах квантовой криптографии в настоящее время применяют три вида кодирования квантовых состояний: поляризационное и фазовое кодирование, а также кодирование временными сдвигами. Установлено, что реальная квантовая криптографическая система с поляризационным кодированием требует создания механизма активной компенсации поляризационных изменений. Несмотря на наличие принципиальной возможности создания такого механизма, его практическая реализация затруднена. Фазовое кодирование решает проблемы поляризационного кодирования, однако реальны коммерческие реализации фазового кодирования слишком дорогие и сложные. Идея кодирования временными сдвигами позволяет упростить волоконно-оптическую часть системы квантовой криптографии и полностью отказаться от применения интерферометров. Предложенная схема позволяет реализовать большинство известных протоколов квантовой криптографии. На основе выполненного обзора предложено устройство передачи данных по оптическому каналу связи с временным кодированием состояний фотонов. Заявляемое устройство позволяет расширить функциональные возможности устройства путем введения автоматического контроля вероятности ошибки

регистрации и упростить его за счет устранения дополнительной линии связи для передачи импульсов синхронизации.

В **третьей главе** проведено математическое моделирование канала однофотонной связи с учетом статистического распределения импульсов на выходе счетчика при воздействии на него оптического излучения, статистического распределения темновых импульсов и порогового уровня регистрации. Найдены выражения для расчета скорости передачи информации и пропускной способности канала однофотонной связи. Проведены расчеты зависимости пропускной способности от величины порогового уровня и скорости счета сигнальных импульсов при условии отсутствия мертвого времени фотоприемника. Проведена экспериментальная оценка пропускной способности оптического канала связи при передаче сообщения отдельными фотонами, учитывающая вероятность образования темновых импульсов, квантовую эффективность регистрации фотоприемника и длительность передачи одного символа.

ЗАКЛЮЧЕНИЕ

На основании выполненного аналитического обзора литературных источников 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.

Выполненное сравнение существующих криптосистем показало, что использование асимметричных криптосистем целесообразно в тех случаях, когда передача общего для источника и приемника секретного ключа нелегитимному пользователю может привести к несанкционированному вскрытию всей передаваемой информации. Однако скорость шифрования симметричных криптосистем на несколько порядков выше, чем асимметричных, поэтому при создании высокоскоростных криптосистем следует использовать симметричные схемы.

В ходе работы были исследованы возможные способы съема информации с оптического волокна, а так же изучены квантово-криптографические средства защиты волоконно-оптических линий связи от несанкционированного доступа.

В результате анализа недостатков каждого из методов защиты ОВ было предложено устройство автоматического обнаружения несанкционированного доступа путем введения автоматического контроля вероятности ошибки регистрации. Для повышения эффективности этого устройства предложено использовать для регистрации параметров сигнала счетчик фотонов на базе лавинного фотоприемника.

Максимально достижимая скорость передачи информации в используемой установке составляет C_{max} ≈1,2 Мбит/с. При этом для уменьшения вероятности появления темновых импульсов предлагается выбирать длительность импульса стробирования $\Delta t \approx 0{,}8$ мкс.

Для получения максимального значения скорости передачи информации по оптическому каналу связи, содержащему в качестве приемного модуля счетчик фотонов на лавинном фотодиоде, необходимо подбирать оптимальное напряжения питания ЛФП, мощность оптического сигнала, транслируемого по каналу, и пороговый уровень регистрации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А 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, А.Ю. Зябликов, 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-А 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.