МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Физико-технический факультет**

**Кафедра оптоэлектроники**

**КУРСОВОЙ ПРОЕКТ**

**ФИЗИЧЕСКИЕ КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ В КВАНТОВО-КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Василенко Андрей Андреевич

Курс 2

Направление 03.03.03 Радиофизика

Научный руководитель

канд. физ.-мат. наук, доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О. А. Кулиш

Нормоконтролер преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В. Е. Лысенко

Краснодар 2017

**Реферат**

Курсовой проект 22 с., 3 рис., 7 источников.

КВАНТОВАЯ КРИПТОГРАФИЯ, ОПТОВОЛКНО, ОПТИЧЕСКИЕ СИСТЕМЫ, ПОЛЯРИЗАЦИЯ, ИНТЕРФЕРЕНЦИЯ

Объектом рассмотрения данного курсового проекта является процесс передачи информации в квантово-криптографических системах.

Целью проекта является рассмотрение принципов передачи информации в квантово-криптографических системах.

В результате выполнения проекта были получены знания о квантовой криптографии, как средство защиты коммуникаций, а также изучен процесс передачи квантовой информации.

**Содержание**

|  |  |
| --- | --- |
| Введение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
| 1 Квантовая криптография . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 5 |
| 2 Передача квантовой информации через канал связи . . . . . . . . . . . . .  |  9 |
| 3 Передача квантовой информации через атмосферу . . . . . . . . . . . . . .  | 12 |
| 4 Применение оптического волокна . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 15 |
| Заключение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 21 |
| Список используемых источников . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 22 |

**ВВЕДЕНИЕ**

Изучение принципов передачи квантовой информации связано с рассмотрением квантовой криптографии и каналов связи.

Криптография - это наука о шифрах. Она представляет собой огромное количество методов изменения открытого сообщения для того, чтобы передаваемое сообщение стало бесполезным для криптоаналитика, специалиста по криптоанализу. Криптоанализ – наука о вскрытии шифров. Криптографические преобразования служат для достижения двух целей по защите информации. Во-первых, они обеспечивают недоступность ее для лиц, не имеющих ключа, и, во-вторых, поддерживают с требуемой надежностью обнаружение несанкционированных искажений. Важным понятием в квантовой криптографии является ключ – сменный элемент шифра, который применяется для шифрования конкретного сообщения.

Привлекательность криптографических методов состоит в том, что в отличие от других подходов они основаны на преобразовании самой информации и никак не связаны с характеристиками ее материальных носителей, вследствие чего наиболее универсальны и потенциально дешевы в реализации.

 Целью данной работы является исследование видов физических каналов передачи информации в квантово-криптографических системах.

При этом существенно важным является решение следующих задач:

– изучить принципы передачи квантовой информации;

– рассмотреть возможности применения оптических волноводов в системах квантовой криптографии.

**1 Квантовая криптография**

Квантовая криптография – метод защиты коммуникаций, основанный на определенных явлениях квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике информации, так как рассматривает случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приёма информации всегда выполняется физическими средствами, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. А подслушивание может рассматриваться, как измерение определенных параметров физических объектов – в нашем случае, переносчиков информации.

Одним из направлений квантовой информации, наиболее продвинутых в область практических приложений, является квантовая криптография. Задача криптографии состоит в передаче информации между двумя сторонами так, чтобы попытка перехватить передачу или узнать секретный код была обречена на неудачу. Современными методами классической криптографии эта задача почти решается, например, в рамках «симметричной» криптосистемы, опирающейся на создание секретного кода.

Технология квантовой криптографии опирается на принципиальную неопределенность поведения квантовой системы – невозможно одновременно получить координаты и импульс частицы, невозможно измерить один параметр фотона, не исказив другой [5]. Это фундаментальное свойство природы в физике известно как принцип неопределённости Гейзенберга (1927). Используя квантовые явления, можно спроектировать и создать такую систему связи, которая всегда может обнаруживать подслушивание. Это обеспечивается тем, что попытка измерения взаимосвязанных параметров в квантовой системе вносит в неё нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале легитимные пользователи могут распознать степень активности перехватчика.

В этой системе Алиса и Боб, и только они, имеют секретный код – последовательность случайных чисел, например, десятичных: К={12

93 41169 42357...}. По заданному правилу каждой букве алфавита ставится в соответствие десятичное число и Алиса, желающая переслать Бобу послание, заменяет в послании каждую букву соответствующей ей цифрой. Сама по себе эта процедура не имеет защиты и легко дешифруется. Получающаяся последовательность чисел Р={739976827965867…}, послание, затем шифруется – к каждому числу послания прибавляется число из кода и получающиеся цифры в разряде единиц представляют собой криптограмму C={85680 09338 07114...}, которую можно пересылать по открытому каналу (телефону и пр.). Боб, получив криптограмму и зная код K, расшифровывает её, получая послание С.



Рисунок 1 – Последовательность действий для квантовой криптографии при использовании кодировки поляризационных состояний

В 1949 Шеннон, опираясь на разработанную им теорию информации, доказал теорему, что данная криптосистема является абсолютно секретной, если секретный код истинно случайный и он используется только один раз. Однако на практике реализация данной системы наталкивается на серьёзные трудности. Одна из них – создание и передача большого секретного кода, необходимого каждый раз, когда посылается новое сообщение. Избежать этой сложности можно было бы при наличии физического канала, секретность которого обеспечивалась бы физическими законами. Именно такой канал и представляет квантовая физика. Квантовая криптография опирается на невозможность клонирования отдельного квантового объекта. Если в качестве передатчика секретного кода выступают состояния отдельных частиц, то при попытке зарегистрировать эти состояния внешним наблюдателем они разрушаются. Факт попытки перехвата можно обнаружить, используя определенное соглашение (протокол) между Алисой и Бобом [3].

Один из таких протоколов связан с кодировкой поляризационных состояний фотонов в двух альтернативных базисах, не ортогональных друг другу.

Передача секретного кода осуществляется в несколько этапов (рисунок 1). Предварительно Алиса и Боб договариваются о кодировке (фотоны с поляризацией 0° и 45° кодируют число 0, фотоны с поляризацией 90° и 135° – единицу). Затем Алиса случайным образом меняет поляризацию фотонов, посылаемых по квантовому каналу Бобу. Боб измеряет поляризацию получаемых фотонов, случайным образом меняя ориентацию анализатора для распознавания поляризации 0° и 90° или 45° и 135°. Криптосистема будет секретной только в случае, если используемый код случайный. Именно случайности кода и добиваются Алиса и Боб, случайно меняя поляризаторы. По открытому каналу Боб сообщает Алисе, какой тип измерения он выполнял для каждого фотона, а Алиса подтверждает, верно или нет он выбрал его. От всей последовательности только верно выбранные измерения, Алиса и Боб создают секретный код [7].

Внешний наблюдатель, пытаясь узнать секретный код, обязательно должен пытаться считывать информацию и квантового канала. Но при этом он вызовет несовпадения в кодах, которые получат Алиса и Боб, так как измерения внешнего наблюдателя необратимым образом разрушают поляризационные состояния фотонов, передаваемых по квантовому каналу. Делая проверку совпадений по случайной выборке, Алиса и Боб обнаружат превышение уровня ошибок по сравнению с уровнем ошибок, генерируемых детекторами. Тем самым будет установлен факт попытки нарушения секретности. Другим протоколом, который может использоваться при передаче квантового кода, является фазовая модуляция с интерферометрическим детектированием, основанным на интерференции.

**2 Передача квантовой информации через канал связи**

Любая схема передачи информации состоит из передатчика (возможно, включающего в себя устройство, кодирующее сообщения), канала связи и приёмника (с декодирующим устройством). Обычно все три названные компоненты описываются на языке классической физики и статистики. Посылаемый передатчиком сигнал (для простоты 0 или 1) подвергается в канале случайным помехам и может исказиться. Поэтому сигнал на выходе приёмника не обязательно совпадает с посланным сигналом, а качество связи характеризуется вероятностью ошибки. Обычно требуется разработать такую конструкцию приёмника, которая обеспечивала бы оптимальное обнаружение или оценивание посланного сигнала для заданного канала и метода передачи. Подобные задачи решаются методами теории статистических решений. Теория информации преследует цель: для заданного канала с помехами разработать методы кодирования и декодирования сигнала, которые позволили бы передавать за единицу времени большие сообщения, практически неуязвимые для помех. В квантовом мире передатчик приготовляет квантовое состояние носителя информации в зависимости от поступающего сообщения. Например, передатчиком может быть лазер, который излучает либо вертикально, либо горизонтально поляризованные фотоны. Посылаемый двоичный сигнал кодируется соответствующим состоянием поля излучения. В канале связи он искажается, и на приёмник поступают состояния, отличные от посланных передатчиком. Приёмник осуществляет квантовое измерение той или иной физической величины, возможно, с последующей обработкой получаемой классической информации. Конечный результат такого измерения – выходной сигнал 0 или 1, дающий более или менее достоверную оценку посланного исходного сигнала, причём качество линии связи вновь характеризуется вероятностью ошибки. Аналогия с классической линией связи очевидна. Рассмотрение понятия квантового измерения с информационно-статистической точки зрения привело к парадоксальному выводу: добавление независимого квантового шума в наблюдения позволяет увеличить количество получаемой информации. Парадокс в том, что такого никогда не бывает в классической статистике: добавление шума только портит качество наблюдений.

Важнейшая характеристика квантового канала – его классическая пропускная способность, т.е. предельная максимальная скорость безошибочной передачи классических сообщений при использовании оптимального кодирования/декодирования длинных сообщений. Из известного энтропийного неравенства вытекает, что количество передаваемой классической информации не может быть больше, чем log d, где d – размерность пространства квантового носителя информации. То обстоятельство, что любое гильбертово пространство содержит бесконечно много различных векторов состояний, не помогает передать неограниченное количество информации: чем больше состояний используется для передачи, тем они ближе друг к другу и, следовательно, неразличимее [5].

 Однако, классическая пропускная способность канала может быть увеличена путем использования дополнительной сцеплённости между входом и выходом канала. Сцеплённость играет роль «катализатора», выявляющего скрытые информационные ресурсы квантовой системы, но сама по себе не позволяет передавать информацию: это означало бы мгновенную передачу на конечное расстояние. Если канал без шума, то выигрыш в пропускной способности, обеспечиваемый сверхплотным кодированием, двукратен. Чем сильнее канал отличается от идеального, тем выигрыш больше, и для каналов с очень большим шумом может быть сколь угодно велик. Классическая пропускная способность с использованием сцеплённого состояния – самая большая. При передаче классической информации по квантовому каналу сообщение записывается в квантовом состоянии. Однако вся полнота информационного содержания не может быть сведена к классическому сообщению и заслуживает специального термина – квантовая информация, т.к. квантовое состояние содержит в себе информацию о статистике всевозможных, в том числе и взаимоисключающих (дополнительных) измерений системы. Количество квантовой информации измеряется величиной энтропии состояния.

Принципиальное отличие квантовой информации от классической заключается в невозможности копирования: не существует «квантового ксерокса», т.е. физического устройства, позволяющего копировать произвольное квантовое состояние. Теория предсказывает возможность нетривиального способа передачи квантовой информации, при котором носитель состояния физически не передаётся, а пересылается лишь некоторая классическая информация. Необходимым дополнительным ресурсом вновь становится сцеплённость между входом и выходом канала связи. Свести передачу произвольного квантового состояния только к передаче классической информации без использования дополнительного квантового ресурса невозможно: поскольку классическая информация копируема, это означало бы возможность копирования и квантовой информации. Квантовая пропускная способность – предельное максимальное количество квантовой информации, которое может быть сколь угодно точно передано каналом. Есть глубокая аналогия между квантовым каналом и каналом с подслушивателем, причём в квантовом случае роль перехватчика информации играет окружение рассматриваемой системы. Криптографические характеристики канала: пропускная способность для секретной передачи классической информации и скорость распределения случайного ключа.

**3 Передача квантовой информации через атмосферу**

Фотоны, распространяющиеся в открытом пространстве, не испытывают явления двулучепреломления. Поэтому эти среды лучше, чем оптоволокно подходят для поляризационного кодирования. Однако атмосфера приводит к другим шумовым воздействиям. Ниже рассмотрены некоторые из этих особенностей.

Открытое пространство (земная атмосфера) предоставляет широкие возможности для передачи фотонов различных длин волн, являясь альтернативой оптическому волокну. В качестве генераторов и приемников излучения в данном случае также используются лазеры и фотодетекторы (простейший пример – пульт дистанционного управления). Современные системы беспроводной передачи данных способны передавать световые сигналы на расстояние в несколько километров со скоростью до 160 Гбит/с (коммерческие системы — до 2,5 Гбит/с).

Как и в случае с оптическим волокном, наибольшая эффективность передачи достигается для фотонов определенных энергий (рисунок 2). Наиболее прозрачна земная атмосфера для излучения с длиной волны более 1 см. К сожалению, практическая реализация протоколов квантовой криптографии с использованием фотонов сантиметрового диапазона невозможна из-за малой величины энергии фотона и, следовательно, невозможности его эффективного детектирования, поэтому наиболее подходящими являются два спектральных окна: 0,3–1,3 мкм и 1,5–1,8 мкм, тем более что генераторы и приемники фотонов в данных диапазонах хорошо разработаны и широко применяются при передаче фотонов посредством оптического волокна [4].



Рисунок 2 – Прозрачность земной атмосферы для излучения различной

длины волны

При передаче фотонов через атмосферу существуют четыре основных вида потерь: дифракционные потери, статические атмосферные потери (рассеяние и поглощение), турбулентность атмосферы, оптические потери.

– Дифракционные потери приводят к увеличению диаметра светового пучка с увеличением расстояния передачи.

– Статические атмосферные потери возникают и при отсутствии турбулентности атмосферы и представляют собой процессы рассеяния и поглощения полезного сигнала. Причем дождь или легкий туман затрудняет, или даже делает практически невозможной, передачу сигнала. Затухание сигнала в данном случае зависит также и от угла его распространения по отношению к зениту и изменяется на 3–5 % при изменении угла от 0° до 50°.

– Турбулентность атмосферы может приводить к ряду негативных эффектов: увеличение диаметра светового пучка подобно тому, как это происходит вследствие дифракционных потерь, отклонение светового пучка, когерентные потери, колебание интенсивности пучка около его среднего значения.

– Оптические потери связаны с использованием телескопов для приема-передачи сигнала: диаметр принимаемого пучка может быть слишком велик, в результате чего возможны потери.

В случае одиночных фотонов дополнительной проблемой является фоновое излучение (Солнце, Луна, свет звезд), поэтому важным элементом практических схем является синхронизация между приемником и передатчиком, чтобы фотодетектор включался только на короткое время в момент прихода очередного фотона для уменьшения вероятности регистрации посторонних фотонов.

Очевидно, что слабые однофотонные сигналы будут в значительной мере подвержены описанным помехам, поэтому резко снизится скорость и расстояние эффективной передачи. Чтобы разрешить эту проблему были предложены схемы квантовой криптографии, использующие спутники на различных орбитах от 300 до 30 000 км. Эффективность передачи в данном случае возрастает из-за того, что плотность атмосферы падает с ростом высоты над Землей и потери при достижении фотоном спутника, находящегося на 300-километровой орбите сравнимы с потерями при прохождении 10–15 км у поверхности планеты. На сегодняшний день нескольким группам уже удалось достаточно эффективно передать одиночные фотоны в открытом пространстве на 7,8 км и 13 км [7].

Использование атмосферы в качестве среды передачи фотонов приводит к необходимости использования в экспериментальных установках телескопов для передачи и приема оптических сигналов.

**4 Применение оптического волокна**

Поскольку оптоволоконная оптика является относительно новой технологией, на данный момент не существует каких либо жестких стандартов на ее характеристики. Они не появятся до тех пор, пока рынок не склонится к определенному кругу продуктов. Тем не менее, существуют определенные стандарты на размеры оптоволокна, измерительную технику и два стандарта телекоммуникационных оптических сетей. Ниже приводятся некоторые особенности оптических волокон, которые необходимо учитывать при разработке квантовых криптографических систем.

 Излучение распространяется в волокне благодаря наличию профиля показателя преломления поперек сечения оптоволокна. Свет удерживается в волокне за счет эффекта полного внутреннего отражения. В волокне может существовать несколько мод (режимов распространения). Моды, по сути, являются различными решениями уравнения Максвелла для волновода и определяются частотой и поляризацией света.



Рисунок 3 – Типичное оптическое волокно

 На рисунке 3 приведено сечение обычного оптоволокна. Центральная область волокна называется сердцевиной. Если сердцевина достаточно большая, то в волокне может существовать много волноводных мод. Такие волокна называют многомодовыми и диаметр их сердцевины обычно равен 50 мкм. Отдельный фотон взаимодействует с таким набором мод как с незамкнутой системой. Следовательно, многомодовое волокно не является подходящим квантовым каналом. Если же диаметр сердцевины мал по сравнению с длиной волны, то в волокне распространяется одна волноводная мода. Для телекоммуникационных длин волн (т. е. 1,3, 1,5 мкм) типичный диаметр сердцевины равен 8 мкм. Одномодовые волокна хорошо подходят для передачи одиночных фотонов. Например, оптическая фаза на выходе волокна может устойчиво зависеть от фазы на входе. Таким образом, одномодовое волокно с цилиндрической симметрией может являться идеальным квантовым каналом. В действительности оптические волокна обладают определенными нарушениями симметрии. Это приводит к снятию вырождения мод по поляризации и приобретению ими различных постоянных распространения. Подобный эффект вызывается хроматической дисперсией (зависимостью групповой скорости от частоты). Поляризационные эффекты в одномодовых волокнах. Поляризационные эффекты являются источником ошибок для любых коммуникационных схем, как классических, так и квантовых [4].

Эффект двулучепреломления в современных оптоволокнах достаточно мал, чтобы оказывать влияние на классический канал связи. Для квантового канала даже очень малое двулучепреломление необходимо принимать во внимание. Все реализации квантовой связи, основанные на оптоволокне, сталкиваются с этой проблемой. Учет поляризационных эффектов важен не только для систем, основанных на кодировании поляризации, но и для систем, основанных на кодировании фазы. Рассмотрим в деталях четыре различных поляризационных эффекта: эффект геометрической фазы, двулучепреломление, дисперсию мод по поляризации, зависимость потерь от поляризации. Геометрическая фаза является разновидностью фазы Берри и может возникать при адиабатическом изменении параметров системы, осуществляющей движение по циклу. При распространении поляризованного света по волокну, замкнутому в петлю, адиабатическому изменению подвержен волновой вектор. Например, если в волокно ввести вертикально поляризованный свет, то сохранится ли на выходе направление поляризации? В принципе можно проследить изменение линейной поляризации вдоль такого волокна и определить угол, на который поворачивается вектор поляризации. Если петля остается на плоскости, то поляризация не меняется. Если же петля замыкается вследствие трехмерной конфигурации, то при параллельном переносе поляризация изменяется на величину очерченного телесного угла, которая и есть геометрическая фаза. Схожие соображения сохраняются и для эллиптической поляризации. По мере распространения две круговые поляризации, являющиеся собственными состояниями, приобретают противоположные геометрические фазы. Наличие геометрической фазы не является критичным для квантовой коммуникации. Для ее преодоления Алисе и Бобу необходимо изначально повернуть свои системы на некоторый угол. Если изменения геометрической фазы происходят медленно, то их возможно отследить и ввести в схему коммуникации с помощью активной обратной связи. Однако если изменения происходят слишком быстро, то связь может быть прервана. Следовательно, натянутые кабели, качающиеся на ветру, не являются подходящими. Двулучепреломление. Даже одномодовый волновод, строго говоря, не является одномодовым, поскольку он может поддерживать две вырожденные моды, которые преимущественно поляризованы в двух ортогональных направлениях. При идеальных условиях совершенной цилиндрической геометрии и изотропии вещества, ортогонально поляризованные моды не взаимодействуют. Однако в реальных условиях малые отклонения от цилиндрической геометрии или малые флуктуации в анизотропии вещества (например, вызываемые статическим напряжением в сердцевине волокна) приводят к смешиванию двух поляризационных состояний, снимая вырождение мод. Постоянные распространения становятся различными для мод, поляризованных в x- и y-направлениях. Это свойство называется двулучепреломление мод [5].

Существуют оптоволокна, сохраняющие состояние поляризации. В них преднамеренно создается сильное двулучепреломление, так что малые случайные флуктуации двулучепреломления существенно не влияют на поляризацию света. Один из способов создания сильного двулучепреломления состоит в нарушении цилиндрической симметрии и создания оптоволокон с эллиптической формой сердцевины либо подкладки. В другом методе двулучепреломление вызывается статическими упругими напряжениями. Если эффект двулучепреломления является устойчивым во времени, то Алиса и Боб могут его скомпенсировать. Так, эффект двулучепреломления является схожим с эффектом геометрической фазы и в дополнение к нему может оказывать влияние на эллиптичность света. Устойчивость эффекта требует медленного изменения температурного режима и механических напряжений. Дисперсия мод по поляризации приводит к наличию двух различных групповых скоростей для ортогонально поляризованных мод. Две групповые скорости локально создаются двулучепреломлением. В оптических волокнах локальная дисперсия приблизительно равна фазовой дисперсии. По порядку она составляет несколько пикосекунд на километр. Оптический импульс локально распределяется по “быстрой” и “медленной” моде. Но так как двулучепреломление мало, эти моды слабо взаимодействуют. Даже малые неоднородности в волноводе вызывают перекачку энергии из быстрой моды в медленную и наоборот. Дисперсия мод по поляризации схожа со случайным блужданием и нарастает пропорционально квадратному корню из длины волокна [6].

 Длина взаимодействия мод варьируется от нескольких до сотен метров в зависимости от типа волокна. При сильном взаимодействии мод уменьшается дисперсия мод по поляризации, поскольку моды не успевают далеко уйти друг от друга. В современных оптоволокнах взаимодействие мод увеличивается искусственно в процессе изготовления. Вызываемая этим эффектом деполяризация схожа с процессом потери когерентности. Чтобы избежать этого эффекта, в квантовых каналах связи используются лазерные импульсы со временем когерентности большим, чем наибольшее из времен задержки. Зависимостью потерь от поляризации можно пренебречь для оптоволокон, но она может оказаться существенной в таких оптических компонентах, как фазовые модуляторы. В частности, некоторые оптические волноводы поддерживают только одну поляризацию. Сама по себе зависимость потерь от поляризации является устойчивой, но при наложении двулучепреломления могут возникнуть флуктуации . Зависимость потерь от поляризации не описывается унитарным преобразованием в пространстве состояний поляризации. Также не сохраняется скалярное произведение. В частности, неортогональные состояния могут перейти в ортогональные с некоторыми потерями. Отметим, что это обстоятельство может быть использовано для перехвата информации. Как было отмечено выше, воздействие поляризационных эффектов может быть скомпенсировано. Рассмотрим вначале, что произойдет с состояние поляризации света, отраженного от обычного зеркала. Пусть зеркало расположено в плоскости xy, а импульс падает на него перпендикулярно. Ясно, что линейно поляризованный свет не испытает каких-либо изменений. Но две круговые поляризации света поменяются местами: правая перейдет в левую и наоборот. То же самое выполняется для эллиптически поляризованного света. Соответственно, на сфере Пуанкаре подобное преобразование. Эволюция состояния поляризации светового импульса на сфере Пуанкаре при распространении импульса по оптоволокну, на одном из концов которого установлено Фарадеевское зеркало. Начальное состояние поляризации вследствие распространения по волокну переходит в состояние 1. Прохождение через среду, осуществляющую Фарадеевское вращение, приводит к вращению 1 → 2. Отражение от зеркала описывается преобразованием 2 → 3. Второе прохождение через Фарадеевскую среду отображается как поворот на π/2. Обратное прохождение через волокно приводит к конечной поляризации, ортогональной начальной описывается симметричным отображением относительно экваториальной плоскости. Причем, это преобразование не является унитарным. Рассмотрим далее воздействие Фарадеевского вращателя. Он вызывает поворот вектора поляризации на сфере Пуанкаре относительно вертикальной оси на угол π/2. Эффект Фарадея не является взаимным, и, следовательно, направление вращения не зависит от направления распространения света. Соответственно, после отражения на зеркале и после второго прохождения через Фарадеевский вращатель поляризация осуществляет поворот на π/2 в том же направлении. В итоге выходное состояние поляризации, после прохождения того же оптоволокна, оказывается ортогональным начальному [1].

В дополнение к поляризационным эффектам хроматическая дисперсия также может вызывать определенные проблемы. Например, схемы фазового и фазовременного кодирования основываются на предположении, что фотоны локализованы в пространстве и приходят в определенные моменты времени. Однако в дисперсионной среде, такой как оптоволокно, различные групповые скорости действуют как шум. Следовательно, спектральная ширина фотонов и их пространственное размытие связаны. Это подразумевает использование фотонов, спектральная ширина которых мала, или фотонов в области малой хроматической дисперсии. Для стандартных оптоволокон это область расположена около 1310 нм (второе телекоммуникационное окно). Потери на этой длине волны относительно малы и составляют ∼0,35 дБ/км. Третье телекоммуникационное окно находится вблизи 1550 нм, где потери достигают своего абсолютного минимума (0,25 дБ/км). Первое телекоммуникационное окно (800 нм) не используется, поскольку для этого требуются специфические источники и детекторы. Хроматическая дисперсия также зависит от параметров волокна: диаметра сердцевины и разности показателей преломления сердцевины и подкладки. Это можно использовать для смещения длины волны нулевой дисперсии. Хроматическая дисперсия не представляет серьезной проблемы для ослабленных лазерных импульсов, поскольку их спектральная ширина мала. Однако она становится проблемой при использовании фотонов, полученных в ходе параметрического распада. Для компенсации размывания фотонов могут использоваться перепутанные по времени фотоны. Также для компенсации хроматической дисперсии могут использоваться дополнительные волокна с отрицательной дисперсией.

**ЗАКЛЮЧЕНИЕ**

Основные результаты курсового проекта состоят в следующем:

1 Изучена литература, посвященная квантовой криптографии.

2 Были рассмотрены методы, используемые для построения физического канала передачи информации, а также протоколы квантовой криптографии.

3 Исследована применимость оптического волокна, как канала для передачи квантовой информации.

4 Были изучены принципы передачи квантовой информации в квантово-криптографических системах. При изучении принципов передачи информации были рассмотрены два способа ее передачи: через физический канал и через атмосферу. В обоих случаях посылаемая информация будет отличаться от полученной. В физическом канале это связано со случайными помехами самого канала, также немало важную роль играет качество этого канала. При передаче квантовой информации через атмосферу существуют четыре вида потерь: дифракционные потери, статические атмосферные потери (рассеяние и поглощение), турбулентность атмосферы, оптические потери.

**СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

1 Физика квантовой информации / Д. Бауместер [и др.] − М. : Постмаркет, 2003. − 375 с.

2 Чмора, А. Л. Современная прикладная криптография / А. Л. Чмора − М.: Гелиос АРВ, 2002. − 244 с.

3 Килин С. Я. Квантовая информация / С. Я. Килин // Успехи физических наук. − 1999. − Т.169, № 5. − С. 507−525.

4 Килин С. Я. Квантовая криптография: идеи и практика / С. Я. Килин, Д.Б. Хорошко – Минск: Беларуская наука, 2007. – 391 с.

5 Альбов А. Квантовая криптография / А. Альбов – Страта, 2016.– 236 с.

6 Килин, С. Я. Квантовая оптика: поля и их детектирование / С. Я. Килин. – М.: Едиториал УРСС, 2003. – 176 с.

7 Харин, Ю. С. Математические основы криптологии / Ю. С. Харин, В. И. Берник, Г. В. Матвеев. – Минск: БГУ, 1999. – 319 с.