Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Санкт-петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича»

(СПбГУТ)

Отчет  
о научно-исследовательской работе

Оптические системы связи

КВАНТОВЫЕ КОММУНИКАЦИИ: ИСТОРИЯ И ПЕРСПЕКТИВЫ

(заключительный)

Руководитель,  
канд. техн. наук,  
доцент каф. ССС Лукин. К. И.

подпись, дата

Зав. кафедрой ССС,  
д-р. техн. наук, доцент Котов В. В.

подпись, дата

Исполнитель,  
группа ИКТС-72 Теребенина Ю.Д.

подпись, дата

РЕферат

Отчет 27 с.. 1 кн.. 6 рис., 7 источн., 1 прил.

КВАНТОВЫЕ КОММУНИКАЦИИ, КРИПТОГРАФИЯ, ШИФРОВАНИЕ, КОДИРОВАНИЕ, КЛЮЧ, ПРОТОКОЛ, ФОТОН, БАЗИС, БОКОВЫЕ ЧАСТОТЫ, ВОЛС

Объектом исследования являются квантовые коммуникации.

Цель работы — изучить, что такое квантовых коммуникаций, как они появились, их возможности и основные принципы работы.

В процессе работы проводились исследования по изучению истории криптографии и квантовых коммуникаций, так же были разобраны квантовым коммуникациям по волоконно-оптическим линиям связи.

В результате исследования было выяснено, что в России разработана и введена в эксплуатацию самая длинная в мире ВОЛС с квантовым шифрованием.

Степень внедрения — рынок квантовых технологий пока невелик, но он стремительно развивается.

Содержание

[Термины и определения 4](#_Toc72101573)

[Перечень сокращений и обозначений 5](#_Toc72101574)

[Введение 6](#_Toc72101575)

[1 История криптографии 7](#_Toc72101576)

[1.1 Как была изобретена квантовая криптография? 11](#_Toc72101577)

[2 Квантовые коммуникации 12](#_Toc72101578)

[2.1 Принцип квантового распределения ключей 12](#_Toc72101579)

[2.2 Квантовые протоколы передачи данных 13](#_Toc72101580)

[2.3 Квантовые коммуникации по ВОЛС 17](#_Toc72101581)

[2.4 Использование боковых частотах модулированного излучения 18](#_Toc72101582)

[2.5 Самая длинная в мире ВОЛС с квантовым шифрованием 21](#_Toc72101583)

[2.6 Перспективы квантовых коммуникаций 22](#_Toc72101584)

[Заключение 24](#_Toc72101585)

[Список использованных источников 26](#_Toc72101586)

[Приложение А Прогноз динамики развития квантовых коммуникаций 27](#_Toc72101587)

Термины и определения

В настоящем отчете о НИР применяют следующие термины с соответствующими определениями.

Базис – упорядоченный набор векторов в векторном пространстве, такой, что любой вектор этого пространства может быть единственным образом представлен в виде линейной комбинации векторов из этого набора

Блокчейн – это база данных, в которой блоки информации, организованные строго определенным образом, идут друг за другом

Кубит – квантовый разряд, или наименьший элемент для хранения информации в квантовом компьютере

Поляризация – процессы и состояния, связанные с разделением каких-либо объектов, преимущественно в пространстве

DataEncryptionSystem – симметричный алгоритм шифрования, в котором один ключ используется как для шифрования, так и для расшифрования данных

RivestShamirAdleman – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел

WavelengthDivisionMultiplexing – разделение спектрального ресурса оптического волокна между длинами световых волн с последующим мультиплексированием

Перечень сокращений и обозначений

В настоящем отчете о НИР применяют следующие сокращения и обозначения.

ВОЛС – Волоконно-оптическая линия связи

ККЦ КНИТУ-КАИ – Казанский квантовый центр Казанского национального исследовательского технического университета им. А. Н. Туполева-КАИ

DES – Data Encryption System

IBM – International Business Machines

RSA – Rivest, Shamir, Adleman

WDM – Wavelength Division Multiplexing

Введение

Квантовые коммуникации представляют собой технологию криптографической защиты информации, использующей для передачи ключей индивидуальные квантовые частицы. Главное преимущество квантовых коммуникаций — защищенность информации, гарантированная законами физики.

Ключевой вопрос в том, как сделать это эффективно, так как мы используем не идеальную систему, а физические линии связи – оптическое волокно или открытое пространство. На пути к получателю на фотон может воздействовать много факторов, которые могут его разрушить. Так как мы говорим о практическом применении, нас интересует скорость передачи данных между такими системами и максимальное расстояние, на которое мы можем разнести узлы.

Традиционной задачей криптографии является проблема обеспечения конфиденциальности информации при передаче сообщений по открытому каналу, который контролируется злоумышленниками, которые могут пытаться делать что угодно, использовать любой инструментарий и оборудование, но перехватить данные они не должен.

В простейшем случае криптографический сценарий можно описать взаимодействие трех сторон: владелец информации (отправитель, передатчик), получатель (приемник) и злоумышленник (противник).

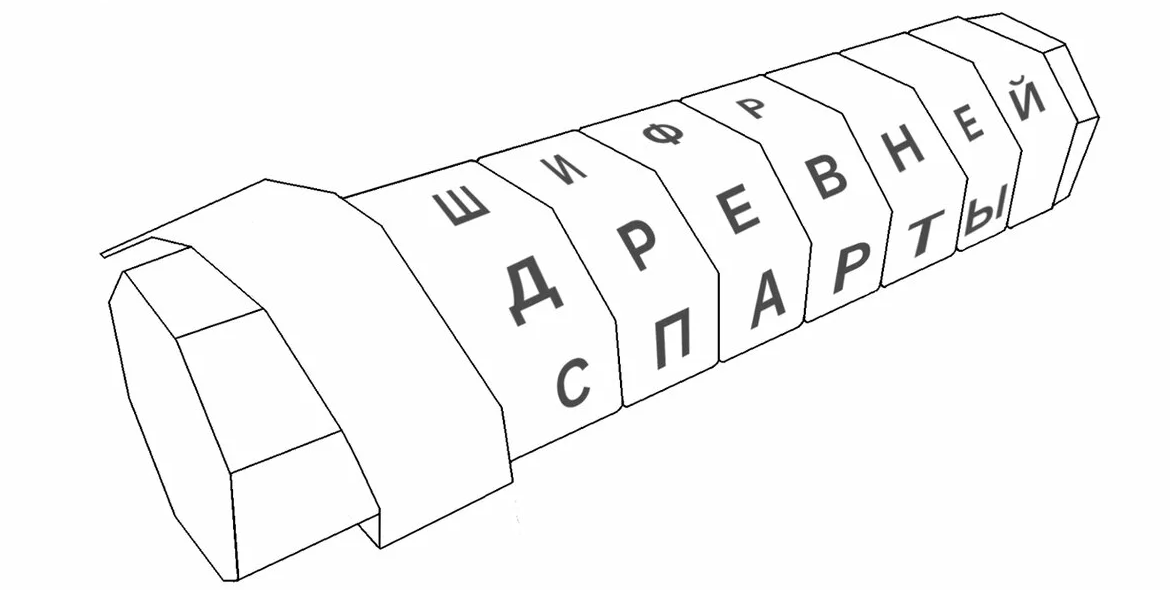
Квантовые коммуникации устраняют угрозы информационной безопасности, в том числе — со стороны квантовых компьютеров. Приоритетными отраслями для их внедрения являются: защита национальных информационно-телекоммуникационных сетей, обеспечение защиты информации для финансового сектора, государственных органов, крупных технологических компаний и держателей критической информационной инфраструктуры.

# История криптографии

Всевозможные способы усложнения задачи получения злоумышленником доступа к передаваемой информации — одна из центральных идей криптографии с самого начала ее развития.

Криптографические методы использовались еще в древних цивилизациях, таких как Месопотамия, Индия, Китай и Египет. Один из первых криптографических приборов был создан в пятом веке в Спарте.

Данный прибор, называемый сциталой — цилиндр с заранее обусловленным диаметром, известный лишь легитимным сторонам коммуникаций. Тонкая полоска из пергамента наматывалась на цилиндр, а текст выписывался вдоль его оси (рисунок 1). В этом случае секретным параметром является диаметр цилиндра, который подбирается относительно просто.



1. Сцитала

Для сообщения между легионами, разбросанными по Римской республике, Гай Юлий Цезарь использовал шифр, в котором каждая буква сообщения сдвигалась на определенное число букв по алфавиту.

В средние века использовались различные криптографические схемы, основанные на замещениях, перестановках и их комбинациях. В этих случаях ключом является число смещения или таблица подстановки. В отсутствие вычислительной машины, которая могла бы достаточно эффективно перебирать все возможные варианты, задача извлечения информации требовала большого количества времени.

По мере развития криптографии некоторые ее примитивы получили более точное математическое описание. В частности, возникло определение шифрования — семейства обратимых преобразований открытого текста, определяемого криптографическим ключом, а также порядком применения данного преобразования.

Во время Второй Мировой войны Германия использовала электромеханическое устройство «Энигма» для шифрования сообщений. На тот момент казалось, что количество переборных вариантов настолько велико, что «вскрыть» зашифрованное ее сообщение практически невозможно.[1]

Ошибка немецких криптографов состояла в том, что при использовании «Энигмы» каждый день в зашифрованном виде передавалось стандартное сообщение — прогнозы погоды. Знание этого, а также других особенностей сообщений, упростило процедуру дешифрования.

Исторический опыт сформулировал две важных криптографических парадигмы. Если рассматривать определение криптографического алгоритма как совокупности алгоритмов шифрования и расшифровывания, а также криптографического ключа, то для его криптографической стойкости необходимо учитывать следующее:

* мощь криптосистемы не должна основываться на незнании взломщика принципов работы алгоритма, безопасность алгоритмов и протоколов должна быть независимой от их секретности (принцип Керкгоффса);
* нужно проектировать криптографические системы, исходя из предположения, что противник с ними полностью ознакомится (принцип Шеннона).

В начале XX века в работах Клода Шеннона и Владимира Котельникова были сформулированы требования к абсолютно защищенной криптографической системе, позже получившей название «Одноразовый блокнот» или известный также как «шифр Вернама». Она остается стойкой даже при наличии у злоумышленника неограниченных вычислительных ресурсов. [1]

При этом необходимо соблюсти несколько требований:

* ключ генерируется для каждого сообщения;
* ключ статистически надёжен, то есть вероятности появления каждого из возможных символов равны, символы в ключевой последовательности независимы и случайны;
* длина ключа равна или больше длины сообщения;
* исходный (открытый) текст обладает некоторой избыточностью, что является критерием оценки правильности расшифровки.

Исходя из анализа этих требований, можно сделать вывод о том, что центральной и наиболее важной задачей криптографии является задача распределения криптографических ключей. Одна из проблем криптографии состоит в том, что чем больше информации передается с помощью одного ключа, тем большей становится так называемая «нагрузка на ключ», и тем больше данных накапливается для криптоанализа.

Одним из возможных решений задачи распределения ключей является криптография с открытым ключом, заложенная в работах Мартина Хелмана, Уитфилда Диффи и Ральфа Меркла. Она заключается в использовании для распределения ключей односторонних математических функций. Их основным свойством является, с одной стороны, легкость вычисления функции по известному аргументу, а с другой стороны — сложность вычисления аргумента по известному значению заданной функции. [1]

Примером такой «односторонней» задачи является факторизация: перемножить два простых больших числа легко, тогда как сказать, из каких простых множителей состоит заданное число, вычислительно сложно. Именно на предположении о сложности решения некоторых классов математических задач основывается современная криптографическая защиты информации.

Примером является распространенный криптографический алгоритм RSA. Криптография с открытым ключом требует наличия двух ключей: открытого ключа и секретного ключа, которые образуют пару. Получатель послания генерирует два ключа, делает открытый ключ общедоступным, а секретный ключ сохраняет в секрете.

Методы криптографии с открытым ключом могут быть использованы для обеспечения ключами симметричных криптографических алгоритмов. В симметричных криптографических алгоритмах один и тот же ключ используется как для шифрования, так и для расшифровки сообщения. Секретность передачи зашифрованных данных ограничивается, в том числе, секретностью способа распределения ключей.

Именно поэтому используются криптографические методы с открытым ключом. Тем не менее, секретность таких систем, как упоминалось выше, основывается на вычислительной сложности некоторых классов математических задач. Сегодня такой технологический стек, совмещающий криптографию с открытым ключом с симметричной криптографией, достаточно широко распространен. С его помощью защищается подавляющее большинство данных, передаваемых в интернете.

Отличным примером решений на основе вычислительной сложности является DES и основанные на ней различные системы. DES была разработана IBM в 1975 г. Эта система использует очень простые арифметические операции, что позволяет выполнять кодирование электронными устройствами и достигать очень высокой скорости работы. [1]

## Как была изобретена квантовая криптография?

В конце 1960-х годов студент университета Колумбии Стивен Визнер поделился со своим приятелем Чарльзом Беннетом идеей, как сделать банкноты, абсолютно защищенные от подделки.

Для этого на каждую банкноту следовало поместить ловушку для фотонов, причем каждый фотон должен быть поляризован в одном из двух базисов: либо под углом 0 и 90, либо 45 и 135 градусов. Комбинацию поляризаций и базисов, соответствующую серийному номеру банкноты, знает только банк. [2]

Если злоумышленник попытается воспроизвести банкноту, он должен будет измерить поляризацию каждого фотона. Поскольку он не знает, в каких базисах нужно измерять поляризацию, то он не сможет получить верные данные о состояниях фотонов, и его затея провалится. Идею Визнера использовать квантовые методы для защиты информации долго не признавали.

Первый реальный эксперимент по квантовой передаче данных они провели только в 1989 году — квантовая связь была установлена на дистанции 32,5 сантиметра. Прибор менял поляризацию передаваемых фотонов, но при этом шумел по-разному в зависимости от поляризации.

Первой коммерческой компанией, которая вывела на рынок системы квантового распределения ключей, стала американская компания MagiQ Technologies в 2003 году.

В 2007 году система квантовой защищенной связи, разработанная компанией Id Quantique, впервые использовалась для защиты данных о результатах голосования на парламентских выборах в швейцарском кантоне Женева.[2]

# Квантовые коммуникации

Квантовые коммуникации — технология кодирования и передачи данных в квантовых состояниях фотонов. Законы физики не позволяют измерить квантовое состояние так, чтобы оно не изменилось, поэтому квантовый канал связи невозможно прослушать незаметно для адресатов. [2]

## Принцип квантового распределения ключей

Представьте, что вы отправляете письмо, написанное на бумаге, цвет которой необратимо меняется, если вскрыть конверт. Тогда ваш адресат по цвету бумаги сможет понять, читал ли кто-то письмо до него.

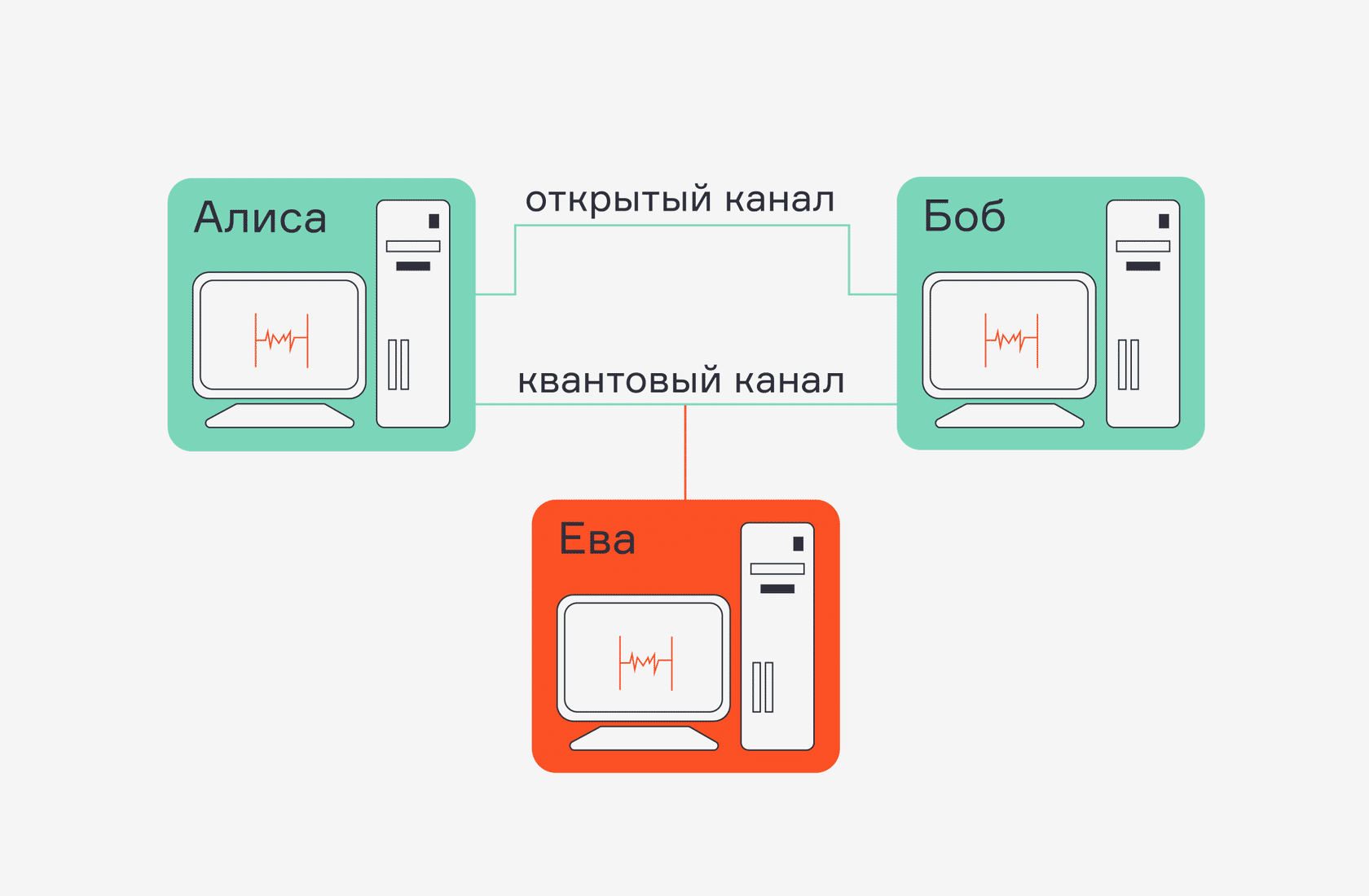
Точно так же устроена и квантовая криптография: данные кодируются в состояниях фотона, которые в соответствии с законами квантовой механики необратимо меняются при попытке измерения.

В теории для квантовой связи можно использовать любые объекты, способные находиться в двух разных квантовых состояниях, иначе говоря, любые кубиты. Однако из-за широкого распространения волоконно-оптических сетей фотоны остаются практически единственным вариантом для квантовой криптографии.

В обычных волоконных линиях информация кодируется в импульсах излучения лазера, например в двухуровневой форме.

Для квантовой связи данные кодируются в состояниях одиночных фотонов — например, в поляризации или фазе. Так, одному варианту поляризации приписывается значение — 1, противоположному — 0.

Два главных участника квантовой беседы традиционно обозначаются как Алиса (отправитель сообщения) и Боб (получатель), иногда к этим героям присоединяется третий — Ева, которая пытается подслушать разговор (рисунок 2). Когда Ева измеряет фотоны, их состояния меняются, и Боб понимает, что линия связи скомпрометирована. [2]



1. Схема организации квантовой связи

Однако в реальных сетях квантовая коммуникация устроена несколько иначе: ключи не формируются в процессе так называемого общения Алисы и Боба, а распределяются по всем участникам сети из одной точки, поэтому технология и называется «квантовое распределение ключей».

## Квантовые протоколы передачи данных

Протоколы квантового распределения ключа описывают механизм работы квантовой связи. В 1984 году Чарльз Беннет и Жиль Брассар придумали первый квантовый протокол передачи данных — BB84, который и сегодня активно используется во многих коммерческих системах.

Для передачи информации используются поляризованные фотоны. Алиса — отправитель сообщения поляризует фотоны в двух разных базисах — под углом 0 и 90 градусов, либо 45 и 135 градусов, причем базисы выбираются каждый раз случайным образом. Затем получатель — Боб получает фотоны и измеряет их состояния, тоже выбирая базисы случайно, как показано на рисунке 3.

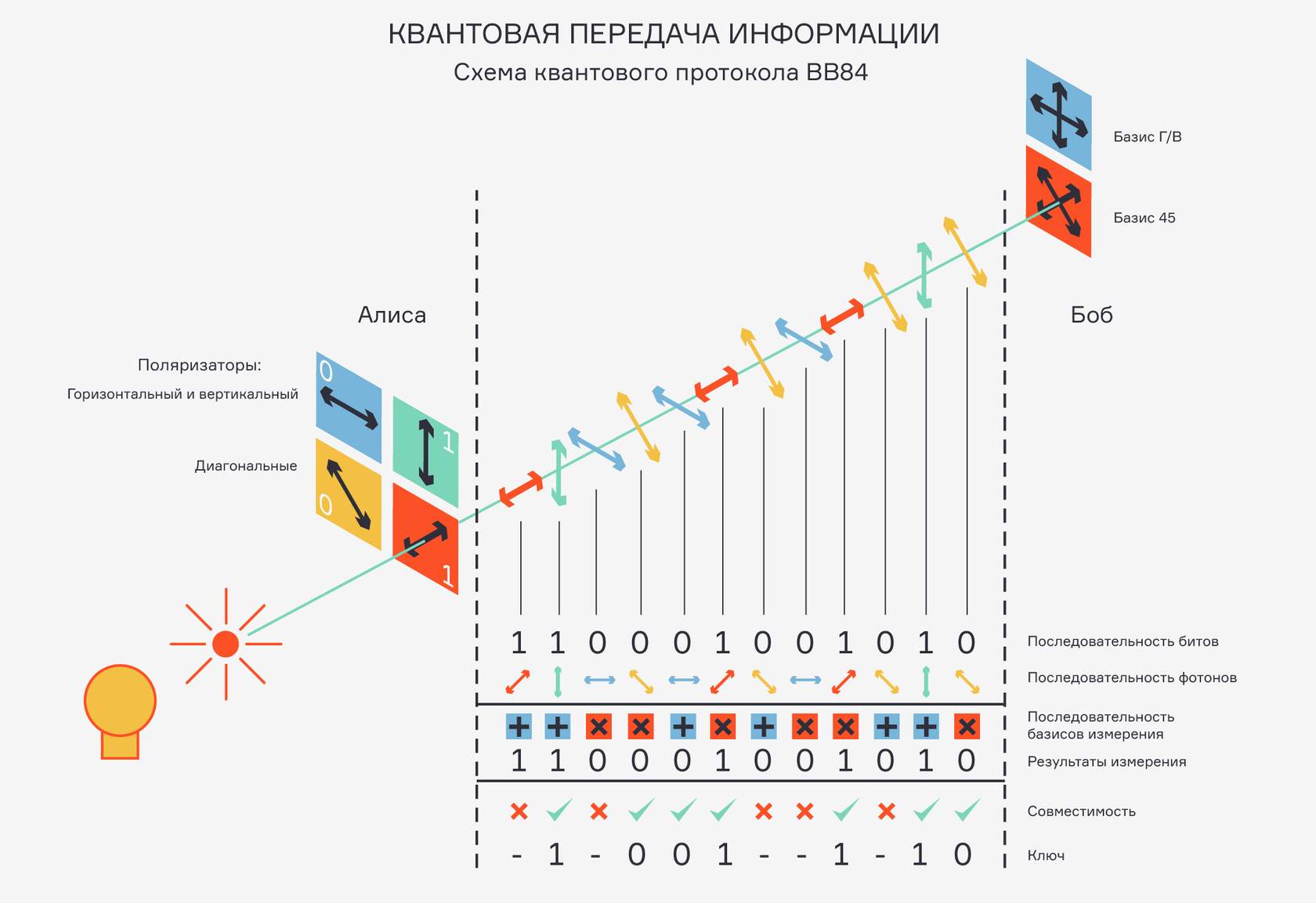
После этого Алиса по открытому каналу сообщает Бобу набор использованных базисов, Боб отбрасывает не совпавшие базисы и говорит Алисе, какие данные не прошли. При этом сами результаты измерений по открытому каналу не передаются.

Несмотря на это, у отправителя и получателя оказывается ключ — одинаковая последовательность нулей и единиц. Если Ева захочет перехватить данные, она должна будет измерять поляризацию фотонов, но она не знает базиса, поэтому, если не угадает правильно, не сможет получить верных данных.

Кроме того, само измерение изменит поляризацию, и ошибки обнаружат и Алиса, и Боб. В этом случае они просто «сбросят» испорченную часть данных, и Ева останется ни с чем.

В случае протокола BB84 допустимый уровень ошибок, вызванных разными причинами, — 11 процентов, если он выше, то считается, что канал прослушивается.

Данный протокол в модернизированном виде может обеспечивать скорость передачи 2,38 Мбит/с на дистанции 25 километров, и 52 кбит/с — на дистанции 70 километров.



1. Схема работы квантового протокола BB84

Аналогом протокола BB84, в котором для передачи данных используется не поляризация, а фаза фотонов, является протокол  B92, предложенный Беннетом в 1992 году. Одно из его преимуществ — увеличенная скорость генерации квантовых битов по сравнению с BB84.

Более современные протоколы DPS и COW позволяют обеспечить большую дальность передачи — до 250 и даже 300 километров. Однако для этих двух протоколов еще нет строгого доказательства защищенности.

В протоколе E91 используется явление квантовой запутанности. Суть его в том, что Алиса и Боб получают квантово запутанные пары фотонов и при измерении получают связанные значения. Однако этот протокол пока считается экзотикой, так как создание запутанных пар фотонов — сложная и ресурсоемкая задача. [2]

Различные типы кодирования информации в квантовых сетях представлены на рисунке 4.



1. Типы кодирования информации в квантовых сетях

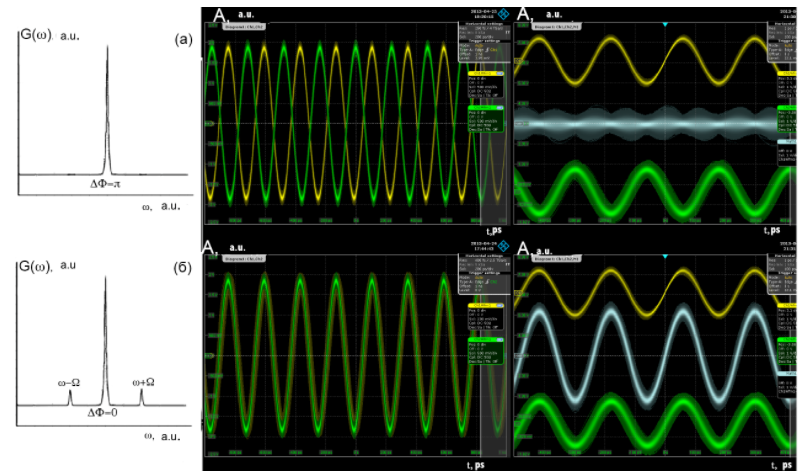
## Квантовые коммуникации по ВОЛС

При построении системы квантовой связи, генерируют слабый импульс, эквивалентный или близкий к энергии одиночного фотона, и отправляют его по линии связи. Чтобы закодировать в импульсе квантовую информацию, проводят модуляцию сигнала – изменяют поляризацию или фазовое состояние. Если мы говорим про волоконно-оптические линии связи, для них более эффективно использовать фазовые состояния, потому что сохранять и передавать поляризацию они не умеют.

Вообще фаза фотона – это вульгаризм, который придумали экспериментаторы в области квантовой физики. Фотон – это частица, у нее нет фазы, но она является частью волны. А фаза волны – это характеристика, которая показывает некоторую отстройку состояния поля электромагнитной волны. Если представить волну как синусоиду на координатной плоскости, сдвиги ее положения относительно начала координат соответствуют некоторым состояниям фазы. [3]

Для того чтобы закодировать в импульсе квантовую информацию, используют модулирующее устройство, которое сдвигает волну, а чтобы измерить сдвиг, мы складываем эту волну с такой же и смотрим, что получится. Если волны находятся в противофазе, то две величины накладываются и гасят друг друга, соответственно на выходе мы получаем ноль (рисунок 5, а). Если же мы угадали, то синусоиды складываются, поле увеличивается и итоговый сигнал получается высокий (рисунок 5, б) - это называется конструктивной интерференцией излучения.

Итак, если наши фазовые предположения совпали и сигнал усилился, значит, фазу фотона мы измерили правильно. В классических системах квантовой коммуникации используются распределенные интерферометры, и они определяют квантовую информацию по положению сдвига фазы волны.



1. Спектр и осциллограмма (а) ослабляющей и (б) усиливающей интерференции

Воплотить это на практике достаточно сложно, так как линии связи могут греться и охлаждаться, может присутствовать вибрация, все это влияет и меняет качество передачи. Фаза волны начинает смещаться сама, и мы не знаем, то ли отправитель ее так «промодулировал», то ли это помехи.

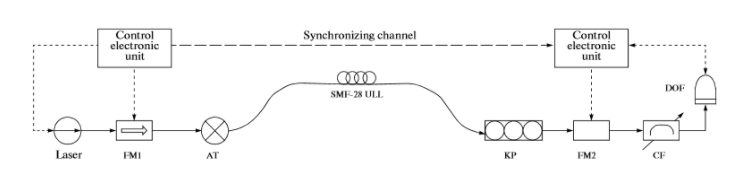
## Использование боковых частотах модулированного излучения

В ряде работ предложена интересная возможность мультиплексирования квантовых каналов в системах квантового распределения ключей на боковых частотах модулированного излучения. В этом классе систем квантовые состояния не излучаются непосредственно источником, а генерируются на боковых частотах спектра оптического сигнала за счёт его фазовой модуляции. На практике это реализуется следующим образом.

Мы берем лазер, который генерирует импульсы только на одной частоте, пропускаем импульс через электрооптический фазовый модулятор. На модулятор подается сигнал на другой частоте, существенно более низкой, и в результате кодирование осуществляется не основной синусоидой, а параметрами вспомогательной синусоиды – ее частотой смены фазы, фазовым положением. Далее передается квантовая информация отстройкой дополнительных частот в спектре импульса относительно центральной частоты. [3]

Такое шифрование становится куда более надежным, так как спектр передается по линиям связи одним импульсом, и если среда передачи вносит какие-то изменения, их претерпевает весь импульс целиком. Мы также можем добавить не одну дополнительную частоту, а несколько, и одним потоком единичных фотонов можем поддерживать до 10 независимых каналов связи. В итоге нам не нужен интерферометр в явном виде – он «зашит» внутри импульса, нет нужды в схемах компенсации дефектов в линии, нет ограничений на скорость и дальность передачи данных. В комбинации с WDM эта технология позволяет увеличить спектральную эффективность систем квантовой криптографии в оптических сетях с сегодняшних 4% до 40% и более, реализовав квантовые сети со скоростью передачи данных порядка 400 Мбит/с. Все это делает технологию экономически эффективной – сейчас скорость лучших в мире квантовых систем всего 1-2 Мбит/с, в то время как пропускная способность канала в сети Ethernet – порядка 1 Гбит/с.

На рисунке 6 приведена упрощённая схема системы. Полупроводниковый лазер генерирует излучение с узким спектром на длине волны 1550 нм. После этого излучение поступает в фазовый модулятор FM1, управляемый электронным блоком управления (control electronic unit). В результате фазовой модуляции появляются две боковые частоты, отличающиеся от несущей модулирующего радиосигнала на величину 4,4 ГГц. [6]



1. Принципиальная схема системы квантовой криптографии, основанной на применении боковых частот

Мощность боковых частот контролируется путем изменения амплитуды модулирующего сигнала. Модулированный сигнал поступает на аттенюатор AT, на выходе которого мощность сигнала на боковых частотах соответствует среднему числу фотонов на импульс. Каждый бит передаваемого сигнала кодируется с помощью фазового сдвига, добавляемого в модулирующий сигнал. Фазовый сдвиг контролируется электронным блоком управления и на каждый бит выбирается случайно из четырёх величин: 0, 45, 90 и 135 градусов.

Электронные блоки управления в передающем и принимающем модулях синхронизируются с помощью сигнала специальной формы: синусоиды с частотой 10 МГц и стробирующего импульса длительностью 10 нс. Стартовый строб-сигнал инициирует генерацию ключа, а последующие – синхронизируют запись квантовых отсчетов в буферную память передающего и принимающего модулей. Модуляционные генераторы передающего и принимающего модулей синхронизирует синусоидальный сигнал. Синхросигналы передаются по отдельному оптическому волокну.[6]

По протоколу BB84 генерируется криптографический ключ с сильным опорным импульсом. Квантовый сигнал в принимающем модуле возникает в момент прохождения поляризационного контроллера КР, фазового модулятора FM2 и спектрального фильтра СF, подключенных последовательно.

Спектральный фильтр выделяет сигнал боковых частот, который отслеживается с помощью детектора фотонов DOF. На этом этапе сигнал подвергается повторной фазовой модуляции. Фазовый модулятор FM2 управляется электронным блоком управления, а битовая последовательность кодируется точно так же как в передающем модуле. [6]

Обмен информацией, необходимой для обработки результатов измерения, выполняется по открытому каналу. При этом ключ генерируется одновременно в передающем и принимающем модулях. После вычисляется коэффициент ошибок, по которому легитимные пользователи могут определить, была ли предпринята попытка прослушивания. Если прослушивания не было, то ошибки корректируются, а в передающем и принимающем модулях генерируется секретный криптографический ключ.

В настоящее время кодирование квантовой информации на боковых частотах также развивают две научные группы во Франции и Испании, но в наиболее развернутом и полном виде система реализована в России.

## Самая длинная в мире ВОЛС с квантовым шифрованием

Казанский квантовый центр в 2019 году [провел тестирование ВОЛС](http://www.cnews.ru/news/top/2019-09-25_v_rossii_zarabotala_samaya) длиной 143 километра с квантовым шифрованием. По словам разработчиков, это достижение является мировым рекордом. Эксперимент проводился на сетях «Ростелекома» и «Таттелекома».

В 2018 году «Ростелеком» также тестировал квантовую линии связи, но тогда ее длина составила всего 58 километра. Эксперимент проводился на сетях двух операторов связи в Татарстане. ВОЛС продолжили от Лаборатории практической квантовой криптографии ККЦ КНИТУ-КАИ до узла связи «Ростелекома» в Апастово. [5]

Что касается криптографической линии связи, то участникам эксперимента удалось решить задачу передачи квантовых ключей по ВОЛС на большое расстояние. Для этого участники задействовали прототип комплекса передачи и приема данных с гибридной квантово-классической защитой. Комплекс, который разработан в КНИТУ-КАИ, дает возможность передавать квантовые ключи на большие расстояния.

В состав этого комплекса входят система квантового распределения ключей на боковых частотах, криптомаршрутизатор и высокоэффективный детектор одиночных фотонов, который выпущен российской компанией «СКОНТЕЛ». Исходная схема квантовой рассылки ключа разработана специалистами Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университет ИТМО). [5]

Оптические потери во время тестирования криптомаршрутизатора составили 37 дБ. При помощи потока одиночных фотонов участники эксперимента произвели обмен ключами. Была произведена их запись в квантовые состояния классической информации.

Частота смены фазы модуляции, по словам участников эксперимента, составила 100 МГц, среднее количество фотонов на один такт модуляции — 0,2. В ходе тестирования применялся 256-битный ключ до двух раз в минуту. Такую возможность обеспечила средняя скорость генерации ключей в канале.

Эксперты считают, что квантовые коммуникации обеспечивают наивысшую из существующих на сегодняшний день степень защиты передачи данных по ВОЛС, ведь технология основана на использовании фундаментальных законов квантовой физики, которые невозможно обойти.

## Перспективы квантовых коммуникаций

Квантовые коммуникации открывают новые возможности в области передачи и защиты данных. Прогноз динамика развития квантовых коммуникаций представлен в приложение А.

Среди перспективных направлений для разработок в области квантовых коммуникаций:

1. Квантовый блокчейн. Сегодня уже разработана платформа блокчейна, в рамках которой можно использовать квантовое распределение ключей. При определенных конфигурациях сети это позволяет отказаться от элементов блокчейна, которые уязвимы к атакам с помощью квантового компьютера. [4]
2. Квантовый интернет, основным преимуществом которого будет полная безопасность коммуникации. В первую очередь подобная защищенная сеть необходима для финансового сектора, госструктур и военной сферы, поскольку у них самая высокая потребность в безопасной передаче данных.
3. Технологии безопасности на базе квантовых коммуникаций: например, квантово-защищенные подписи для физических лиц.
4. Передача энергии на расстоянии. В основе возможности сбора и передачи энергии с помощью квантовых технологий лежит идея о том, что при квантовой телепортации измерение на первой частице вводит квантовую энергию в систему. Предполагается, что, тщательно выбирая измерение для второй частицы, можно извлечь исходную энергию. Это возможно, потому что существуют квантовые флуктуации в энергии любой частицы. Процесс телепортации позволяет вводить энергию квантов в одну точку Вселенной, а затем использовать квантовые энергетические колебания, чтобы извлечь ее из другой точки. Разумеется, энергия системы в целом не меняется. [4]
5. Беспроводная оптическая связь на открытом пространстве и на большие расстояния.

Заключение

Квантовые технологии начинают играть центральную роль в широком спектре технологических направлений. Квантовая криптография – это уже реальность, с которой мы в скором времени неизбежно столкнемся.

Квантовое шифрование позволяет ликвидировать одну из основных проблем современных систем шифрования — необходимость передавать по каналу связи ключи. Их можно перехватить, после чего шифрование теряет смысл — данные становятся доступными третьим лицам. Что касается квантовых систем шифрования, то здесь в случае подключения третьего лица к линии связи меняется состояние одиночных фотонов, что делает перехват информации невозможным в текущих условиях.

Есть и недостаток такого типа связи — легкость изменения состояния фотонов, из-за чего передавать информацию становиться затруднительным, если длина канала превышает 100 км. Скорость передачи также оставляет желать лучшего.

Вследствие чего, в большинстве случаев квантовая связь используется в пределах одного населенного пункта. Для больших дистанций квантовые сети строятся из множества отдельных фрагментов, связанных особо защищенными узлами.

Более высокой скоростью генерации ключей и низкой вероятностью возникновения ошибок характеризуются системы на боковых частотах. Однако их главным преимуществом является возможность генерировать сразу несколько боковых частот в окрестности одной центральной, что позволяет размещать до 10 независимых квантовых каналов внутри одного окна мультиплексора.

Сегодня на мировом рынке коммерческих систем квантовой коммуникации доминируют три компании: китайские Qasky и QuantumCTek, а также швейцарская ID Quantique. Они поставляют практически весь спектр решений и компонентов: начиная с источников и детекторов одиночных фотонов, квантовых генераторов случайных чисел до интегрированных устройств.

Квантовые коммуникации устраняют угрозы информационной безопасности, в том числе — со стороны квантовых компьютеров. Приоритетными отраслями для их внедрения являются: защита национальных информационно-телекоммуникационных сетей, обеспечение защиты информации для финансового сектора, государственных органов, крупных технологических компаний и держателей критической информационной инфраструктуры.

Смогут ли эти технологии изменить нашу жизнь? – зависит от того, как мы распорядимся созданным исследовательским потенциалом.

Список использованных источников

1. Как Россия потратит 11,2 млрд рублей на развитие квантовых коммуникаций [Электронный ресурс] / CNews, 28.02.2020 — URL: <https://www.cnews.ru/articles/2020-02-27_kak_rossiya_potratit_112_mlrd_rublej>
2. Квантовые технологии. Модуль 5 [Электронный ресурс] / N+1, 6 февраля 2020 — URL: [https://nplus1.ru/material/2020/02/06/course-quantum-technology-chapter5](https://nplus1.ru/material/2020/02/06/course-quantum-technology-chapter5#:~:text=Квантовые%20коммуникации%20(или%20квантовая%20криптография),данных%20в%20квантовых%20состояниях%20фотонов)
3. Абсолютная защита: что такое квантовые коммуникации и как они работают [Электронный ресурс] / ITMO.NEWS — URL: <https://news.itmo.ru/ru/archive/news/5070/null/>
4. Развитие квантовых технологий: основные направления приложения научных усилий [Электронный ресурс]. — 2017. — URL: <http://www.csr-nw.ru/files/publications/kvantovyj_forsajt1.pdf>
5. В России успешно протестирована самая длинная в мире ВОЛС с квантовым шифрованием [Электронный ресурс]. — 25 сентября 2019. — URL: <https://habr.com/ru/news/t/468893/>
6. Квантовые коммуникации: от НИР до технологического бизнеса [Электронный ресурс]. — 20 октября 2015. — URL: <https://habr.com/ru/company/spbifmo/blog/269127/>
7. Принцип Керкгоффса [Электронный ресурс] / Википедия — URL: <https://ru.wikipedia.org/wiki/Принцип_Керкгоффса>
8. Прогноз динамики развития квантовых коммуникаций

