ИНТЕГРАЦИЯ СИСТЕМЫ ЗАЩИТЫ КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ МЕТОДАМИ КВАНТОВОЙ КРИПТОГРАФИИ НА ПРЕДПРИЯТИЯХ СТРАТЕГИЧЕСКОГО ЗНАЧЕНИЯ

С. А. Якунина, К. В. Леванов, Н. Н. Вовк, Е. А. Жуненко, А. Н. Гаврилин, Р. В. Ефремов, И. В. Понеделко, А. С. Егоров, М. С. Сазанов

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Введение

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.

Идея использования квантовых состояний была предложена еще в 1970 году студентом Колумбийского университета Стивеном Визнером. Он подал статью по теории кодирования в журнал IEEE Information Theory. Которая не была опубликована, так как изложенные в ней предположения показались фантастическими, а не научными. Стивен Визнер предложил использовать квантовые состояния для защиты денежных банкнот. Для этого было предложено встроить в каждую банкноту 20 световых ловушек, а затем поместить в каждую из них по одному фотону, поляризованному в строго определенном состоянии. После чего банкноты маркировались специальным серийным номером, который включал информацию о положении поляризационного фотонного фильтра. В результате этого, при применении отличного от заданного фильтра, комбинация поляризованных фотонов стиралась. Тогда развитие технологий еще не позволяло рассуждать о таких возможностях. Но в 1983 году работа Стивена Визнера «Сопряженное кодирование», все-таки была опубликована в SIGACT News и высоко оценена в научных кругах. В последствии опираясь на принципы, описанные в этой работе, ученые Чарльз Беннет и Жиль Брассард создали способ кодирования и передачи сообщений. Они подготовили доклад на тему «Квантовая криптография: Распределение ключа и подбрасывание монет». Протокол, который был описан в работе, в дальнейшем был признан первым базовым протоколом квантовой криптографии, и назван в честь его создателей BB84. Носителями информации в протоколе BB84 выступают фотоны, поляризованные под углами 0, 45, 90, 135 градусов. Суть метода квантовой криптографии заключается в наблюдении за квантовыми состояниями фотонов, которые задает отправитель информации, а получатель их регистрирует. Используется квантовый принцип неопределенности Гейзенберга, когда две квантовые величины нельзя изменить одновременно с необходимой точностью. В случае, если отправитель и получатель не договорятся, какой вид поляризации квантов будет взят за основу, получатель может разрушить посланный отправителем сигнал и не получит полезной информации. Практическая реализация квантовой криптографии показана на рис. 1. Передающая сторона находится слева, а принимающая – справа. Ячейки Покеля необходимы для импульсной вариации поляризации потока квантов передатчиком и для анализа импульсов поляризации приемником. Передатчик может формировать одно из четырех состояний поляризации. Передаваемые данные поступают в виде управляющих сигналов на эти ячейки. В качестве канала передачи данных может быть использовано оптоволокно. В качестве первичного источника света можно использовать лазер.

На принимающей стороне после ячейки Покеля установлена кальцитовая призма, которая расщепляет пучок на два фотодетектора (ФЭУ), измеряющие две ортогональные составляющие поляризации. При формировании передаваемых импульсов квантов возникает проблема их интенсивности, которую необходимо решать. Если квантов в импульсе 1000, есть вероятность, что 100 квантов по пути будет отведено злоумышленником на свой приемник. В последующем, анализируя открытые переговоры между передающей и принимающей стороной, он может получить нужную ему информацию. Поэтому в идеале число квантов в импульсе должно быть около одного.

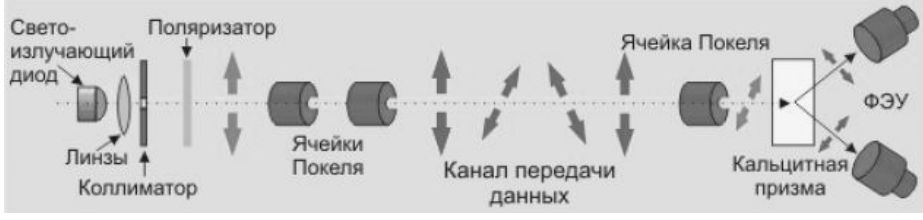


Рис. 1. Схема практической реализации квантовой криптографии

В этом случае любая попытка отвода части квантов злоумышленником приведет к существенному изменению всей системы в целом и, как следствие, росту числа ошибок у принимающей стороны. В подобной ситуации принятые данные должны быть отброшены, а попытка передачи повторена. Но, делая канал более устойчивым к перехвату, специалисты сталкиваются с проблемой "темнового" шума (получение сигнала, который не был отправлен передающей стороной, принимающей стороной) приемника, чувствительность которого повышена до максимума. Для того, чтобы обеспечить надежную передачу данных, логическому нулю и единице могут соответствовать определенные последовательности состояний, допускающие коррекцию одинарных и даже кратных ошибок.

Что такое квантовая криптография и ее отличие от обычной криптографии

Классическая криптография решает фактически только две задачи: защиту передаваемых сообщений от прочтения и от модификации сторонними лицами. Она базируется на использовании симметричных алгоритмов шифрования, в которых зашифровывание и расшифрование различаются лишь порядком исполнения и направлением некоторых простых шагов. Эти методы используют один и тот же скрытый элемент (ключ), и второе действие (расшифрование) является простым обращением первого (зашифрования). Поэтому любой из участников обмена может как зашифровать, так и расшифровать сообщение. По причине большой избыточности естественных языков непосредственно в зашифрованное сообщение очень тяжело внести осмысленное изменение, поэтому классическая криптография гарантирует также защиту от навязывания ложных данных. Если же естественной избыточности оказывается недостаточно для надежной защиты сообщения от модификации, она может быть искусственно увеличена методом добавления к нему особой контрольной комбинации. Если кратко, то защищенность классической криптографии строится на уверенности в том, что злоумышленник не успеет за разумное время «взломать» шифр ввиду сложности используемых алгоритмов.

Квантовая криптография – способ защиты коммуникаций, основанный на определенных явлениях квантовой физики. В отличие от традиционной криптографии, которая использует математические способы, чтобы обеспечить секретность информации, квантовая криптография сконцентрирована на физике, изучая случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приема информации постоянно 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. Обобщенно можно сказать, что защищенность квантовой криптографии выстраивается на утверждении о том, что никто не сможет «взломать» шифр, так как это противоречит физическим законам природы.

Преимущества квантовой криптографии

К преимуществам квантовой криптографии можно отнести:

– обнаружение пассивного перехватчика – атака злоумышленника вносит значительно больше ошибок, чем их возникает в квантовом канале в результате естественного шума;

– теоретико-информационная стойкость распределения ключей – ключи, распределенные с помощью квантовых протоколов с теоретико-информационной стойкостью, используется для дальнейшего шифрования с использованием известных классических симметричных алгоритмов. Поэтому общий уровень стойкости криптосистемы повышается;

– защищенность основана на фундаментальных физических законах и принципах.

Использование методов квантового шифрования в организации сетей специального назначения

Квантовая связь (КС) – это некая система методов и средств передачи квантовой информации, т. е. данных, закодированных в квантовых состояниях, из одной пространственной точки или пользователя в другую. Носителями квантовой информации являются сами квантовые системы, которые могут существовать в различных квантовых состояниях. Существует несколько возможных способов осуществления этих принципов, разные подходы, которые, конечно, вносят свои перспективы по росту скорости и дальности передачи данных. Системы квантовой криптографии давно производятся коммерческими компаниями в исследовательских и научно-практических целях. Квантовые сигналы выносятся на боковые частоты, что позволяет сильно расширить характеристики по скорости и расстоянию и снять явные ограничения по дальности, присущие уже существующим схемам. Чтобы увидеть основное отличие упомянутого способа, рассмотрим сначала принципы работы классических, стандартизированных схем. Обычно при проектировании и построении системы квантовой связи генерируют ослабленный импульс, приблизительно равный или близкий к энергии одиночного фотона, после чего отправляют импульс по линии связи. Для кодировки в импульсе квантовых данных проводят модуляцию сигнала – изменяют поляризацию или фазовое состояние. В качестве основной модели электромагнитного излучения для физического кодирования квантовых данных с помощью выбора векторов поляризации монохроматического когерентного излучения приняты основные уравнения Максвелла:

$$\nabla E = \frac{\rho}{\varepsilon_0}$$ – закон Гаусса,

где E – вектор электрической напряженности; ρ – плотность тока смещения; ε – диэлектрическая проницаемость вакуума; ∇B = 0 – закон Гаусса для магнитного поля; $\nabla E = -\frac{\partial B}{\partial t}$ - связь электрического и магнитного полей;

$$\nabla B = j\mu_0 + \frac{1}{c^2}\frac{\partial E}{\partial t}$$ - циркуляция магнитного поля,

где B – вектор магнитной индукции; μ_0 – магнитная проницаемость вакуума.

Численные решения данных уравнений методом конечных разностей показывают правильность выбранных моделей и возможность практического применения поляризационного кодирования. Строго говоря, фаза фотона – это некое нарушение классической физики элементарных частиц, которое придумали экспериментаторы из этой же области с целью упрощения работы с полученными данными. Фотон – это частица, у нее нет фазы, однако сама по себе она является частью волны. А фаза волны – это характеристика, которая показывает некоторое положение состояния поля этой электромагнитной волны. Если попытаться изобразить волну как синусоиду на плоскости, то сдвиги ее положения относительно начала этой плоскости соответствуют некоторым состояниям фазы. Для сохранения и преобразования в импульсе квантовой информации должно использоваться модулирующее устройство, которое сдвигает волну, а для измерения этого сдвига мы чисто графически или математически складываем эту волну с такой же волной и проверяем, что получится. Если волны находятся в противофазе, то две величины аннигилируют свои значения и гасятся друг о друга, на выходе получаем практически чистый нуль. Если же мы угадали, то синусоиды накладываются, поле растет и конечный сигнал получается высоким. Обмен пользовательской информацией между конечными потребителями, разнесенными на некоторое расстояние, осуществляется с учетом типа квантовых состояний, которые могут быть неортогональными и сцепленными (перепутанными), в отличие от классических состояний. Запись (или кодирование) стандартной, классической информации в неортогональной КС позволяет сопровождать каждое отправленное сообщение новым, уникальным, собственным ключом, т. е. решить одну из главных тем и задач классической криптографии – абсолютно секретное распределение ключей шифрования. Свойство перепутанности квантовых состояний дает возможность осуществить доставку двух идентичных последовательностей информационных битов двум пользователям, разнесенным на конечное расстояние, с гарантией полной недоступности чтения содержащихся в них данных третьим лицам. Как в первом, так и во втором случае полная секретность обмена данных осуществляется не вычислительными и техническими возможностями пользователей, их оборудования и потенциального перехватчика, а законами природы, основанными на линейности и унитарности квантовых преобразований, а также на соотношениях неопределенностей.

Необходимо рассмотреть такое явление, как коллапс волновой функции, то есть мгновенное изменение волновой функции исследуемого объекта при попытке измерить его. Пусть M_i – состояние системы до текущего измерения; i – полученный результат; M_i' – измененное состояние системы; ρ – матрица плотности; ρ_i' – измененная матрица плотности; *TrMi* – след матрицы до проведения измерения.

Тогда с помощью преобразования оператора плотности исходное состояние в результате измерений будет преобразовано в $\rho' = \frac{\sqrt{M_i}}{TrM_i\rho}\rho\sqrt{M_i'}$.

Отсюда можно сделать вывод о том, что попытки измерить состояние системы приводят к возникновению помех в ней, а значит и к возникновению ошибок на стороне приемника. Наиболее подходящими квантовыми системами, используемыми в КС для передачи информации на большие расстояния, являются фотоны. Они распространяются со скоростью света, позволяют кодировать информацию в частотных, фазовых, амплитудных, поляризационных и временных переменных. К тому же использование фотонов как носителей информации позволяет применять ряд технологических достижений в области классических телекоммуникаций – оптические волоконные линии связи, всевозможные модуляторы и преобразователи оптических сигналов.

Любая подобная система квантовой связи состоит из источника или генератора квантовых состояний. Непосредственно из среды, в которой осуществляются и реализуются эти состояния (канала связи), а также детекторов, измеряющих сами состояния. Для генерации квантовых состояний на конечных отдельных фотонах обычно используют весьма сильно ослабленные импульсы, создаваемые лазерной установкой. Основными источниками одиночных фотонов являются полупроводниковые лазеры. Из большого спектра полупроводниковых лазеров обычно используют инжекционные лазеры на основе гетероструктур с высоким коэффициентом инжекции, рис. 2 и 3. Среди множества приемных устройств одиночных фотонов лавинные фотодиоды считаются наиболее перспективными. В приемниках данного типа лавинный пробой возникает, в результате ударной ионизации нейтральных атомов в *p-n*-переходе быстрыми электронами или дырками. В результате генерируются новые пары носителей заряда, которые, двигаясь в электрическом поле перехода, вновь при столкновении с атомами образуют новые пары носителей и т. д., т. е. носители в переходе лавинообразно размножаются. На рис. 4 приведена конструкция лавинного фотодиода на основе кремния. Гетеростуктура была получена методом молекулярнопучковой эпитаксии.

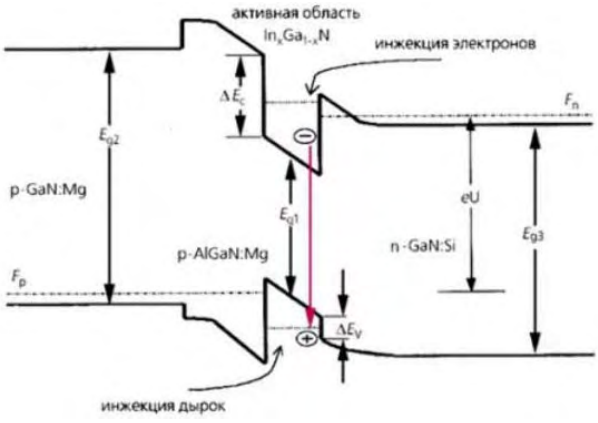


Рис. 2. Зонная диаграма энергетического спектра носителей заряда гетероструктуры с квантовыми ямами

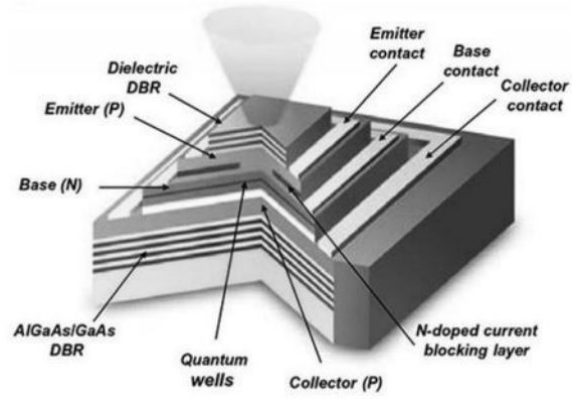
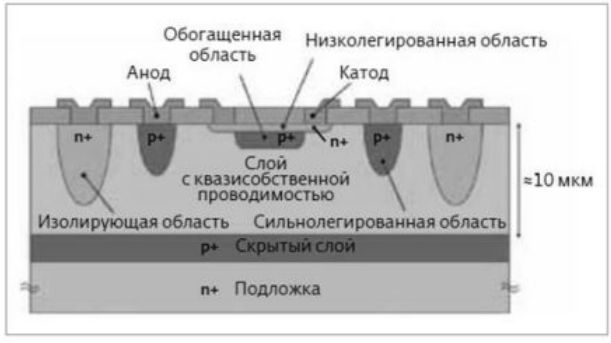


Рис. 3. Конструкция полупроводникового лазера с квантовыми ямами



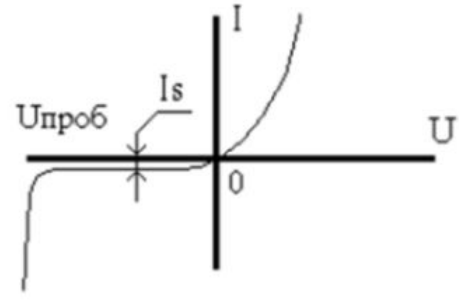


Рис. 4. Конструкция чипа лавинного фотодиода и его вольт-амперная характеристика

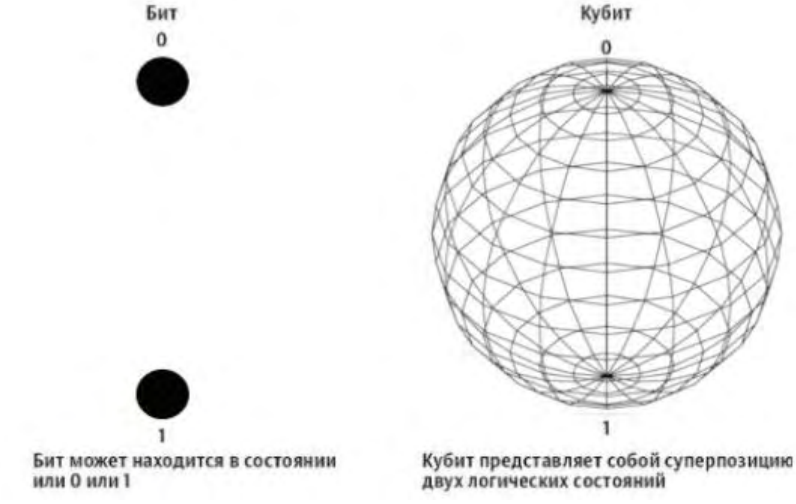


Рис. 5. Кубит квантовой информации

Квантовая механика позволяет корреспондентам на узлах связи A и B получить одинаковые квантовые состояния несущих частиц, обмениваясь кубитами по каналу связи. Кубит – квантовый бит информации (*q*-бит, qubit, от английского quantum bit). Кубиты имеют большое количество всевозможных состояний. Эти состояния можно показать как некую стрелку, указывающую на вполне конкретную и определенную точку внутри сферы. Северный полюс такой сферы эквивалентен нулю, а южный – единице. Другие положения соответствуют квантовым суперпозициям нуля и единицы. Протоколы квантовой связи, основанные на использовании кубитов, рис. 5 (под протоколами понимают алгоритм или некую последовательность действий, приводящих к решению той или иной задачи), являются наиболее разработанными и, как следствие, распространенными и простыми в реализации на нынешний момент. Ниже описана процедура обмена информацией, предложенная Ч. Беннеттом и Дж. Брассардом в 1984 году.

1. Эта процедура называется протокол передачи квантовой информации ББ84. В протоколе ВВ84 используются 4 квантовых состояния фотонов, например, направление вектора поляризации, одно из которых корреспондент на узле связи А (далее просто А) выбирает в зависимости от передаваемого бита: 90° или 135° для «1», 45° или 0° для «0».А случайным образом выбирает один из базисов. Затем внутри базиса случайно выбирает одно из состояний, соответствующее 0 или 1 и посылает фотоны, рис.6.

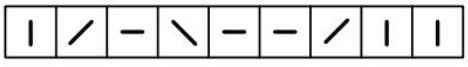


Рис. 6. Фотоны с различной поляризацией

2. Корреспондент на узле связи В (далее просто В) случайно и независимо от А выбирает для каждого поступающего фотона: прямолинейный (+) или диагональный (х) базис, рис. 7:

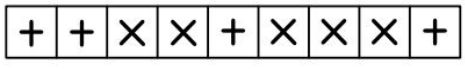


Рис. 7. Выбранный тип измерений

Затем В сохраняет результаты измерений, рис. 8:

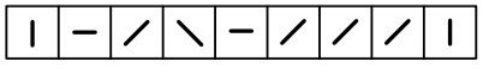


Рис. 8. Результаты измерений

3. В по открытому общедоступному каналу связи сообщает, какой тип измерений был использован для каждого фотона, то есть какой был выбран базис, но результаты измерений остаются в секрете;

4. А сообщает В по открытому общедоступному каналу связи, какие измерения были выбраны в соответствии с исходным базисом А, рис. 9.

Рис. 9. Случаи правильных замеров

5. Далее оставляют только те случаи, в которых выбранные базисы совпали. Эти случаи переводят в биты (0 и 1), и получают, таким образом, ключ, рис. 10:

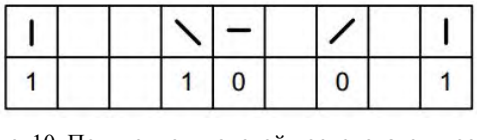


Рис. 10. Получение ключевой последовательности по результатам правильных замеров

Число случаев, в которых выбранные базисы совпали, будет составлять в среднем половину длины исходной последовательности, т. е. $n = 1/2$.

Пример определения количества фотонов, принятых В, показан в таблице.

Формирование квантового ключа по протоколу ВВ84

Двоичный сигнал Алисы	0	1	0	1
Поляризационный код Алисы	↔	↕	⤡	⤢
Детектирование Бобом	✣	✣	✣	✣
Двоичный сигнал Боба	0	1	?	?

Таким образом, в результате передачи ключа Бобом в случае отсутствия помех и искажений будут правильно зарегистрированы в среднем 50 % фотонов. Однако идеальных каналов связи не существует и для формирования секретного ключа необходимо провести дополнительные процедуры поиска ошибок и усиления секретности. При этом для части последовательности бит пользователей, в которых базисы совпали, через открытый общедоступный канал связи случайным образом раскрываются и сравниваются значения бит. Далее раскрытые биты отбрасываются. В идеальном квантовом канале (без шума) достаточно выявить несоответствие в одной раскрытой позиции для обнаружения злоумышленника. В реальной ситуации невозможно различить ошибки, произошедшие из-за шума и из-за воздействия злоумышленника. Известно, что если процент ошибок ≤ 11 %, то пользователи из нераскрытой последовательности, после коррекции ошибок через открытый общедоступный канал связи и усиления секретности, могут извлечь секретный ключ, который будет у них одинаковым и не будет известен злоумышленнику. Ключ, полученный до дополнительных операций с последовательностью, называется "сырым" ключом. При коррекции ошибок эффективным способом для согласования последовательностей А и В является их «перемешивание» для более равномерного распределения ошибок и разбиение на блоки размером k, при котором вероятность появления блоков с более чем одной ошибкой пренебрежимо мала. Для каждого такого блока стороны производят проверку четности. Блоки с совпадающей четностью признаются правильными, а оставшиеся делятся на несколько более мелких блоков, и проверка четности производится над каждым таким блоком, до тех пор, пока ошибка не будет найдена и исправлена. Процедура может быть повторена с блоками более подходящего размера. Наиболее мелкие блоки отбрасываются при наличии в них ошибки. Когда в каком-либо блоке количество ошибок окажется четным, то даже с оптимальным размером блока некоторые из них могут быть не выявлены. Для их исключения производят перемешивание последовательности бит, разбиение ее на блоки и сравнение их четности производится еще несколько раз, каждый раз с уменьшением размера блоков, до тех пор, пока А и В не придут к выводу, что вероятность ошибки в полученной последовательности пренебрежимо мала. В результате всех этих действий А и В получают идентичные последовательности бит. Эти биты и являются ключом, с помощью которого пользователи получают возможность кодировать и декодировать секретную ин-

формацию и обмениваться ей по незащищенному от съема информации каналу связи.

Таким образом, можно всецело заявить об обеспечении надежной передачи данных при помощи квантового шифрования между узлами связи, нуждающимися в обеспечении повышенной информационной безопасности, охраняемой непосредственно законами квантовой механики и не имеющей возможности раскрытия этих данных. Перспективно возможно рассмотрение использования сетей квантовой связи, работающих преимущественно в симплексном режиме между двумя и более абонентами. Аналогично можно провести параллели между использованием сетей квантовой связи воздушно-наземной ориентировки, воздушно-воздушной и, строго говоря, только космической.

Рассматривая перспективы развития воздушного канала связи, можно с должной уверенностью заявить о возможности дальнейшего создания государственных или военных каналов связи, нацеленных преимущественно на оповещение должностных лиц в пределах междугороднего канала связи (срочное оповещение), учрежденческого канала связи в силовых структурах (например, проведение срочных операций).

Экспериментальная реализация

5 июня 2019 года « Ростелеком » представил опытную сеть передачи данных с квантовым шифрованием. Она впервые использует оборудование и решения разных производителей с организацией их корректного взаимодействия на всем пути передачи данных. Также впервые в стране такая сеть имеет несколько узлов с технической возможностью подключения множества пользователей, независимо от места расположения их офисов и используемого криптографического оборудования с КРК (технология квантового распределения ключей).

Опытная сеть в Петербурге включает узлы в лаборатории «Ростелекома» на Синопской набережной, в инжиниринговом центре «СэйфНэт» на Аптекарском проспекте, а также в музее связи на Почтамтском переулке. Все они связаны между собою высокоскоростными волоконно-оптическими линиями передачи данных «Ростелекома».

Для организации защиты передачи информации с использованием КРК задействовано только отечественное оборудование и решения – Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики (Университет ИТМО), «Российского квантового центра», Т8, «С-Терра».

Представленная в Санкт-Петербурге многоузловая сеть за 1 секунду вырабатывает более 2000 бит секретной ключевой информации.

Перспективы развития

Квантовая криптография еще не вышла на уровень практического использования, но приблизилась к нему. В мире существует несколько организаций, где ведутся активные исследования в области квантовой криптографии. Среди них IBM , GAP-Optique, Mitsubishi, Toshiba , Национальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт (Caltech), а также молодая компания MagiQ и холдинг QinetiQ, поддерживаемый британским министерством обороны. Диапазон участников охватывает как крупнейшие мировые институты, так и небольшие начинающие компании, что позволяет говорить о начальном периоде в формировании рыночного сегмента, когда в нем на равных могут участвовать и те, и другие.

Конечно же, квантовое направление криптографической защиты информации очень перспективно, так как квантовые законы позволяют вывести методы защиты информации на качественно новый уровень. На сегодняшний день уже существует опыт по созданию и апробированию компьютерной сети, защищенной квантово-криптографичекими методами – единственной в мире сети, которую невозможно взломать.

Литература

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. Мир, 2006. С. 824.

2. Хренников А. Ю. Введение в квантовую теорию информации. М.: Физматлит, 2008.С. 284.

3. Альбов А. С. Квантовая криптография. М.: Страта, 2016. С. 248.

4. Рябцев И. И., Третьяков Д. Б., Коляко А. В., Плешков А. С., Энтин В. М., Латышев А. В., Асеев А. Л. Элементная база квантовой информатики II: Квантовые коммуникации с одиночными фотонами // Микроэлектроника. 2017. Т. 46. С. 131–141.

5. Молотков С. Н. Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы // Письма в ЖЭТФ. 2009. Т. 79. Вып. 11.