Безопасность информации: применение квантовых технологий

А.У. Актаева, О.А. Баймуратов, Н.Г. Галиева, А.С. Байкенов

Аннотация **- В статье обсуждается значимость в современном информационном обществе информационных ресурсов, требующих надежных методов защиты от несанкционированного доступа. Рассматривается структура и основные принципы технология квантовой криптографии на основе свойств квантовых систем. Предложен метод повышения уровня информационной безопасности и защиты конфиденциальной информации путем квантовой телепортации на каналах инфракрасной лазерной связи. Теоретическая разработка была экспериментально реализована авторами на установке для лазерной связи.**

Ключевые слова **- Квантовая информатика, квантовые каналы связи, квантовая криптография, квантовый компьютер, фотон, кубит.**

I. Введение

В современном информационном обществе существует большое и постоянно нарастающее количество информационных ресурсов, требующих надежных методов защиты от несанкционированного доступа. В последние годы весьма актуальной и востребованной стала проблема применения квантовых технологий в области обеспечения системы информационной безопасности и защиты конфиденциальной информации, передаваемой по открытым каналам связи. Причиной этому стали научные открытия и технологические достижения, сделавшие принципиально возможным решение целых классов сложнейших вычислительных технологий, имеющих стратегическое значение к критически важным технологиям, таким как инновационные технологии: квантовые, лазерные и оптические [20].

Асс. профессор, Ph.D А.У. Актаева работает в Казахской академии транспорта и коммуникаций имени М. Тынышпаева, Казахстан (e-mail: aakhtaewa@gmail.com)

Асс. профессор, д. Ph.D О.А. Баймуратов работает в Казахской академии транспорта и коммуникаций имени М. Тынышпаева, Казахстан (e-mail: alimzhan1@mail.ru)

Исследователь, MSc Н.Г. Галиева работает в Казахской академии транспорта и коммуникаций имени М. Тынышпаева, Казахстан (e-mail: nggaliyeva@gmail.com)

Асс. профессор, Ph.D А.С. Байкенов работает в Алматинском университете энергетики и связи, Казахстан (e-mail: baikenoff@yandex.ru)

II. Основные понятия и определения

В настоящее время квантовая информатика представляет собой новую, быстро развивающуюся отрасль науки, связанную с использованием квантовых технологий для реализации принципиально новых методов инфо-телекоммуникации и вычислений: квантовая информация, квантовая информатика, квантовые каналы связи, квантовая криптография, квантовый компьютер [15 - 21].

Квантовая информация — это физическая величина, характеризующая изменения, происходящие в системе при взаимодействии информационного потока с внешним окружением. Квантовая информация — это новый вид информации, который можно передавать, но нельзя размножать. Квантовый бит или кубит (qubit) описывается единичным вектором в двумерном комплексном векторном пространстве и представляет собой двухуровневую квантовую систему. В качестве кубитов могут выступать ионы, атомы, электроны, фотоны, спины атомных ядер, структуры из сверхпроводников и многие другие физические системы [7].

Квантовые состояния могут использоваться для записи значений классического бита информации. Базис векторного пространства задается всего двумя единичными ортогональными векторами, обозначаемыми соответственно $|0\rangle$ и $|1\rangle$. В отличие от классического бита, квантовый бит может быть представлен произвольной суперпозицией базисных векторов состояния фотона $|\psi\rangle = a|H\rangle + b|V\rangle$, где **a** и ***b***-произвольные комплексные числа, удовлетворяющие условию $|a|^2 + |b|^2 = 1$, может быть представлено, как и в случае спина, на блоховской сфере (рис.2) и однокубитовые операции представляют собой вращение вектора Блоха [1 - 5].

Распространяющийся со скоростью света фотон имеет два состояния вектора поляризации (H) и (V), ортогональных друг другу и ортогональных направлению распространения фотона. Горизонтально поляризованный фотон (H) представляет базисное состояние кубита $|0\rangle$, а вертикально поляризованный (V)-

базисное состояние $|1\rangle: |0\rangle = |H\rangle, |1\rangle = |V\rangle$. Если над кубитом производится измерение в базисе, то кубит может быть реализован в различных физических системах [1 - 5].

С точки зрения классической теории информации, кубиты характеризуют прямые ресурсы передаваемого сигнала, которые могут быть использованы для передачи информации по квантовому каналу связи. Для обеспечения помехоустойчивости квантовых вычислений возможен и другой подход, при котором создаются такие операции на логических кубитах, когда распространение ошибок среди физических кубитов было бы ограничено настолько, чтобы можно было использовать соответствующие корректирующие коды. Этого можно добиться путем построения специальных перекрестных (transversal) вентилей, которые осуществляли бы взаимодействие кубитов одного кодируемого кластера только с соответствующими кубитами в другом кластере [11].

Если имеется источник, производящий чистые состояния $|\psi_1\rangle, \ldots, |\psi_a\rangle$ с вероятностями $p_1, \ldots, p_a$ (аналог классического алфавита), тогда могут посылаться длинные последовательности букв слова, т.е. каждое слово задается последовательностью

$$w = (x_1, \ldots, x_n),\ x_j \in \{1, \ldots, a\}.$$

Экспериментально, такие операции выполняются с помощью двулучепреломляющей волновой пластины, которая задерживает фазу одной поляризации на определенную долю длины волны по отношению к ортогональной к ней поляризации, вызывая вращение вектора Блоха на блоховской сфере (рис.1).

Операции над кубитами носят квантовый, вероятностный характер, что обусловливает некоторые особенности таких операций. В общем случае, выделяют три класса квантовых алгоритмов:

1. алгоритмы, основанные на квантовых версиях преобразования Фурье;
2. алгоритмы квантового поиска;
3. алгоритмы моделирования квантовых систем [1, 2].

Во всех случаях квантовый алгоритм решает задачу эффективней классического [3].

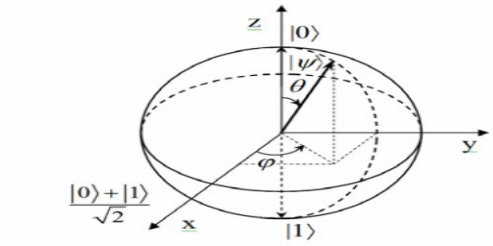

Рис. 1. Кубит на сфере Блоха

Попыткой поиска ответов на квантовые вызовы в области обеспечения системы информационной безопасности и защиты информации является квантовая криптография. Основные усилия в этой области сосредоточены на задачах синтеза стойких к возможностям квантовых компьютеров криптографических алгоритмов и протоколов (рис.2). К настоящему времени предложено несколько десятков различных по назначению протоколов квантовой безопасной связи (BB84, ЭПР, B92(4+2), SARG04, CSS, ЛО-ЧУ, Гольденберга-Вайдмана, Коаши-Имото, Пинг-Понг и др.) [1-5, 7].

Рис. 2. Основные направления исследований в СИБ [7]

Многими экспертами квантовая криптография рассматривается как единственный метод, способный обеспечить реальную защиту системам коммуникаций, как на данный момент, так и в обозримом будущем, основанный на передаче информации квантовыми состояниями фотонов (рис. 3) [1 - 5, 7].

В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография работает с физикой передачи информации [27].

Технология квантовой криптографии опирается на свойства квантовых систем:

- невозможность произвести измерение квантовой системы, не нарушив ее;
- невозможность определить одновременно координату и состояние частицы со сколь угодно высокой точностью;
- невозможность одновременно проверить поляризацию фотона в вертикально - горизонтальном и в диагональных направлениях;
- невозможность дублировать квантовое состояние, пока оно не измерено.

Процесс отправки и приема информации выполняется физическими средствами, при помощи фотонов в линиях волоконно-оптической связи, естественной среде или вакууме. Когерентные оптические состояния могут нести в себе большое число фотонов. Это, с одной стороны, способствует увеличению дальности передачи секретных сообщений, а с другой стороны, создает дополнительные проблемы с защитой информации.

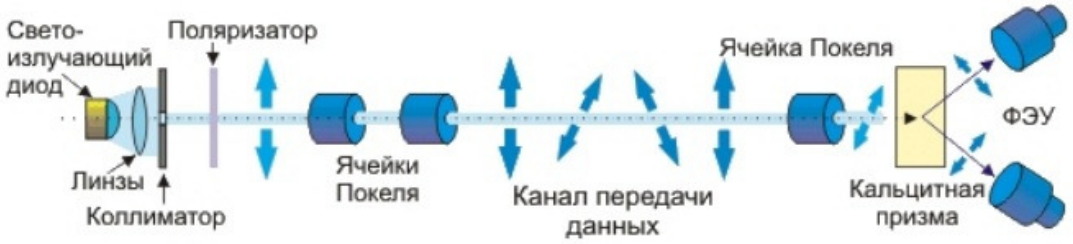

Рис. 3. Схема реализации квантовой криптографии

Особенность квантовой информации, заключающееся в том, что нельзя произвести измерение не изменив состояние системы, лежит в основе создания квантовых каналов связи, передающих классическую информацию без риска ее неконтролируемого перехвата. Квантовая «запутанность» является фундаментальным свойством квантовой механики. Она позволяет распространять квантовую информацию на десятки тысяч километров и ограничивается только лишь тем, насколько быстро и насколько далеко составляющие «запутанной» пары смогут распространиться в пространстве.

Понятно, что из-за ограниченности возможностей по измерению использовать квантовые способы передачи данных в целом невыгодно, однако, 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 нее нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале пользователи могут распознать степень активности перехватчика.

При создании криптосистем, основанных на квантовом распространении ключа, приходится сталкиваться со следующими проблемами:

- низкая скорость передачи – скорость передачи по каналам большой длины ~ Кбит, по коротким каналам ~ 10 – 100 Кбит;
- небольшие расстояния - до 100 км со скоростями порядка ~ Кбит;
- интенсивность импульсов квантов – обычно фотоны излучаются пучком, что позволяет злоумышленнику отделить часть фотонов и проанализировать их состояние;
- излучение одиночных фотонов заданной поляризации возможно только с некоторой вероятностью [11, 18].

В настоящее время для реализации квантового канала в схеме квантовой криптографии наиболее подходящей средой является оптическое волокно, свойство которого позволяет предавать на расстояние до 120 км. Использование волокна накладывает ограничение на возможность работы с поляризационной кодировкой, поскольку оптоволокно обладает ощутимыми флуктуационными двулучепреломления. В силу этого для квантовой криптографии используется фазовая модуляция с интерферометрическими детектированием. Основополагающими принципами защиты данных в квантовых линиях связи являются невозможность копирования заранее неизвестного состояния отдельного квантового объекта и

невозможность получения любой информации о квантовых состояниях этого объекта без их возмущения. Таким образом, гарантией защиты передаваемой информации выступают фундаментальные законы квантовой механики [11, 18, 26].

Квантовая телепортация - передача неизвестного квантового состояния на расстояние при помощи разделенной в пространстве и поделенной между двумя корреспондентами ЭПР-пары и классического канала связи. Квантовая телепортация, в отличие от плотного кодирования, происходит при отсутствии квантового канала связи, т.е. без передачи кубитов (рис. 4).

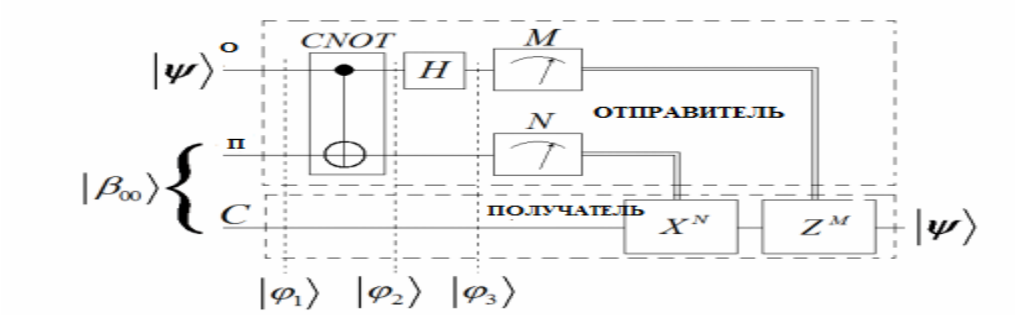

Рис. 4. Схема квантовой телепортации: одинарные линии - квантовые каналы связи; двойные – классические [17]

Телепортация представляет собой идеальный способ передачи секретной информации, а также:

1. процедура телепортации не нарушает теорему о неклонируемости;
2. перенос квантовой информации от фотона к фотону может осуществляться на произвольные расстояние (более 144 км по открытой пространстве, 102 км -по оптическому волокну);
3. телепортация не предполагает передачу информации о факте ее осуществления;
4. классический канал (о факте передачи информации);
5. если не проводить измерение состояний Белла и ограничиться проецированием на фермионное состояние, то телепортация будет успешно осуществлена в среднем один раз из четырех попыток [11, 18, 26].

Квантовая телепортация не дает возможности передавать информацию быстрее скорости света, как может показаться на первый взгляд, поскольку неотъемлемой частью протокола телепортации является передача информации по классическому каналу связи, а классический канал ограничен скоростью света (рис. 5).

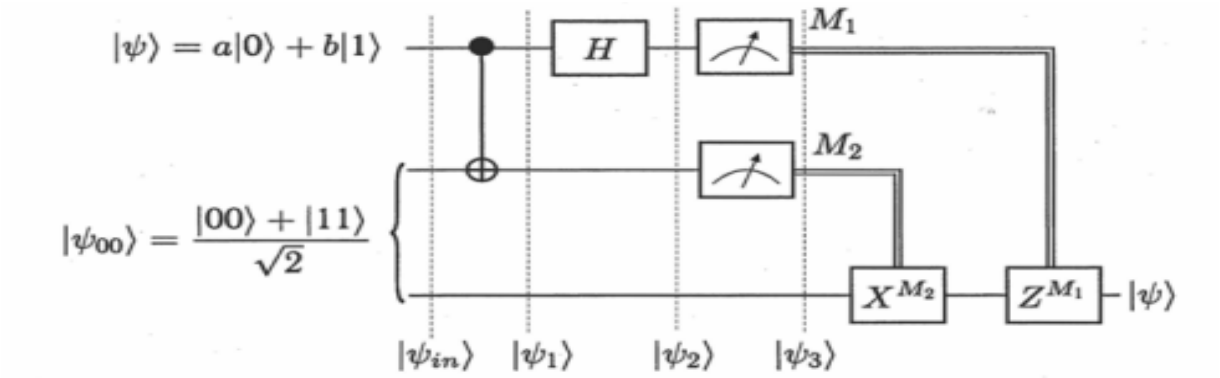

Рис. 5. Квантовая схема телепортации неизвестного состояния |Ψ> кубита [20]

Квантовая телепортация используемая в качестве некоторой базисной составляющей в квантовой схеме, открывает заманчивые возможности для решения этой и ряда других экспериментальных проблем, возникающих при реализации квантовых компьютеров, она позволяет осуществлять целый ряд квантовых логических операций, невозможных при использовании прямых унитарных операций. Формирование помехоустойчивых квантовых логических вентилей сводится в этом случае к приготовлению соответствующего вспомогательного запутанного состояния в схеме однокубитовой телепортации [11].

Новые возможности инфракрасных лазеров для реализации квантовой телепортации состояний открывают преимущество в решении проблемы передачи легко разрушаемых суперпозиционных состояний на большие расстояния без потери ими когерентности.

Лазер генерирует слабо расходящийся в воздухе пучок света (диаметр порядка 1 мм). Это позволяет осуществлять передачу открытым лучом на относительно большое расстояние (до 10 км). Следует учитывать, что солнце создает поток излучения в инфракрасной области не меньше, чем в видимой области. Оптические каналы предполагают использование двух параллельных лучей, по одному для каждого направления передачи. Диаметр чувствительной поверхности детектора обычно не превышает 1 мм [25].

А чтобы исключить влияние конвективных воздушных потоков обычно используют дефокусировку пучка, чтобы даже при отклонении оси пучка пятно засветки не покидало чувствительную область детектора. Этот метод предполагает, что имеется избыток световой мощности передающего лазера. Открытый инфракрасный луч предоставляет достаточно высокий уровень безопасности, а это является следствием самой природы передачи сигнала, а не обеспечивается какими-либо специальными методами. Важнейшее свойство беспроводной оптической связи - высокая степень защищенности канала от несанкционированного доступа. Осуществить перехват канала технически весьма трудно - в силу острой направленности луча и применения уникального для каждой модели метода кодирования информации импульсами излучения. Тем не менее, для обнаружения попыток несанкционированного доступа разработан ряд мер, основанных на разнообразных принципах - обращения волнового фронта, анализа изменения принимаемого сигнала и др., что еще больше повышает защищенность канала связи [24]. Проектируя такие каналы связи надо учитывать ослабление сигнала α^0[дБ], связанное с геометрией пучка:

$$\alpha^0 = 20 \log(\alpha^0 R * d^0) \quad \{Дб\},$$

где α^0- угол расхождения в радианах;
R - расстояние передачи в метрах;
$\mathbf{d^0}$- диаметр входного окна в метрах.

Необходимо также принимать во внимание ослабление, связанное с поглощением и рассеянием:

$$\alpha^1 = \frac{17}{S} * \left(\frac{0.55^{0.195-5}}{\lambda}\right) \quad \{Дб/км\},$$

где α^1- ослабление в децибелах на километр;
λ - длина волны излучения в микронах;
S - дальность видимости [км] [25].

Сигналы входного интерфейса системы используются для модуляции сигнала в открытом оптическом канале. Сама технология передачи основывается на передаче данных модулированным излучением в инфракрасной части спектра через атмосферу. Передатчиком служит – полупроводниковый излучающий диод. В качестве приемника используется высокочувствительный фотодиод. Излучение воздействует на фотодиод, вследствие чего регенерируется исходный модулированный сигнал. Далее, сигнал демодулируется и преобразуется в сигналы выходного интерфейса. С обеих сторон используется система линз, на передающей стороне - для получения коллимированного луча, а на приемной стороне, для фокусирования принятого излучения на фотодиод. Для дуплексной передачи организуется точно такой же обратный канал. Самым непредсказуемым элементом в системе является среда передачи - непрогнозируемость атмосферы с ее погодными явлениями [24]. Дальность и надежность передачи информации при инфракрасной лазерной связи зависит от погодных условий (рис. 6).

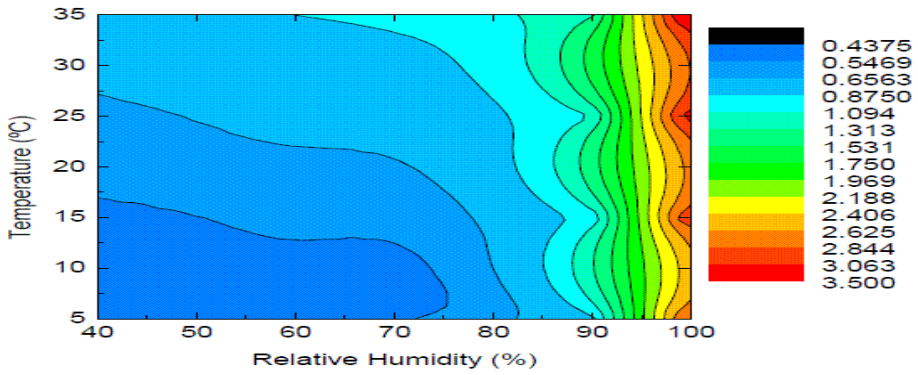

Рис. 6. Зависимость поглощения сигнала на базе в 1 км от температуры и влажности [24]

III. Эксперимент

Обычно информация передается мощными лазерными импульсами. В их квантовом состоянии (поляризации, фазе, времени) кодируется случайная последовательность битов. В один фотон кодируется один бит и передается получателю. Главная проблема в том, что одиночные фотоны очень сильно теряются. Пройдя несколько десятков километров 99% одиночных фотонов рассеиваются. Поэтому необходимо использовать квантовые повторители, принцип которых основан на технологии квантовой телепортации.

При проведении исследования преимущества и возможности применения технологии квантовой телепортации с помощью атмосферной лазерной связи были изучены направление развития проектирования трасс для прокладки линий связи в зависимости от конкретных условий и проведены сопоставления и анализ данных высотных зданий г. Алматы (см. рис.7).

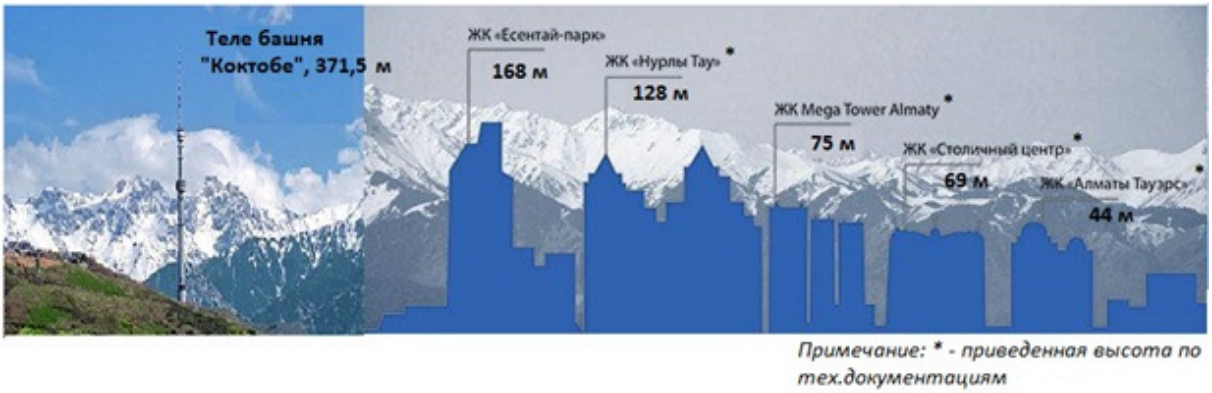

Рис. 7. Сопоставление данных высотных зданий г. Алматы

Одновременно при прокладке трасс анализируются логика маршрутизации канала атмосферной лазерной связи с учетом месторасположении объектов - заказчика и предложен вариант проектирования канала атмосферной лазерной связи (см. рис. 8).

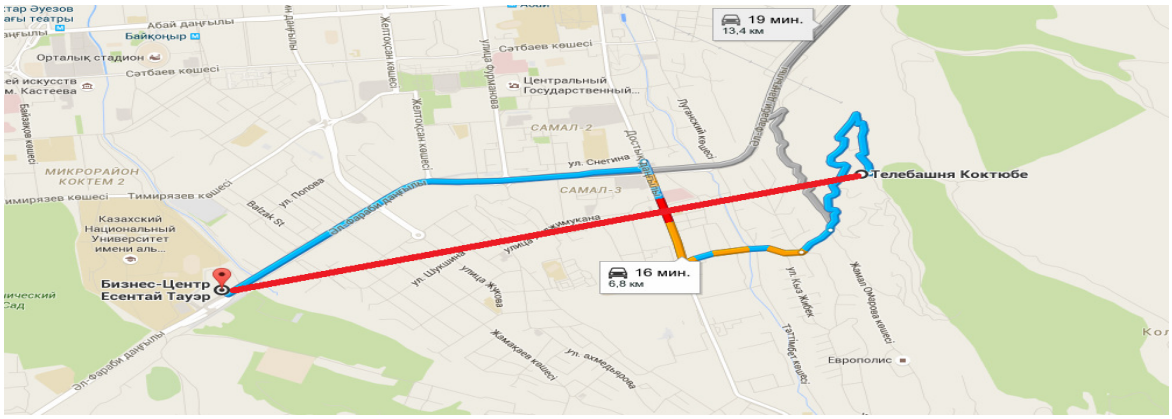

Рис. 8. Предполагаемый канал лазерной связи

Традиционно при проектировании линии связи ставим сервер, затем тянем оптоволокно к каждому потребителю информационных услуг, теперь вместо этого мы предлагаем два направленных друг на друга – ЛПП (лазерный приемник – передатчик), через которые передаются данные по открытому пространству с помощью лазерного света (рис.9).

Проблема телепортации затрагивает ряд вопросов принципиального характера, в частности, обмена квантовой информации в сложных пространственно разнесенных молекулярных структурах, в том числе биологических. Ни одна беспроводная технология передачи не может предложить такую конфиденциальность связи как лазерная.

Перехватить сигнал можно, только установив сканеры-приемники непосредственно в узкий луч от передатчиков.

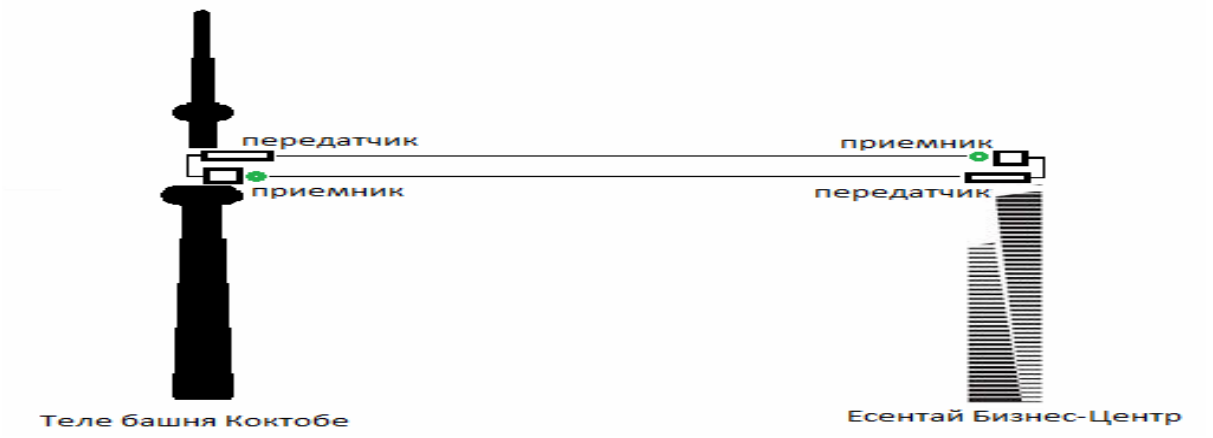

Рис. 9. Схема передачи информационных потоков

Реальная сложность выполнения этого требования делает перехват практически невозможным. Наличие лазерных лучей нельзя определить с помощью различных сканеров. Также используются разнообразные собственные протоколы передачи данных, что обеспечивают дополнительную конфиденциальность. Лазерные системы уже применяются для разнообразных приложений, где требуется высокая конфиденциальность передачи данных, включая финансовые, медицинские и военные организации. Одновременно они анализируются логикой маршрутизации.

IV. Заключение

В связи с интенсивным развитием инновационных технологий особое значение приобретают исследования в электронике, создании интеллектуальных программных и аппаратных продуктов прикладной информатики и квантовых технологий. Квантовая информация и технологии, основанные на ее необычных свойствах, в будущем повлияют на основы и дальнейшее развитие информационного пространства, а сама теория квантовой информации кардинально изменит современные взгляды научного сообщества на основу системы информационной безопасности.

Проведение экспериментов и исследований по обеспечению информационной безопасности представляет большой научный интерес по поиску решения основных задач и проблем, стоящих перед квантовыми криптографическими системами: задача детектирования единичных фотонов с высокой вероятностью в заданном квантовом состоянии при низком уровне ложных срабатываний, отсутствие управляемых источников одиночных фотонов, проблема увеличения дальности передачи и малая скорость генерации квантового ключа. Применение квантовых технологий в области обеспечения системы информационной безопасности - одно из наиболее парадоксальных проявлений квантовой технологии, вызывающее в последние годы огромный интерес специалистов, в первую очередь, при передаче зашифрованных сообщений по двум каналам связи - квантовому и традиционному.

Квантовая телепортация информации является одним из самых стремительно развивающихся прикладных направлений квантовой физики, и обеспечивает информирование о попытке перехвата передаваемой информации из-за необратимости коллапса волновой функции. Исследования в области квантовой телепортации информации могут привести не только к положительным последствиям, но и отрицательным. Квантовая криптография, основанная на применении квантовой телепортации, в будущем заменит все используемые криптографические системы, и будет применяться наравне с обычными средствами инфотелекоммуникации. Актуальность и масштабность проблем, связанных с обеспечением информационной безопасности, с каждым днем будут возрастать, а развитие квантовой информации в ближайшем будущем принесет свои результаты и, возможно, приведет к существенному изменению научной картины мира в области ИТ.

Библиография

[1] Benioff P. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines // J. Stat. Phys. – 1980,V. 22, p.

563–591

[2] Deutsch D. Quantum theory, the Church-Turing principle and the universal quantum computer // Proc. Roy. Soc.- London, 1985, V. A400, p. 96–117

[3] Cleve R., Ekert A., Macchiavello C., Mosca M. Quantum algorithms revisited // Phil. Trans. Royal Soc. - London, 1998, V. A454, p. 339–354

[4] Turing A. On computable numbers with an application to the Entscheidungsproblem // Proc. LondonMath. Society. - 1937. - V. 42.– p. 230–265

[5] Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь. - М.: БАЯРД, 2004

[6] Бауместер Д., Экерт А., Цайлингер А. Физика квантовой информации. - М.: Постмаркет, 2002

[7] Актаева А.У., Илипбаева Л.Б. Инновационные технологии в системе информационной безопасности: квантовые технологии // Современные инновационные технологии и ИТ - образование.-2014, том 1, № 1(9), 320-326 стр.

[8] Белокуров В.В., Тимофеевская О.Д., Хрусталев О.А. Квантовая телепортация – обыкновенное чудо. - Ижевск: РХД, 2000

[9] Бройль Л. Революция в физике. - М: Атомиздат, 1965

[10] Валиев К.А. Квантовая информатика: компьютеры, связь и криптография. - М.: Вестник РАН, 2000

[11] Валиев К.А., Кокин А.А. Квантовые компьютеры: надежда и реальность. - Ижевск: Регулярная и хаотическая динамика, 2001

[12] Гейзенберг В. Физика и философия.- М.:Наука,1989, перевод – Акчурин И.А., Андреев Э.П.

[13] Кадомцев Б.Б. Динамика и информация.- М.:Успехи физических наук, 1999

[14] Клышко Д.Н. Физические основы квантовой электроники. - М.: Наука, 1986

[15] Мандель Л., Вольф Э. Оптическая когерентность и квантовая оптика. - М.: Физматлит, 2000

[16] Прескилл Дж. Квантовая информация и квантовые вычисления.-М.: РХД, 2008

[17] Холево А.С. Введение в квантовую теорию информации. – М.: МЦНМО, 2002

[18] Эйнштейн А., Подольский Б., Розен Н.// «Можно ли считать, что квантово-механическое описание физической реальности является полным?» //УФН, 1934, Том XVI, выпуск 4. - перевод – Любина А.Г., под редакцией Фока А. В.

[19] Долгов В.А. и др. Криптографические методы защиты информации. - Хабаровск, 2008

[20] Емельянов В.И. Квантовая физика: Биты и Кубиты. - М.: Изд. МГУ, 2012

[21] http://www.gartner.com/newsroom/id/2819918?fnl=search&srcId=1-3478922254

[22] http://www.itsec.ru

[23] http://sci-article.ru

[24] http://works.tarefer.ru/71/100019/index.html

[25] http://book.itep.ru/3/optic_32.htm

[26] Килин С.Я. Квантовая информация // Успехи физической науки, 1999, Том 169, №5

[27] http://tcode.tinro.ru/cryptography/src/38.pdf

F. A. -Assoc. Prof., Dr. PhD Department of Computer Science and Information Systems, Kazakh Academy of Transport and Communication after named M. Tynyshbayeva, Kazakhstan (e-mail: aakhtaewa@gmail.com).

S. B. - Assoc. Prof., Dr. PhD Department of Computer Science and Information Systems, Kazakh Academy of Transport and Communication after named M. Tynyshbayeva, Kazakhstan (e-mail: alimzhan1@mail.ru).

T. C. - Reseacher, MSc., Department of Computer Science and Information Systems Kazakh Academy of Transport and Communication after named M. Tynyshbayeva, Kazakhstan (e-mail: nggaliyeva@gmail.com).

F. D. - Assoc. Prof., Dr. PhD Department of Radio engineering and telecommunications faculty, Almaty University of Power Engineering and Telecommunications, Kazakhstan (e-mail: baikenoff@yandex.ru).

Security of information: using of quantum technologies

A.U. Aktayeva, O.A. Baimuratov, N.G. Galiyeva, A.S. Baikenov

Abstract - This paper discusses the importance of the modern information society, information resources requiring reliable methods of protection against unauthorized access. The structure and basic principles of the technology of quantum cryptography based on the properties of quantum systems. A method for improving information security and the protection of confidential information by the quantum teleportation in channel infra-red laser communications. Theoretical development has been implemented experimentally by the authors at the facility for laser communications.

Keywords - Quantum computing, quantum communication channels, quantum cryptography, quantum computer, a photon, qubit.