7. А.с. 1720051 СССР, МКИ5 G 02 B 26/06. Датчик волнового фронта / *Безуглов Д.А., Мищенко Е.Н, Крымский М.И., Серпенинов О.В.* Опубл. в БИ. 1992. №.10.
8. *Noll R.J.* Zernike polynomials and atmospheric turbulence. J. Opt. Soc. Amer. 1976. V66. P. 207-211.

УДК 681.3.067:621.396.2

Д.М. Голубчиков

СТРУКТУРА И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ID 3000 CLAVIS

В мире существует всего три компании, предлагающие системы квантовой криптографии, предназначенные для применения в коммерческих приложениях. Две находятся в Европе – Id Quantique и Smart Quantum, одна в США – MagiQ Technology. Производимое ими оборудование строится по схожим схемам и незначительно отличается по своим характеристикам. В данном обзоре будет детально рассмотрена система квантового распределения ключей Id 3000 Clavis, производства компании Id Quantique. Она предназначена для проведения исследований в области квантовой криптографии и предоставляет пользователю широкие возможности по настройке и оценке параметров и характеристик квантового канала и оборудования предназначенного для его формирования[1].

Вначале будут кратко рассмотрены принципы функционирования системы. Далее проведено детальное описание блоков и модулей, входящих в ее состав.

Описание системы квантового распределения ключей

Квантовая система распределения ключей Id 3000 Clavis состоит из двух устройств размещенных в 19-ти дюймовых корпусах и пакета программного обеспечения для управления устройствами. Первое устройство является приемо-передающим модулем и носит кодовое название QKDS-B или Bob, второе устройство является кодирующим модулем, не содержит приемо-передающей аппаратуры, работающей с квантовыми состояниями, и носит кодовое название QKDS-A или Alice[2].

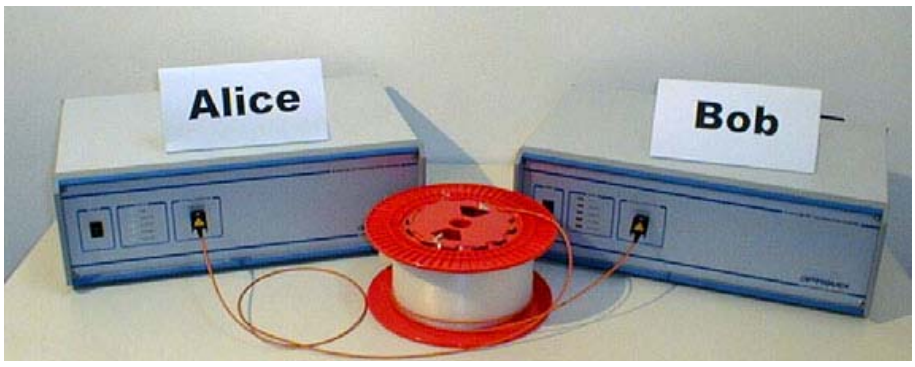

Рис. 1. Внешний вид системы квантового распределения ключей Id 3000 Clavis.

Принцип работы системы

Функционирование системы квантового распределения ключей основывается на принципе «plug&play» (подключай и работай), сама Id 3000 Clavis построена по схеме с автокомпенсацией поляризационных искажений[3]-[7]. Биты ключей кодируются с помощью фазовых состояний двух импульсов, распространяющихся от одного блока системы к другому и обратно.

Мощный лазерный импульс с длиной волны 1550 нм излучается лазером в блоке Bob, проходит светоделитель и разделяется на два оптических импульса. Один проходит напрямую к первому порту поляризационной светоделительной призмы, второй, через линию задержки и фазовый модулятор попадает на второй порт поляризационного светоделителя. В результате распространения по двум разным оптическим путям второй импульс задержан относительного первого на 50нс. Оба плеча выполнены из оптического волокна сохраняющего поляризацию, вследствие этого два импульса попадают на светоделитель ортогонально поляризованными и выходят на один и тот же порт светоделителя. Импульсы проходят к блоку Alice через волоконно-оптическую линию связи, отражаются на зеркале Фарадея, ослабляются и следуют обратно к блоку Bob ортогонально поляризованными. По очереди оба импульса проходят поляризационный светоделитель и попадают в плечо, по которому не распространялись при прямом прохождении, в результате чего попадают на светоделитель одновременно и интерферируют. Затем результат интерференции регистрируется одним или другим приемным модулем. Так как оба импульса проходят один и тот же оптический путь, то такой интерферометр считается автокомпенсирующимся. Для реализации протокола BB84 в Alice второй импульс сдвигается по фазе на одно из случайно выбранных значений из ряда 0, $\pi/2$, π, $3\pi/2$, а в Bob выбирается базис измерения посредствам фазового сдвига первого импульса на 0 или $\pi/2$ при обратном распространении импульса.

Оптическая часть устройства Bob

Устройство предназначено для формирования оптических импульсов, приема и обработки закодированных квантовых состояний.

В состав первого устройства входят: источник излучения, оптический циркулятор, два фотоприемных модуля, оптический делитель, линия задержки, фазовый модулятор, поляризационный светоделитель и волоконный световод, сохраняющий поляризацию и связывающий все перечисленные блоки[1].

На рис. 2 изображена оптическая часть схемы устройства Bob.

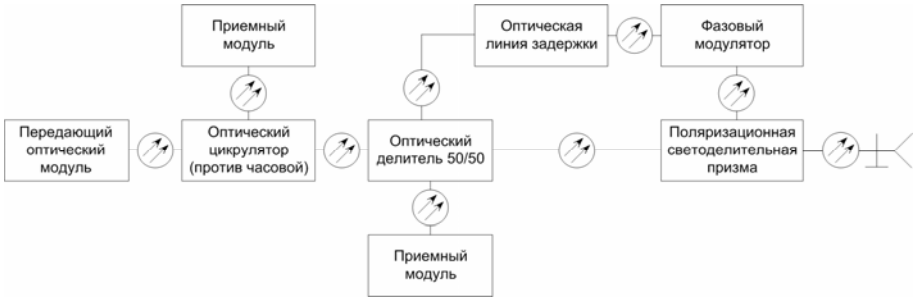

Рис. 2. схема оптической части устройства Bob

Перейдем к более детальному описанию блоков входящих в первое устройство. Это позволит разобраться в принципах функционирования системы в целом.

1. Передающий оптический модуль (источник излучения) – лазер, предназначенный для формирования когерентного оптического излучения с основной длиной волны 1550 нм и шириной спектра порядка 0,6 нм. Работа источника излучения основана на принципе распределенной обратной связи, за счет которой удается достичь столь узкого спектра излучения. Малая ширина спектра позволяет излучать сигнал с высоким временем когерентности, что позволяет повысить расстояние передачи. Источник так же обладает встроенным фотодиодом, который предназначен для измерения мощности излучения лазера. Источник излучения является электронно-управляемым модулем и позволяет регулировать и контролировать интенсивность излучения, а так же позволяет пользователю изменять длительность излучаемых импульсов в пределах от 300 до 2500 пикосекунд.
2. Оптический циркулятор – устройство, имеющее три порта, каждый из которых может быть как входом, так и выходом. Принцип работы основан на переносе энергии входящего излучения от первого порта, который в данной схеме подключен к лазеру и является входом, к ближайшему выходу (второму порту), подключенному через волоконный световод к оптическому делителю, обратный процесс между этими портами запрещен и приводит к большому затуханию сигнала. Однако вся энергия со второго порта без затухания переносится к третьему порту-выходу. Данный компонент является пассивным оптическим элементом и не имеет электрических управляющих входов.
3. Приемный модуль – предназначен для приема слабых оптических сигналов. Устройство этого модуля довольно сложное и имеет множество управляющих сигналов, таких как напряжение смещения, регулировка времени нечувствительности(dead time), период ожидания сигнала и прочие. Модуль состоит из лавинного фотодиода, системы охлаждения, схемы усиления и управляющей системы. Лавинный фотодиод – технологически доступный элемент, который позволяет регистрировать слабое излучение, с уровнем энергии порядка одного фотона. Однако с работой этого элемента связанно множество трудностей, например ложное срабатывание детектора при порождении лавины электронов в отсутствии фотона на входе. Такие процессы объединены в единый класс и определены как частота темнового счета. Т.е. количество ложных срабатываний на интервале времени. Одним из значимых факторов, оказывающих влияние на частоту темнового счета, является температура лавинного фотодиода. В приемном модуле температура фотодиода устанавливается равной -50 градусов по Цельсию и контролируется непрерывно с помощью термистора, т.к. перепады температуры на 1 градус оказывают существенное влияние на частоту темнового счета. Для охлаждения фотодиода используется элемент Пельтье. Дрейф температуры не превышает 0,1 градуса. Схема усиления предназначена для увеличения амплитуды электрического сигнала на выходе детектора. Управляющая схема предназначена для анализа полученных от фотодиода сигналов, контроля температуры, регулирования амплитуды, длительности и момента подачи напряжения смещения. (Не исключен случай, при котором на управляющем входе фотодетектора напряжение смещения подано постоянно, но на уровне, недостаточном для порож-

дения лавины, это позволяет снизить время переходных процессов при резкой подаче полного напряжения смещения, необходимого для регистрации однофотонного сигнала.)

4. Оптический делитель – пассивный элемент, с 4 портами входа-выхода, предназначен для суммирования двух волн. Так как излученный импульс при прямом распространении приходит только на один порт то делитель распределяет энергию входного импульса на два оптических выхода. Примененный делитель разделяет цуг волны на два равных по амплитуде импульса. При прохождении обратного сигнала именно здесь две пришедших волны интерферируют друг с другом, а затем направляются на один из двух выходов, ведущих к приемным модулям, в зависимости от разности фаз пришедших сигналов.
5. Оптическая линия задержки – состоит из отрезка волоконно-оптического кабеля, сохраняющего поляризацию, и предназначена для внесения временной задержки между двумя сигналами, идущими по разным оптическим плечам. Длительность задержки составляет 50 нс, из чего можно рассчитать протяженность оптического волокна равную приблизительно 9,2 м.
6. Фазовый модулятор – блок, выполненный на основе электрооптического кристалла ниобата лития. Принцип действия фазового модулятора основан на эффекте Керра. Фазовый модулятор позволяет внести фазовый сдвиг в сигнал, проходящий по длинному плечу при обратном распространении сигнала. Диапазон изменения значения фазы от 0 до 2π.
7. Поляризационный светоделитель – пассивный элемент, представляющий собой поляризационный мультиплексор. Сигналы, распространяющиеся по разным плечам интерферометра, поляризованы ортогонально, это связанно с применением волокна сохраняющего поляризацию. «Быстрые» оси волокон двух плеч повернуты на угол в 90 градусов друг относительно друга. Это позволяет направить сигналы, приходящие на два порта в один выходной порт мультиплексора, который объединен с выходным портом всего устройства Bob. Импульсы, распространяющиеся в обратном направлении, придя на этот же порт поляризационного светоделителя будут перенаправлены в противоположные плечи интерферометра, так как пройдя ВОЛС в обоих направлениях в устройстве Alice они попадут на зеркало Фарадея, которое изменит поляризацию каждого импульса на ортогональную.

Электронная часть устройства Bob

Перейдем к описанию электронной части устройства Bob. Она построена на основе микропроцессорной логики с применением микроконтроллеров, цифро-аналоговых и аналогово-цифровых преобразователей, цифровых линий задержки и мультиплексора.

Электронная часть устройства Bob предназначена для выполнения пяти основных функций:

1. Мониторинг состояния устройства. Т.е. контроль уровня напряжений, температуры устройства, тока и температуры охладителя приемных модулей.
2. Управление источником излучения. Контроль и регулировка длительности импульсов и их амплитуды.
3. Управление фазовым модулятором. Регулировка длительности импульсов, их амплитуды, а также задержка импульса фазового модулятора.

4. Управление однофотонными детекторами. Независимое изменение напряжения смещения лавинных фотодиодов и задержка его приложения.
5. Хранение и передача значений бит ключей, как от компьютера к устройству, с последующей передачей на схему управления фазовым модулятором, так и в обратном направлении – результатов детектирования приемных модулей. Сопряжение с компьютером происходит посредствам USB интерфейса.

Функциональная схема электронной части системы Bob приведена на рис. 3.

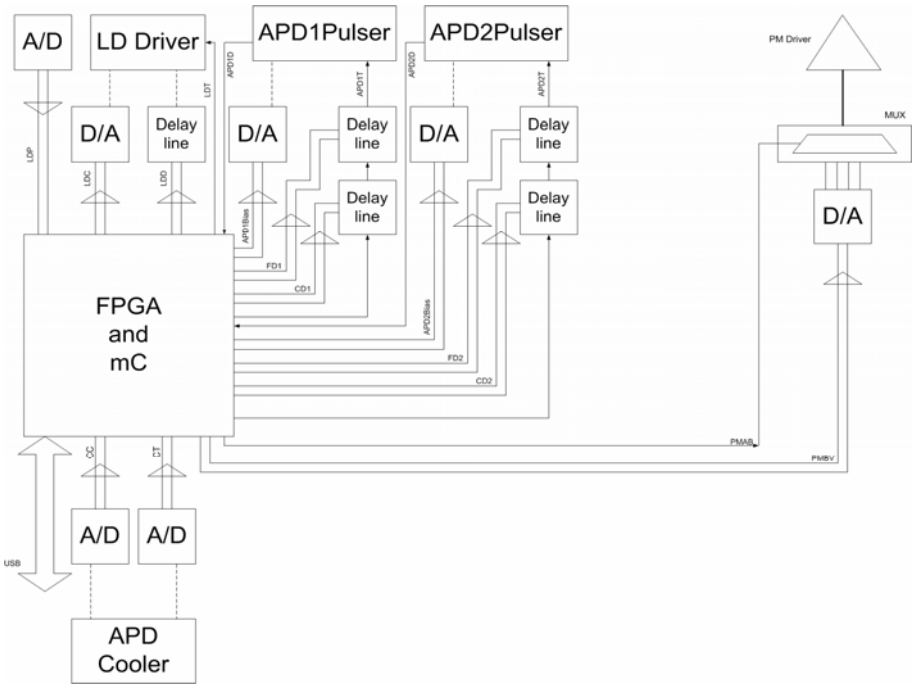

Рис. 3. Функциональная схема электронной части устройства Bob

Оптическая часть устройства Alice

Устройство предназначено для кодирования бит ключей в фазовых состояниях импульсов.

В состав второго устройства входят: оптический делитель, два перестраиваемых оптических аттенюатора, приемный модуль, линия задержки, фазовый модулятор, зеркало Фарадея и волоконный световод, связывающий все перечисленные блоки.

На рис. 4 изображена оптическая часть схемы устройства Alice.

Рис. 4. Схема оптической части устройства Alice

1. Оптический делитель – пассивный элемент, с 3 портами входа-выхода, предназначен для разделения энергии оптического сигнала в необходимых направлениях с заданными коэффициентами. Импульсы прошедшие ВОЛС попадают на входной порт делителя, где разделяются в соотношении 1 к 9 и направляются в соответствующих направлениях к перестраиваемым оптическим аттенюаторам. 90 процентов мощности сигнала через аттенюатор направляется в приемный модуль, функции которого будут рассмотрены ниже. Оставшиеся 10 процентов мощности входных импульсов будут направлены на вход оптической линии задержки через аттенюатор. При прохождении делителя в обратном направлении сигнал будет направлен на единственный противоположный порт.
2. Перестраиваемые оптические аттенюаторы – электронно-управляемый оптический аттенюатор с диапазоном ослабления сигнала от 1,5 до 50 дБ. Аттенюатор, установленный перед приемным модулем, предназначен для предотвращения повреждения приемного модуля при слишком высокой мощности приходящего излучения. Это может произойти в двух случаях: протяженность ВОЛС слишком мала и импульс, проходя по каналу связи, недостаточно ослабляется; в линий присутствует злоумышленник и пытается реализовать «широкую импульсную атаку». Приложение напряжения к управляющему входу второго аттенюатора, установленного перед линией задержки, так же позволяет предотвратить повреждение оптических компонентов системы при попытках съема информации по средствам введения мощных оптических импульсов, и ослабить отраженный от зеркала Фарадея выходной сигнал до уровня однофотонного импульса.
3. Линия задержки – представляет собой отрезок оптического волокна длинной порядка 12 км, и предназначается для предотвращения ложного срабатывания детекторов на приемном устройстве в результате Релеевского обратного рассеяния света от всех элементов системы, установленных до зеркала Фарадея.
4. Фазовый модулятор – блок, выполненный на основе электрооптического кристалла ниобата лития. Фазовый модулятор позволяет внести фазовый сдвиг во второй импульс, при обратном распространении сигнала. Диапазон изменения значения фазы сигнала от 0 до 2π. Для реализации протокола квантовой криптографии BB84 на данном фазовом модуляторе используются следующие значения сдвига фазы: 0 в горизонтальном базисе кодируется нулевым сдвигом фазы, 1 в горизонтальном базисе кодируется сдвигом фазы на π, 0 в диагональном базисе - $3\pi/2$, 1 в диагональном базисе - $\pi/2$. Фазовый сдвиг применяется **только** ко второму импульсу последовательности, задержанному относительно первого на 50 нс.
5. Зеркало Фарадея – представляет собой поляризационный вращатель с фиксированным углом поворота поляризации – 90 градусов. Таким образом, при обратном распространении в линии задержки импульсы уже обладают противоположной поляризацией.
6. Приемный модуль – представляет собой классический детектор оптического излучения. В данной схеме выполняет две функции: синхронизацию тактовых генераторов, с отметкой момента прихода импульса для последующей выдачи электроникой управляющего сигнала на фазовый

модулятор, и, мониторинг уровня приходящих сигналов с целью определения наличия в канале злоумышленника.

Электронная часть устройства Alice

Принцип построения электронной части системы Alice аналогичен принципу построения системы Bob и использует аналогичную элементную базу.

Электронная часть устройства Alice предназначена для выполнения пяти основных функций:

1. Мониторинг состояния устройства. Контроль уровня напряжений и температуры устройства.
2. Управление перестраиваемыми оптическими аттенюаторами. Передача значений затухания на цифро-аналоговые преобразователи.
3. Управление приемным модулем. Установка значения напряжения смещения и контроль срабатывания дискриминаторов синхронизации и тревоги.
4. Управление фазовым модулятором. Установка амплитуды импульса, и времени задержки относительно времени прихода первого оптического импульса.
5. Хранение и передача значений бит ключей, от компьютера к устройству, с последующей передачей на схему управления фазовым модулятором. Сопряжение с компьютером происходит посредствам USB интерфейса.

Функциональная схема электронной части системы Alice приведена на рис. 5.

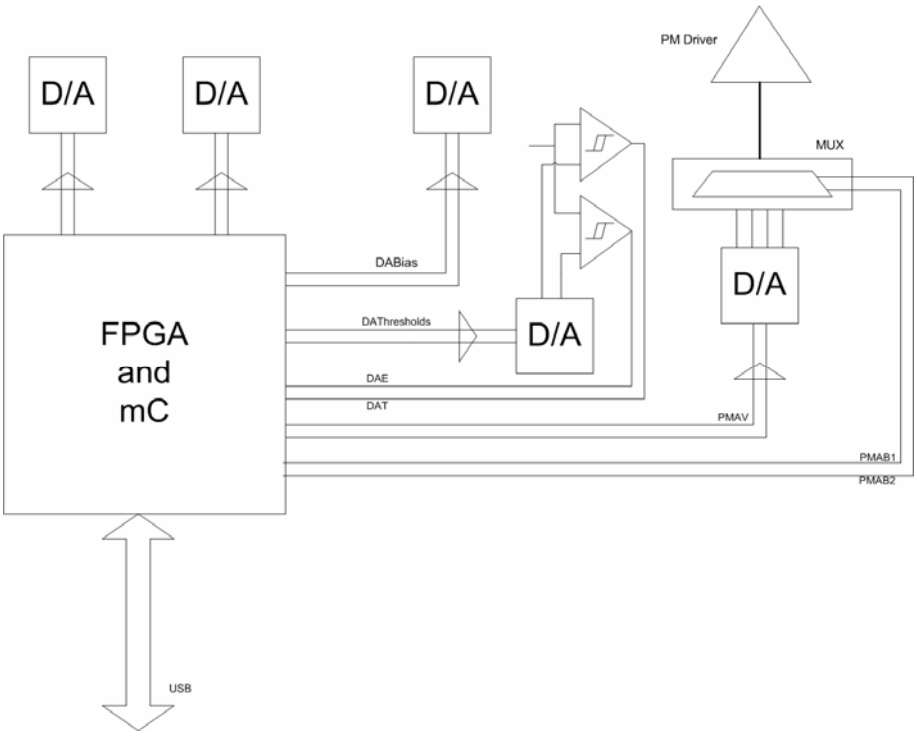

Рис. 5. Функциональная схема электронной части устройства Alice

Покадровая стратегия передачи квантовых состояний

Как упоминалось ранее, система квантового распределения ключей предназначена для использования в исследовательских целях и имеет большой выбор настроек, посредством изменения которых пользователь получает возможность детального анализа квантового канала и факторов, влияющих на его функциональные характеристики.

Синхронизация устройств системы квантового распределения ключей, осуществляется за счет синхронизации тактовых импульсов двух генераторов, находящихся в Bob и Alice соответственно. В устройстве QKDS-B тактовый генератор работает на частоте 10Мгц, в устройстве QKDS-A на частоте 20МГц. Синхронизация осуществляется за счет отведения части мощности оптических импульсов в оптическом делителе Alice и регистрации их приемным модулем. Необходимость применения в Alice тактового генератора с повышенной частотой следования тактовых импульсов связанна с необходимость различать два оптических сигнала с интервалом в 50 нс и изменять фазовое состояние **только** второго оптического импульса.

Для формирования ключей применяется покадровая стратегия функционирования. Источником излучения формируется последовательность из k оптических импульсов, которые проходят через все блоки системы Bob и Alice, отражаются на зеркале Фарадея и следуют обратно к детекторам устройства Bob. Кол-во импульсов k задается оператором системы и может принимать значения от 0 до 1000[8]. Кадром называется интервал времени от начала излучения первого из k импульсов, до момента регистрации на одном из приемных модулей Bob последнего из k импульсов. На рис. 6 приведена пространственно-временная диаграмма работы системы в масштабе одного кадра. Покадровая стратегия и наличие длинной линии задержки в Alice позволяет снизить процент ложных срабатываний приемных модулей Bob вследствие эффекта Релеевского обратного рассеяния света, соответственно снизить частоту квантовых ошибок(QBER) и повысить скорость формирования ключей (*Rraw*).

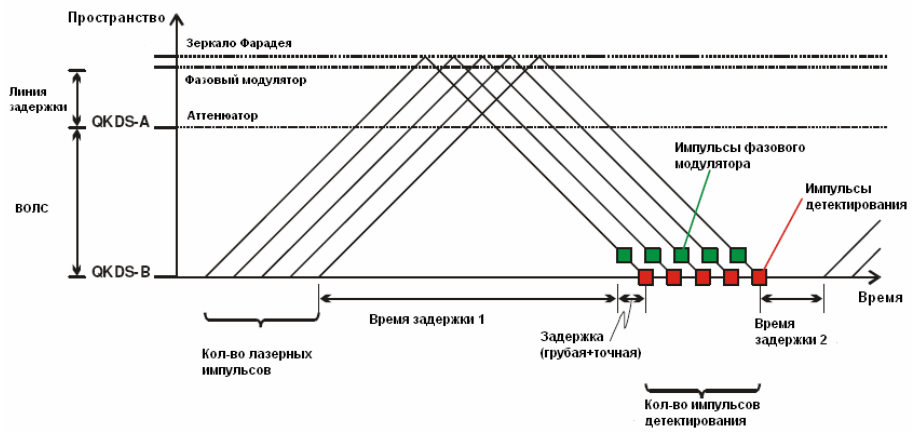

Рис. 6. Ппространственно-временная диаграмма обработки кадра

Выводы

Экспериментальное исследование системы Id 3000 Clavis представляет большой интерес с точки зрения анализа характеристик квантового канала формируемого системой. Программное обеспечение позволяет изменять множество параметров регулирующих работу системы, что показывает влияние конкретных компонентов системы на качественные характеристики канала, а так же дает возможность оценки влияния внешних факторов на работу оборудования. На основе полученных данных появляется возможность создания моделей квантовых каналов[9], максимально приближенных к реальным характеристикам систем. Данные модели могут широко применяться в учебном процессе и при постановке экспериментов, что целесообразно в связи очень высокой стоимостью оборудования и риском его повреждения в ходе экспериментов. Полученные результаты могут быть применены для поиска новых способов несанкционированного съема информации с квантовых каналов[10] и создания устройств их реализующих[11],[12].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Quantum Key Distribution System id 3000 User Guide, V-2.35, June 2005, Id Quantique
2. *D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden,* "Quantum key distribution over 67 km with a plug&play system", *New Journal of Physics* 4 (2002) 41.1–41.8
3. *Muller A, Herzog T, Huttner B, Tittel W,* Zbinden H and Gisin N 1997 Plug&play systems for quantumcryptography *Appl. Phys. Lett.* 70 793–5
4. *Ribordy G, Gautier J-D, Gisin N,* Guinnard O and Zbinden H 2000 Fast and user-friendly quantum keydistribution *J. Mod. Opt.* 47 517–31
5. *Bethune D and Risk W* 2000 An auto-compensating fiber-optic quantum cryptography system based onpolarization splitting of light *IEEE J. Quantum Electron.* 36 340–7
6. *Nielsen P M, Schori C, Sorensen J L, Savail L,* Damgard I and Polzik E 2001 Experimental quantum keydistribution with proven security against realistic attacks *J. Mod. Opt.* 48 1921–42
7. *Bourennane M, Ljunggren D, Karlsson A, Jonsson P,* Hening A and Ciscar J P 2000 Experimental longwavelength quantum cryptography: from single-photon transmission to key extraction protocols J. Mod.Opt. 47 563–79
8. Id 3000 Device Access Library Reference Guide, V-2.35, June 2005, Id Quantique
9. *Д.М. Голубчиков*, «Моделирование квантового канала распределения ключей», Известия ТРТУ, №9, 2006
10. *Д.М. Голубчиков*, «Анализ способов съема информации с квантового канала распределения ключей и методы их обнаружения», Сборник тезисов конференции «Современные информационные технологии - 2007», 2007
11. *Д.М. Голубчиков*, «Применение квантовых усилителей для съема информации с квантовых каналов распределения ключей», Известия ТТИ ЮФУ. Технические науки, 2008
12. *Д.М. Голубчиков*, «Использование статистической модели квантово-криптографического канала при проектировании устройства съема информации», Сборник тезисов докладов «Новые информационные технологии - 2007», 2007