УДК 681.3.067:621.396.2

Я. С. Розова, Д. М. Голубчиков

ИССЛЕДОВАНИЕ ПРИНЦИПОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА ПРИМЕРЕ ID 3000 CLAVIS

Квантовая криптография — одно из многообещающих направлений в рамках квантовой теории информации. И лидеры направления спешат с коммерческой реализацией своих наработок, учитывая то, что цена секретности и безопасности коммуникаций очень высоки. Сферы применения охватывают дипломатическую связь, военное дело, бизнес и другие сферы, где требуется передача секретной (конфиденциальной) информации.

Мировыми лидерами в области производства систем квантового распределения ключей для применения в коммерческих приложениях являются компании, две из которых находятся в Европе – Id Quantique и Smart Quantum, третья в США – MagiQ Technology. Производимые ими системы построены по двунаправленной схеме с автокомпенсацией поляризационных искажений. В данной работе рассмотрена система - Id3000 Clavis, производства компании Id Quantique, которая 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 [1-2].

Описание работы системы id3000 Clavis

Работа системы id 3000 Clavis основана на использовании технологии Plug&Play (подключай и работай). Рассмотрим в общих чертах принцип работы данной системы.

Система состоит из трех частей: устройство, излучающее и принимающее закодированный сигнал (станция Bob), пассивное устройство, модулирующее излученный сигнал (станция Alice) и среда распространения сигнала, в качестве которой выступает одномодовое оптическое волокно [3] (Рис. 1).

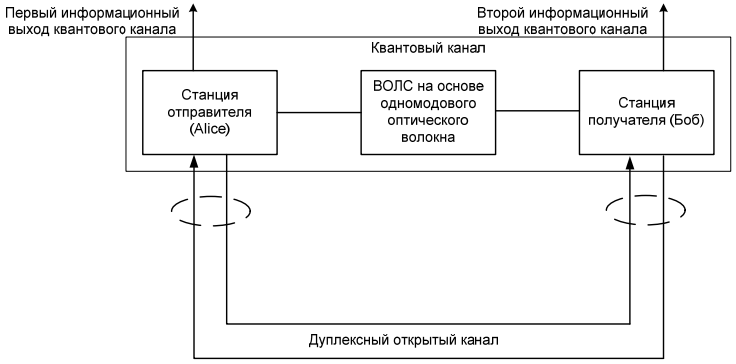


Рис. 1. Структурная схема системы id3000 Clavis

Схема оптической части станции Bob приведена на рис. 2. Рассмотрим, как преобразуется сигнал, проходя прямой путь от станции Bob к станции Alice).

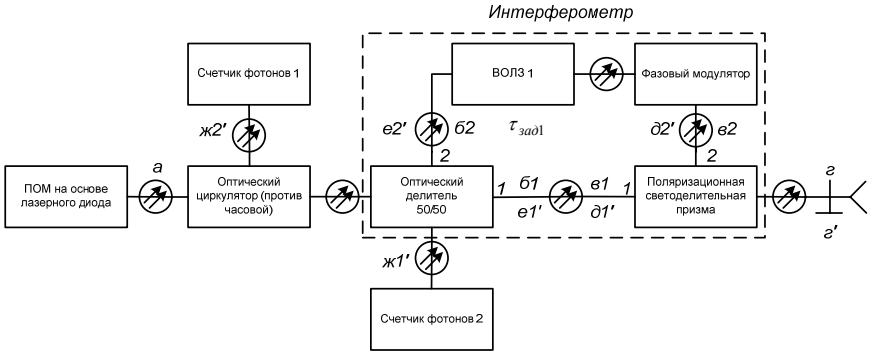


Рис. 2. Схема оптической части станции Bob

Лазер, работающий на длине волны 1550 нм, излучает импульс. Излученный импульс, пройдя через отрезок волокна (все волокна, использующиеся внутри станций, являются *волокнами сохраняющими поляризацию*) попадает на оптический делитель, где разделяется на два импульса равных по амплитуде.

Импульс, выведенный через порт 1, проходит через короткое плечо интерферометра, другой, выведенный через порт 2 – через длинное, получая при этом временную задержку и более значительное ослабление, чем первый импульс. Далее импульс, прошедший через короткое плечо и импульс, прошедший через длинное плечо, по средствам поляризационного светоделителя, работающего как оптический мультиплексор, вводятся в линию передачи.

Таким образом, сигнал, состоящий из двух импульсов (импульс с большей энергией и ослабленный импульс, задержанный на 50 нс) выводится из станции Bob и направляется к станции Alice через оптическое волокно. Причем до того, как сигнал попадет в станцию Alice, он не несет никакой информации.

Далее, сигнал попадает в станцию Alice, структурная схема которого приведена на рис. 3.

Рис. 3. Схема оптической части станции Alice

На входе данного устройства энергия всего сигнала разделяется как 10/90. Таким образом, 90 % энергии сигнала направляется через порт 3 в плечо, где расположен приемный оптический модуль, необходимый для синхронизации и обеспечения безопасности, а 10 % энергии через порт 2 распространяется по плечу с фазовым модулятором (ФМ). Эти 10 % энергии дополнительно ослабляются для обеспечения однофотонности отраженных импульсов. Далее импульсы проходят линию задержки и ФМ. Последний узел станции Alice (зеркало Фарадея), отражает импульсы, при этом изменяя плоскость их поляризации на 90^0. И сигнал осуществляет обратный путь к станции Bob. Сигнал на обратном пути уже несет информацию о закодированном бите в фазовом состоянии второго импульса.

После отражения от зеркала, при прохождении ФМ, только малый однофотонный импульс кодируется по фазе. Далее, сигнал с помощью оптического мультиплексора вводится в интерферометр станции Bob, причем тот сигнал, который проходил длинное плечо, проходит, теперь короткое и наоборот. После этого они попадают одновременно на светоделитель и интерферируют. Результат интерференции регистрируется одним или другим приемным модулем, представляющим собой счетчики фотонов. Если разность фаз импульсов составляет π, наблюдается деструктивная интерференция и импульсу присваивается значение *«1»*. Когда разность фаз составляет *0* или π – наблюдается конструктивная интерференция и импульсу присваивается значение «0». Если интерференция имеет место на обоих счетчиках, то это случай ошибочного приема. Так как оба импульса проходят один и тот же оптический путь, то такой интерферометр считается автокомпенсирующимся. Для реализации протокола BB84 в станции Alice второй импульс сдвигается по фазе на одно из случайно выбранных значений из ряда *0,* $\pi/2$, π, $3\pi/2$, а в станции Bob выбирается базис измерения посредствам фазового сдвига первого импульса на *0* или $\pi/2$ при обратном распространении импульса [4].

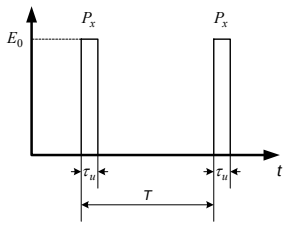
Эпюры импульсов в характерных точках системы id3000 Clavis

Точки на рисунках системы обозначены прописными буквами и цифрами. При обратном распространении сигнала, к обозначению добавлен апостроф (′)

На рисунках 4-9 показаны эпюры импульсов в характерных точках системы id3000 Clavis при распространении импульсов от станции Alice к станции Bob (см. рисунки 2 и 3).

Лазер станции Bob излучает импульсы с заданным вертикальным направлением поляризации. Эпюры этих импульсов показаны на рис. 5

а

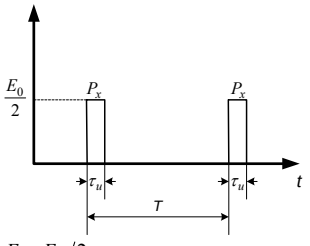


$\tau_u = 300...2500нс$;
$T = 200нс$;
$P_x = \updownarrow$ – вертикальная поляризация;
$E = E_0$.

Рис. 4. Импульсы излученные станцией Bob

Энергия этих импульсов делится пополам на оптическом делителе 50/50 (Рис 5).

б1



$E = E_0/2$

б2

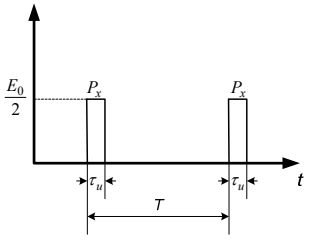
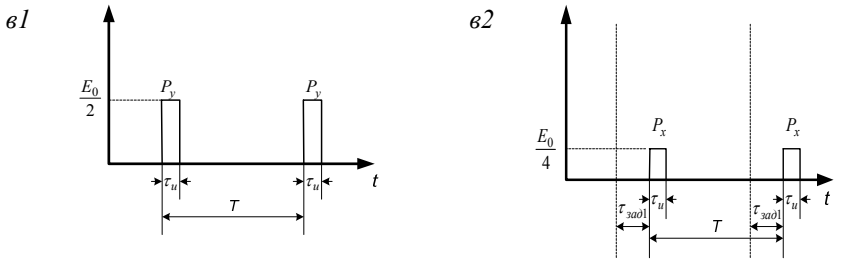


Рис. 5. Импульсы, прошедшие через оптический делитель 50/50 станции Bob

Пройдя через короткое плечо, поляризация первой половины (P_1) исходного импульса меняет свое направление на горизонтальное. При этом энергия P_1 меняется незначительно, поэтому этим изменением можно пренебречь. Энергия второй половины (P_2) исходного импульса уменьшается в 2 раза. Это достигается подбором длины этого плеча. Эпюры импульсов показаны на рис. 6.



$P_y = \leftrightarrow$ - горизонтальная поляризация

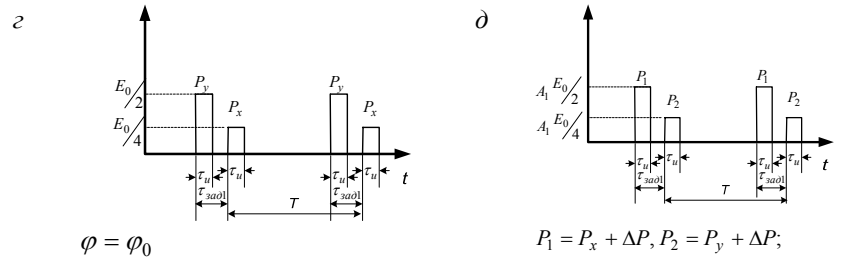
$E = A_0 E_0/2 = E_0/4;$

$\tau_{зад1} = 50нс;$

A_0 – затухание в длинном плече станции Bob.

Рис. 6. Импульсы прошедшие короткое (в1) и длинное (в2) плечо интерферометра станции Bob

Поляризационная светоделительная призма вводит обе части импульса в ВОЛС (Рис. 7г) фаза импульсов остается неизменной. Проходя ВОЛС, суммарная энергия импульса снижается (Рис. 7д). При этом поляризация импульсов изменяется случайным образом на ΔP для импульса P_1 и на ΔP - для P_2 . А так же при прохождении ВОЛС импульсы получают фазовый сдвиг $\varphi_{ВОЛС}$.



$\varphi = \varphi_0$

$P_1 = P_x + \Delta P, P_2 = P_y + \Delta P;$

$\varphi = \varphi_0 + \varphi_{ВОЛС};$

A_1 – коэффициент передачи ВОЛС.

Рис. 7. Сигнал, введенный в ВОЛС (г) и прошедший через ВОЛС (д)

Сигнал поступает в станцию Bob. В станции Bob, при помощи оптического делителя 10/90, 0,1 часть энергии сигнала выводится на порт 2, а 0,9 – на порт 3 (Рис. 8).

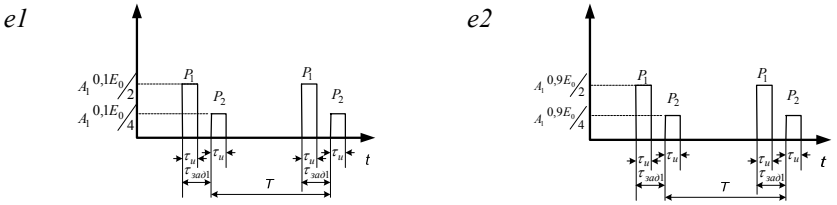


Рис. 8. Разделение сигнала на оптическом делителе 10/90

Сигнал, выведенный через 3 порт, служит для выработки сигнала синхронизации. Перед поступлением на фотоприемник сигнал должен быть ослаблен, что и осуществляется с помощью ПОА2. Величина данного затухания зависит от длины линии связи. Сигнал, выведенный через порт 2, при обратном прохождении будет нести информацию о закодированном двоичном символе. Этот сигнал, для обеспечения условия однофотонности, ослабляется ПОА1. Величина затухания, вносимая ПОА1 так же зависит от длины линии связи и от среднего количества фотонов в импульсе, заданного пользователем. Эпюры сигналов показаны на рис. 9.

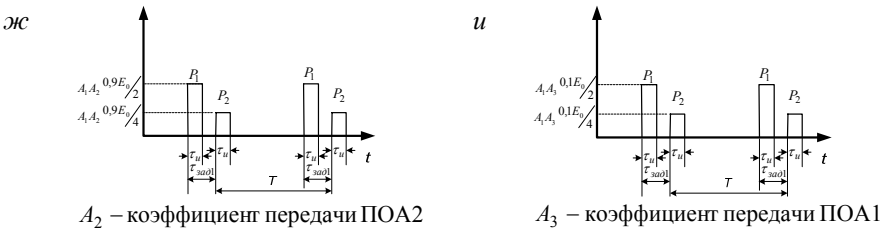


Рис. 9. Сигналы, ослабленные ПОА2 (ж) и ПОА1 (и)

Далее импульсы отражаются от зеркала Фарадея, и в них изменяется направление поляризации на ортогональное. После отражения, сигнал снова вводится в оборудование станции Alice и распространяется в обратном направлении. Эпюры отраженных импульсов показаны на рис. 10.

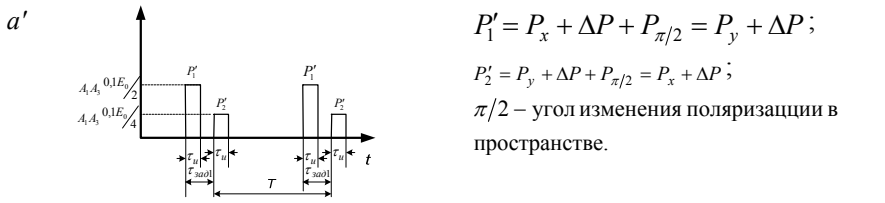


Рис. 10. Сигналы, отраженные от зеркала Фарадея

Сигнал с измененной поляризацией попадает на фазовый модулятор, где вносится сдвиг фаз $\varphi_м$ (Рис. 11).

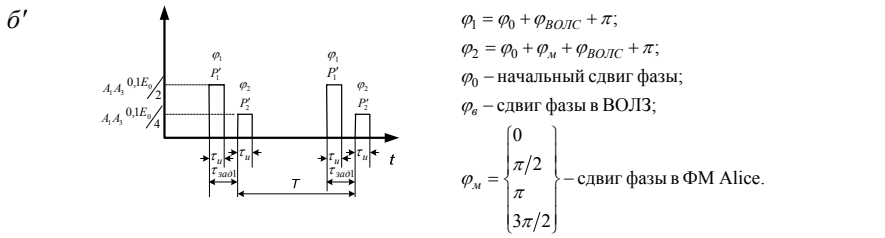
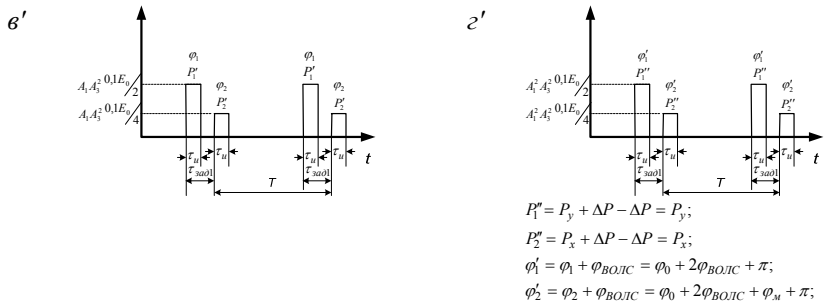


Рис. 11. Сигналы, после прохождения фазового модулятора станции Bob

Далее импульсы ослабляются в ПОА1 и через оптический делитель поступает в ВОЛС. Пройдя ВОЛС, импульсы ослабляются, происходит изменение поляризации, а так же импульсы получают дополнительный фазовый сдвиг $\varphi_{ВОЛС}$ (Рис. 13).



$P_1'' = P_y + \Delta P - \Delta P = P_y;$

$P_2'' = P_x + \Delta P - \Delta P = P_x;$

$\varphi_1' = \varphi_1 + \varphi_{ВОЛС} = \varphi_0 + 2\varphi_{ВОЛС} + \pi;$

$\varphi_2' = \varphi_2 + \varphi_{ВОЛС} = \varphi_0 + 2\varphi_{ВОЛС} + \varphi_м + \pi;$

Рис. 12. Сигналы на входе (в′), и выходе (г′) ВОЛС

Приходя в станцию Bob, импульсы входящие в сигнал разделяются. P_1'' выводится через порт 2, а P_2'' через порт 1 поляризационной светоделительной призмы (Рис. 13).

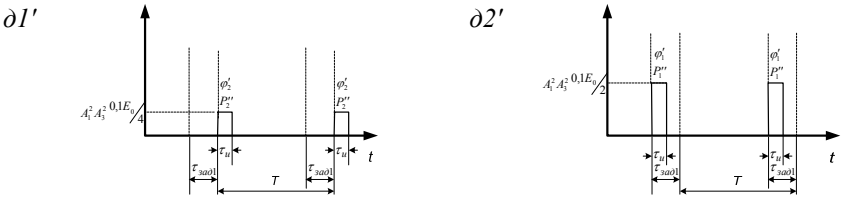
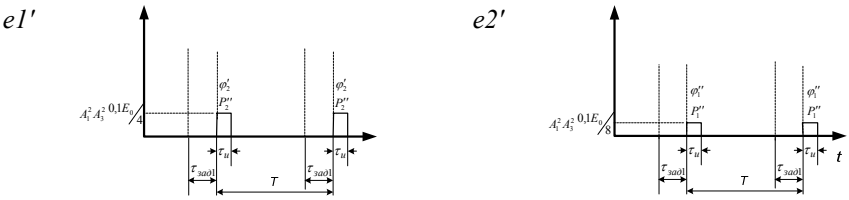


Рис. 13. Импульсы поступающие в короткое (д1′) и длинное (д2′) плечи интерферометра станции Bob

Импульс, прошедший через короткое плечо практически не получит изменений, поэтому мы ими пренебрежем. Импульс, прошедший через длинное плечо, в котором расположен модулятор, получает фазовый сдвиг $\varphi_м'$ (Рис. 14).



$\varphi_1'' = \varphi_1' + \varphi_м';$

$\varphi_м' = \begin{Bmatrix} 0 \\ \pi/2 \end{Bmatrix}.$

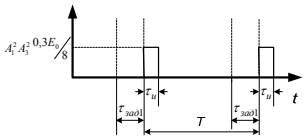
Рис. 14. Импульсы, после прохождения короткого (е1′) и длинного (е2′) плеч интерферометра станции Bob

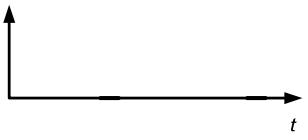
В зависимости от разности фаз пришедших импульсов получается азличное значение двоичного символа. Разность фаз по приходу импульсов на счетчик фотонов определяется по формуле:

$$\Delta\varphi = \varphi_2' - \varphi_1'' = (\varphi_0 + \varphi_м + 2\varphi_{ВОЛС} + \pi) - (\varphi_0 + \varphi_м' + 2\varphi_в + \pi) = \varphi_м - \varphi_м' = \begin{Bmatrix} 0 \\ \pi/2 \\ \pi \\ 3\pi/2 \end{Bmatrix} - \begin{Bmatrix} 0 \\ \pi/2 \end{Bmatrix}$$

Все возможныеслучаи, регистрации однофотонных импульсов счетчиками фотонов 1 и 2 согласно протоколу BB84 показаны на рис. 15.

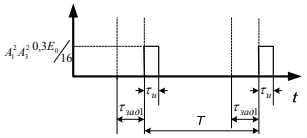
при $\varphi_м = 0$ и $\varphi_м' = 0$

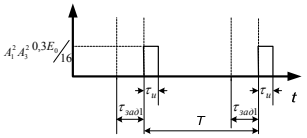
ж1' 

ж2' 

Значение бита: 0

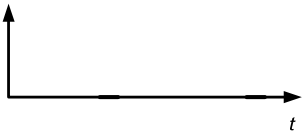
при $\varphi_м = \pi/2$ и $\varphi_м' = 0$

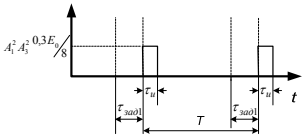
ж1' 

ж2' 

Значение бита не может быть определено однозначно

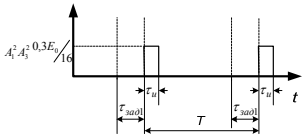
при $\varphi_м = \pi$ и $\varphi_м' = 0$

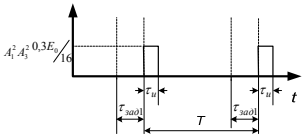
ж1' 

ж2' 

Значение бита: 1

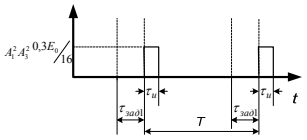
при $\varphi_м = 3\pi/2$ и $\varphi_м' = 0$

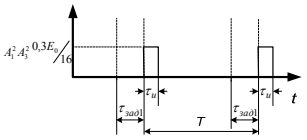
ж1' 

ж2' 

Значение бита не может быть определено однозначно

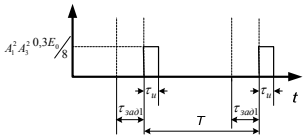
при $\varphi_м = 0$ и $\varphi_м' = \pi/2$

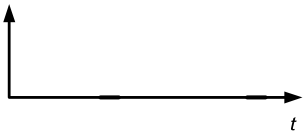
ж1' 

ж2' 

Значение бита не может быть определено однозначно

при $\varphi_м = \pi/2$ и $\varphi_м' = \pi/2$

ж1' 

ж2' 

Значение бита: 0

при $\varphi_м = \pi$ и $\varphi'_м = \pi/2$

Значение бита не может быть определено однозначно

Рис. 15. Эпюры импульсов при детектировании на счетчиках фотонов при различных разностях фаз

при $\varphi_м = 3\pi/2$ и $\varphi'_м = \pi/2$

Значение бита: 1

Рис. 15. Эпюры импульсов при детектировании на счетчиках фотонов при различных разностях фаз

Описание принципа работы фотодетектора в токовом режиме станции Alice системы id3000 Clavis

Станция Alice осуществляет модуляцию импульса излученного станцией Bob. В состав станции входит фотодетектор работающий в токовом режиме, предназначенный для обеспечения синхронизации. Структурная схема детектора станции Alice представлена на рис. 16.

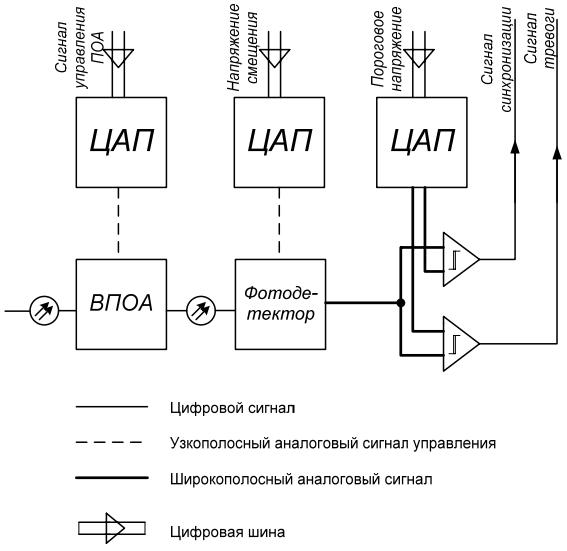


Рис. 16. Структурная схема детектора в станции Alice

На схеме введены обозначения:
ЦАП – цифроаналоговый преобразователь;
ПОА – перестраиваемый оптический аттенюатор.
Рассмотрим подробнее принцип работы детектора.

На входе детектора стоит перестраиваемый оптический аттенюатор. Он используется для предотвращения повреждения фотодетектора мощным излучением. Величина затухания устанавливается в зависимости от длины линии передачи.

Чтобы фотодетектор всегда находился в состоянии готовом к работе, на него подается напряжение смещения. На выходе фотодетектора устанавливают два компаратора для сравнения мощности принимаемых импульсов с вырабатываемыми микропроцессорной логикой уровнями энергии.

Первый компаратор производит сравнение пришедшего сигнала с уровнем, ниже которого сигнал воспринимается как шум. Если пришедший сигнал обладает энергией выше заданного уровня, то вырабатывается сигнал синхронизации. Если сигнал обладает энергией намного превышающий заданный уровень, то можно предположить, что излишняя энергия была введена злоумышленником с целью осуществления широкой импульсной атаки или атаки типа «Троянский конь». Чтобы предотвратить воздействие мощного излучения на узлы станции и вывода их из строя используют второй компаратор. На нем происходит сравнение с максимально возможным уровнем мощности сигнала и в случае превышения его вырабатывается сигнал тревоги [5].

Следует отметить, что фотодетектор не чувствителен к состоянию поляризации приходящего сигнала.

Все сигналы, с которыми работает фотодетектор и компаратор – аналоговые. Так как управляющие сигналы и сигналы пороговых уровней являются цифровыми, то их преобразуют, используя ЦАП. Сигналы на выходе компараторов так же являются цифровыми, так как их появление зависит от результатов сравнения с пороговыми значениями.

Заключение

В идеальном случае, каналы квантового распределения ключа являются абсолютно безопасными, так как, исходя из законов физики, невозможно произвести измерение квантового состояния без его разрушения. И подобный перехват моментально обнаруживается участниками обмена по возникающим ошибкам в передаче. Однако реальные системы отличаются от идеальных.

Во-первых, аппаратура участников информационного обмена несовершенна, что приводит к появлению ошибок приема-передачи. В этих обстоятельствах наличие определенного уровня ошибок не должно восприниматься системой как попытка подслушивания. А наличие собственного фона ошибок позволяет противнику осуществлять перехват, маскируя неизбежно возникающие при этом искажения под собственные ошибки системы.

Во-вторых, в реальных линиях передачи существует затухание сигнала, что вынуждает отправителя увеличивать энергию импульса, т.е. число фотонов в нем. Это приводит к потере части импульсов в канале. В первом случае, если импульс содержит множество фотонов, поляризованных одинаковым образом, появляется возможность с помощью светоделителя сделать отвод и измерить уже состояния отведенных фотонов, не искажая основной сигнал. Понятно, что такой перехват следует осуществлять как можно ближе к отправителю — там уровень сигнала выше. Во втором случае затухание сигнала приводит к увеличению общего уровня ошибок, и у противника увеличиваются шансы замаскировать перехват под собственные ошибки системы.

Поэтому практическое исследование системы Id 3000 Clavis, являющееся одной из первых коммерческих реализаций систем квантового распределения ключа, представляет большой интерес с точки зрения анализа характеристик квантового канала формируемого системой. Программное обеспечение системы 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, максимально приближенных к реальным характеристикам системы. А, следовательно, полученные результаты могут быть применены для поиска новых способов несанкционированного съема информации с квантовых каналов и создания устройств предотвращающих атаки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden.* Quantum Cryptography, submitted to Reviews of Modern Physics, January 19, 2001.
2. *Charles H. Bennett et al.* Experimental Quantum Cryptography, Journal of Cryptology, no. 5, 1992.
3. *Голубчиков Д.М.* Моделирование квантового канала распределения ключа. Известия ТРТУ. Специальный выпуск. Технические науки. Материалы LII научно-технической конференции профессорско-преподавательского состава, аспирантов и сотрудников ТРТУ. Таганрог: Изд-во ТРТУ. 2006. №9(64) С.162-163
4. Quantum Key Distribution System id 3000 User Guide, V-2.35, June 2005, Id Quantique
5. *Румянцев К.Е., Хайров И.Е. Троцюк Е.В.* Исследование квантово- криптографического метода формирования секретного ключа. // Научно-практ. журнал "Информационное противодействие угрозам терроризма". 2004. №2. С.24-26.
6. *Wolfgang Tittel, Gregoire Ribordy and Nicolas Gisin*. Quantum Cryptography, Physics World, March 1998.
7. *Paul D.* Townsend. Secure key distribution system based on Quantum cryptography, Elect. Letters, 30, 1994.
8. *R. J. Hughes, G. L. Morgan, C. G. Peterson*. Practical quantum key distribution over a 48-km optical fiber network, Journal of Modern Optics, 47, 2000.
9. *Martinelli M.,* A universal compensator for polarization changes induced by birefringence on a retracting beam. Opt. Commun., 1989, vol. 72, pp. 341-344
10. *Townsend, P. D., Rarity, J. G., and Tapster, P. R.*, Single photon interference in 10 km long optical fibre interferometer. Electronics Letters, Vol. 29, no. 7, 1993, pp. 634-635.