УДК 621.383.92

О.К. Барановский, О.Ю. Горбадей, А.О. Зеневич, Е.В. Василиу, И.В. Лимарь

КВАНТОВЫЙ МЕТОД БЕЗОПАСНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ШИФРОВАНИЯ

В работе показана возможность использования счетчиков фотонов на основе лавинных фотодиодов для создания квантовой системы распределения ключей шифрования по оптоволоконным линиям связи. Для решения задачи безопасной передачи ключей предложен квантовый метод. Определены условия и характеристики системы, позволяющие организовать защищенный канал для генерации и передачи ключей.

Ключевые слова: квантовая система распределения ключей, оптоволоконная линия связи, обнаружение несанкционированного пользователя, счетчик фотонов.

Введение

Сегодня широко применяемой средой передачи цифровых данных является оптическое волокно, что позволяет обеспечить скорость передачи до 10 Тбит/с. Для решения задач обеспечения конфиденциальности используют алгоритмы криптографической защиты информации. В связи со значительно более высоким быстродействием симметричных систем шифрования по сравнению с ассиметричными, выбор осуществляется в пользу симметричных криптографических систем. Однако, одной из основных трудностей при использовании таких систем является проблема распределения ключей [1], особенно когда необходимо организовать передачу ключа шифрования двум или более санкционированным пользователям, используя незащищенный канал связи.

Квантовое распределение ключей является новейшей технологией, решающей эту проблему [2,3]. Предлагаемые в настоящее время на рынке системы квантового распределения ключей реализуют стек протоколов, который состоит как из непосредственно протоколов передачи информации отдельными фотонами, так и из реализующих дополнительные процедуры усиления секретности, позволяющие безопасно распределить ключ даже при наличии несанкционированного подключения к каналу связи (если уровень ошибок, создаваемых перехватом в канале, не превышает некоторого порога). Однако, предлагаемые на рынке системы предназначены для распределения ключей только между парами пользователей и имеют высокую рыночную стоимость.

Еще одним путем решения проблемы распределения ключей может быть их квантовое распределение по упрощенному протоколу, в основе реализации которого лежит контроль отсутствия в канале связи несанкционированного пользователя. Это позволит упростить и, соответственно, снизить себестоимость готовой системы квантового распределения ключей.

Как показано в работах [3,4], наиболее эффективными являются методы контроля отсутствия несанкционированного подключения к каналу, основанные на регистрации изменения состояния фотонов на выходе оптического волокна в случае подключения несанкционированного пользователя по сравнению со штатным режимом работы. Однако предложенные методы могут быть использованы только в случае организации связи между двумя санкционированными абонентами.

Важным фактором в криптографических системах является процедура формирования ключа шифрования. Как показано в работе [5], для создания ключа шифрования предпочтительно использовать генераторы случайных чисел, в основу работы которых положены шумовые или хаотические физические процессы. Наиболее подходящими среди них, для применения в линиях связи на основе оптического волокна, являются квантовые генераторы случайных чисел [6].

В криптографических системах, использующих оптическое волокно, целесообразно использовать квантовые генераторы случайных чисел с реализацией функции обнаружения несанкционированного подключения к волокну во время формирования ключа шифрования. Указанная функция позволит также обеспечить безопасность передачи ключа шифрования.

На основании вышеизложенного, *целью работы* является создание квантового метода распределения ключей шифрования, включающего процедуры генерации и передачи по оптическому волокну между несколькими санкционированными пользователями, на основе принципов работы квантовых генераторов случайных чисел и реализующего функцию надежного обнаружения несанкционированного подключения.

Обоснование метода

Несанкционированный доступ к оптическим линиям связи реализуется с использованием способов разрывного и безразрывного подключения. Для реализации первого способа подключения необходимо разделение волокна на отдельные части и подключение несанкционированного пользователя как минимум между двумя его частями. Второй способ подключения позволяет осуществлять снятие информации с оптического волокна без разделения его на части.

Разрывный способ подключения несанкционированного пользователя является более надежным для съема данных по сравнению с другими. Однако факт несанкционированного подключения к находящемуся в эксплуатации волокну легко обнаруживается, так как требует временного отключения линии передачи данных.

Разрывный способ подключения реализуется в местах, где находятся механические контакты и соединения в виде коннекторов, розеток, переходников, разветвителей, аттенюаторов, муфт, патчкордов, сборок и других элементов. Меры защиты в целях ограничения доступа посторонних лиц к контактам и соединениям оптического волокна реализуются в форме организационно-технических мероприятий.

Также разрывный способ подключения реализуется путем врезки в оптическое волокно. В этом случае в местах врезки образуются сварные швы. Наличие сварных швов в оптическом волокне достаточно хорошо диагностируется [7]. Поэтому угрозы разрывного способа подключения далее рассматриваться не будут.

Безразрывный способ подключения несанкционированного пользователя имеет более высокую скрытность по сравнению с разрывным способом, поскольку он реализуется на участках оптического волокна с наличием бокового излучения. Под боковым излучением понимают процесс испускания оптических волн с поверхности волокна, вдоль которой распространяется оптическое излучение.

Появление бокового излучения связано с нарушением закона полного внутреннего отражения оптического излучения в волокне. Это может произойти из-за различных внешних воздействий на некоторый участок волокна. Такие воздействия могут быть механические, электрические, магнитные, химические, радиационные и др. Также боковое излучение может возникать в местах неправильной укладки и монтажа оптического кабеля.

Существуют следующие способы регистрации оптического излучения с боковой поверхности оптического волокна:

- пассивный – регистрация излучения с боковой поверхности оптического волокна в местах неправильной укладки и монтажа оптического кабеля;
- активный – создание неоднородностей в оптическом волокне для обеспечения вывода излучения через его боковую поверхность с последующей регистрацией;
- компенсационный – регистрация излучения, выводимого через боковую поверхность оптического волокна с последующим формированием и вводом в волокно излучения, компенсирующего потери энергии при выводе излучения.

Наличие участков оптического волокна с боковым излучением можно исключить путем контроля за правильностью проведения работ по укладке и монтажу оптического кабеля. Поэтому далее пассивный способ рассматриваться не будет.

Остановимся на рассмотрении метода обнаружения несанкционированного подключения к оптическому волокну при помощи активного и компенсационного способов.

При активном способе съема оптического излучения с боковой поверхности оптического волокна происходит уменьшение энергии передаваемого информационного сигнала. Минимальное уменьшение энергии сигнала соответствует энергии одного фотона.

При компенсационном способе съема оптического излучения с боковой поверхности оптического волокна возникает временная задержка в распространении информационного сигнала или его части по сравнению со штатным режимом работы. Минимальная задержка в таком случае будет являться суммой времен прохождения фотоном расстояния от места его вывода из оптического волокна до места детектирования, поглощения фотона в фотодетекторе, излучения фотона, прохождения фотона до места ввода его в оптическое волокно. Оценка времени минимальной задержки показывает, что она составляет около 1 нс.

Таким образом, определить наличие подключения при помощи активного способа съема можно путем контроля уменьшения мощности или энергии информационного сигнала. Поскольку минимальное уменьшение энергии информационного сигнала эквивалентно энергии одного фотона, то для регистрации соответствующего уменьшения необходимо использовать фотоприемные устройства, обладающие высокой чувствительностью. Такие фотоприемные устройства должны быть способны регистрировать отдельные фотоны. Поэтому для обнаружения подключения при помощи активного способа съема необходимо использовать фотоприемники, работающие в режиме одноквантовой регистрации.

Для обнаружения факта подключения компенсационным способом съема необходимо оценить изменение времени распространения информационного сигнала по оптическому волокну при наличии подключения указанным способом по сравнению со штатным режимом работы линии связи. Отметим, что измерить это время с субнаносекундным разрешением можно при помощи метода одноквантовой регистрации [8].

В связи с этим для обнаружения несанкционированного подключения к оптическому волокну указанными способами необходимо использовать устройства регистрации оптического излучения на основе фотоприемников, работающих в режиме одноквантовой регистрации. Как показано в работах [8,9], для этих целей эффективным является использование лавинных фотоприемников.

Согласно работе [6], лавинные фотоприемники, работающие в режиме одноквантовой регистрации, могут применяться для формирования случайных двоичных последовательностей. Это значит, что их можно применять для создания ключей шифрования.

На основании вышеизложенного можно предложить квантовый метод генерации и передачи ключа шифрования нескольким абонентам, заключающийся в следующем: вначале, по оптическому волокну от одного из пользователей-абонентов системы приема-передачи информации к пользователю, отвечающему за формирование и передачу ключей шифрования, передается непрерывное оптическое излучение постоянной интенсивности со статистикой фотонов, соответствующей распределению Пуассона; оптическое излучение регистрируется лавинным фотоприемником, работающим в режиме одноквантовой регистрации; после чего формируется выборка выходных импульсов лавинного фотоприемника; на основании выборки создается случайная двоичная последовательность, которая может служить в качестве ключа шифрования; выше приведенная последовательность действий выполняется для других пользователей-абонентов системы приема-передачи информации, пока не будет сформировано необходимое число ключей шифрования; затем один, например, выбранный случайным образом, из полученных ключей шифрования передается от пользователя, отвечающего за формирование и передачу ключей шифрования, другим пользователям-абонентам системы приема-передачи информации с одновременной проверкой наличия несанкционированного пользователя (злоумышленника) в линии связи; в случае обнаружения несанкционированного пользователя передача ключа прекращается по указанной линии; осуществляется смена ключа на другой и его передача по другим линиям связи с одновременной проверкой наличия несанкционированного пользователя (злоумышленника).

Отметим, что особенностью предложенного метода является постоянное наличие оптического контрольного сигнала в оптическом волокне, что не позволит несанкционированному пользователю реализовать скрытным образом разрывное подключение к волокну.

Квантовая система безопасного распределения ключей шифрования

Структурная схема квантовой системы, реализующей предложенный метод, представлена на рис. 1. Система состоит из устройств приема и передачи информации (санкционированные пользователи) A1 – A8 и устройства формирования и передачи ключей шифрования и информации B. Устройства приема и передачи информации A1 – A8 связаны последовательно по кольцу между собой и радиально с устройством B при помощи оптического волокна, как показано на рис. 1.

Формирование ключа шифрования выполняется следующим образом. По оптическому волокну в радиальном направлении от A1 – A8 к B передается непрерывное оптическое излучение постоянной интенсивности со статистикой фотонов, соответствующей распределению Пуассона. Используются лазерные диоды с длиной волны оптического излучения 850 нм, ослабление интенсивности излучения для реализации режима счета отдельных фотонов реализуется при помощи нейтральных светофильтров. Регистрация оптического излучения осуществляется кремниевыми лавинными фотоприемниками (ЛФП), работающими в режиме одноквантовой регистрации.

Вследствие статистического характера оптического излучения из последовательности выходных импульсов ЛФП формируется случайная выборка. На основании совокупности выборок формируется случайная двоичная последовательность следующим образом. Уровень логического нуля соответствует случаям, когда за фиксированное время формирования выборки регистрируется четное число импульсов. При регистрации за указанное время нечетного числа импульсов, устанавливается уровень логической единицы. Таким образом, формируется случайная двоичная последовательность, содержащая нули и единицы, которая может служить в качестве ключа шифрования. Поскольку оптическое излучение к устройству B передается от всех устройств A1 – A8, то в B происходит формирование до 8 ключей.

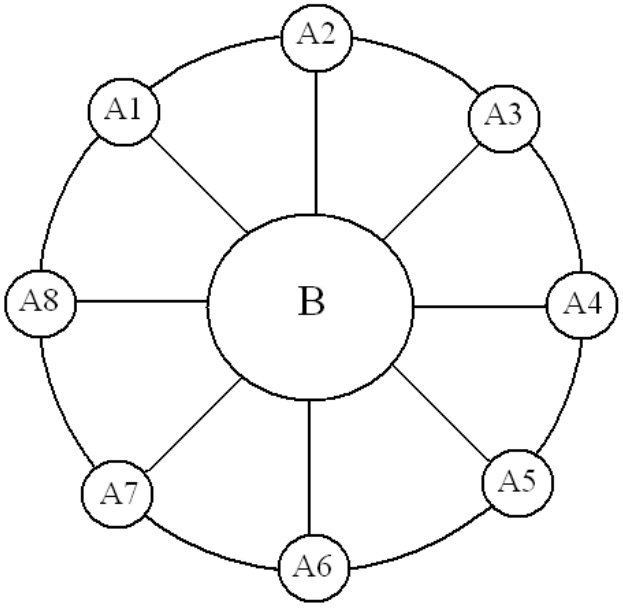

Рис.1. Структурная схема системы, реализующей квантовый метод генерации и передачи ключей. A1-A8 – устройства приема и передачи информации (санкционированные пользователи), B – устройство формирования и передачи ключей шифрования

Передача ключа шифрования реализуется по вышеописанному способу. При этом из общего числа ключей шифрования, хранящихся в устройстве В, выбирается случайным образом один и передается к устройствам А1 – А8. Во время передачи ключа осуществляется контроль отсутствия подключения несанкционированного пользователя. При обнаружении несанкционированного пользователя передача ключа прекращается по тому оптическому волокну, где он обнаружен. После чего происходит смена ключа на другой с последующей его передачей по другим оптическим волокнам, в которых подключение несанкционированного пользователя не обнаружено, к устройствам А1 – А8. Отметим, что в этом случае передача ключа может осуществляться не напрямую от устройства В к другим устройствам, а в обход оптического волокна с несанкционированным пользователем, через устройства А1 – А8. Таким образом, даже при наличии несанкционированного пользователя удается осуществить передачу ключа шифрования, не раскрыв его содержания злоумышленнику.

На рис.2 представлена детализированная схема приема и передачи информации между устройствами В и А1, реализующая процедуры формирования и передачи ключей шифрования, организации защищенной связи между устройствами.

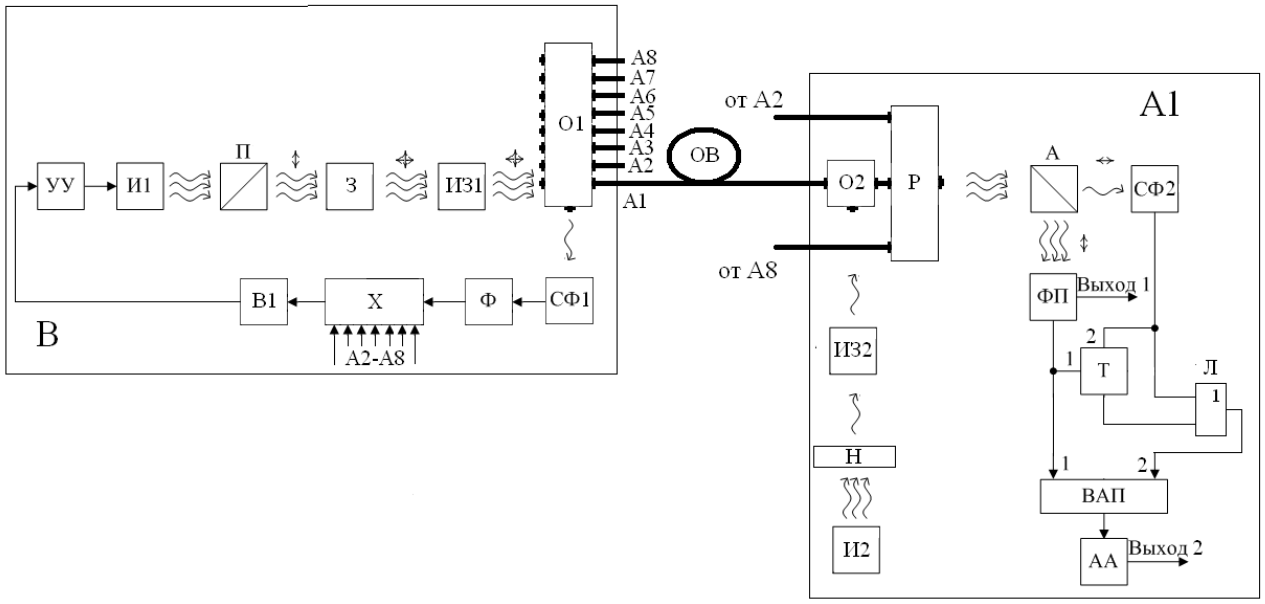

Рис.2. Детализированная схема приема и передачи информации между устройствами В и А1.

Процедура формирования ключа начинается в устройстве А1 путем направления оптического излучения от источника И2 через нейтральный светофильтр Н для ослабления его интенсивности. После чего оптическое излучение подается на оптический изолятор ИЗ2. Оптический изолятор пропускает оптическое излучение только в одном направлении от источника И2 к оптическому ответвителю О2. Оптическое излучение проходит через ответвитель О2 и поступает в оптическое волокно ОВ. На выходе ОВ в устройстве В оптическое излучение попадает через оптический ответвитель О1 на счетчик фотонов СФ1. Счетчик фотонов СФ1 формирует выборки. Выборки поступают на формирователь Ф, который создает случайную двоичную последовательность, состоящую из символов «0» и «1», с последующим формированием ключа шифрования. Затем сформированный ключ записывается в блок хранения ключей Х. Аналогичным образом происходит формирование в устройстве В ключей шифрования, полученных с участием устройств А2 – А8. Ответвитесь О1 обеспечивает передачу сигналов от устройств А2 – А8, которые каждый от своего выхода (см. рис. 2) проходят те же последовательности блоков (счетчик фотонов, формирователь), которые установлены на его выходах. После чего поступают на один из входов блока хранения ключей Х.

Процедура передачи ключа из устройства В в устройство А1 происходит следующим образом. В устройстве В при помощи блока В1 случайным образом из блока хранения Х выбирается один из ключей шифрования. После чего этот ключ подается на вход блока управления УУ. При подаче на вход УУ символа «0» на его выходе устанавливается уровень напряжения, соответствующий логическому нулю. При этом оптическое излучение на выходе источника И1 отсутствует. При появлении на входе УУ символа «1» на его выходе устанавливается уровень напряжения, соответствующий логической единице. В этом случае на выходе источника И1 появляется оптическое излучение. Излучение от источника И1 поступает на поляризатор П. Поляризатор П линейно поляризует излучение. Затем оптическое излучение поступает на формирователь сигналов З, который создает контрольный и информационный сигналы. При этом контрольный и информационный сигналы поляризованы во взаимно перпендикулярных плоскостях, а также контрольный сигнал задерживается на некоторое время относительно информационного. Формирователь З создает контрольный сигнал таким образом, чтобы он содержал в среднем один фотон на сигнал. Отметим, что информационный сигнал используется для передачи данных между санкционированными пользователями, а контрольный сигнал для обнаружения несанкционированного подключения к оптическому волокну.

Далее излучение через оптический изолятор ИЗ1 подается на оптический ответвитесь О1, после чего оно поступает одновременно на устройства А1 – А8. Оптический изолятор ИЗ1 используется для того, чтобы оптическое излучение от устройств А1 – А8 не поступало на вход формирователя сигналов З. Детально рассмотрим работу устройства А1. Отметим, что построение и работа других устройств А2 – А8 аналогична.

Излучение на устройство А1 передается по оптическому волокну ОВ. С выхода оптического волокна в устройстве А1 излучение поступает на вход ответвителя О2, а затем на вход оптического разветвителя Р. С выхода разветвителя Р оптическое излучение подается на анализатор А.

Анализатор А разделяет оптическое излучение в зависимости от его поляризации. После чего информационный сигнал подается на фотоприемное устройство ФП, а контрольный сигнал – на счетчик фотонов СФ2.

С выхода 1 фотоприемного устройства ФП снимается передаваемый информационный сигнал. Второй выход ФП подсоединен к первому входу время-амплитудного преобразователя ВАП и первому управляющему входу таймера Т. В случае приема символа «1» на втором выходе ФП вырабатывается электрический импульс, который является «стартовым» для ВАП. По переднему фронту импульса запускается работа ВАП и таймера Т.

Выход счетчика фотонов СФ2 подключен ко второму управляющему входу таймера Т и через логический элемент «ИЛИ» Л ко второму входу ВАП. При приходе на вход СФ2 контрольного сигнала, на его выходе создается электрический импульс, который останавливает работу ВАП и таймера Т. Остановка работы происходит по переднему фронту этого импульса. В результате чего на выходе ВАП формируется электрический импульс с амплитудой, прямо пропорциональной времени задержки между появлением импульсов на его первом и втором входах.

Выход ВАП соединен со входом амплитудного анализатора АА. Анализатор сравнивает амплитуду импульса напряжения U, поступившего на его вход с ВАП, с некоторым заданным значением напряжения $U_з$. Если выполняется соотношение $U > U_з$, то на выходе анализатора появляется уровень напряжения, соответствующий логической единице, что свидетельствует о наличии несанкционированного пользователя, подключенного к оптическому волокну ОВ. В противном случае на выходе АА присутствует уровень напряжения, соответствующий логическому нулю.

В случае если счетчик фотонов СФ не зарегистрирует контрольный сигнал, то таймер Т через некоторый интервал времени $t >> \tau$ формирует импульс, который через логический элемент Л поступит на второй вход ВАП и останавливает его работу.

При приеме ключа шифрования подсчитывают число N зарегистрированных контрольных сигналов за некоторый временной интервал. Выполняется сравнение N с некоторым заранее заданным значением N_n. Если $N<N_n$, то делается вывод о наличии несанкционированного пользователя, подключенного к оптическому волокну ОВ.

В случае обнаружения наличия подключения несанкционированного пользователя к оптическому волокну, находящемуся между устройствами А1 и В, ключ шифрования может быть передан через другие устройства. Как было отмечено выше, например, в устройство А1 ключ шифрования может быть передан от устройства А2. Для этого оптическое волокно, соединяющее устройства А1 и А2 подключено к разветвителю Р (см. рис.2). Во время передачи ключа шифрования между указанными устройствами также проверяется наличие несанкционированного подключения к волокну. При обнаружении подключения несанкционированного пользователя к оптическому волокну, находящемуся между устройствами А1 и А2, ключ шифрования может быть передан через устройство А8. Для этого оптическое волокно, соединяющее устройства А1 и А8, подключено к разветвителю Р (см. рис.2). При передаче ключа шифрования в этом случае также осуществляется контроль отсутствия подключения несанкционированного пользователя к оптическому волокну, находящемуся между устройствами А1 и А8. При обнаружении подключения злоумышленника передача ключа прекращается.

Отметим, что принцип обнаружения несанкционированного пользователя между всеми устройствами соответствует описанному при передаче информационного сигнала между А1 и В.

Исследование параметров обнаружения несанкционированного пользователя

Определим физические ограничения возможности обнаружить несанкционированного пользователя описанной выше системы. Для этого оценим влияние длины оптического волокна на возможность реализации квантовой системы с описанным выше принципом обнаружения несанкционированного пользователя, а также определим минимальное время обнаружения несанкционированного подключения к оптическому волокну.

В качестве объектов исследования выбрано оптическое волокно PANDA, сохраняющее поляризацию, и кремниевые лавинные фотодиоды промышленного серийного изготовления ФД-115Л. Для передачи информационного и контрольного сигналов использовалась длина волны оптического излучения 850 нм. Отметим, что лавинный фотодиод использовался в качестве приемника оптического излучения в счетчиках фотонов СФ1 и СФ2 (см. рис.2).

Реализация описанного выше принципа защиты реализуется в устройстве В (рис. 2) путем формирования задержки 1 нс между информационным и контрольным сигналами. Значение временной задержки выбрано с учетом выполненной в работе [9] оценки погрешности измерения времени задержки между информационным и контрольным сигналами $\Delta\tau$, которая для лавинных фотодиодов *ФД-115Л составляет 0,1 нс.* Длительность информационного сигнала составляла 100 нс. Мощность информационного сигнала на входе оптической линии связи была выбрана $2{,}4\cdot10^{-10}$ Вт, что соответствует условиям вывода фотона из оптического волокна путем формирования неоднородности, которая с вероятностью P_n = 0,01 и более обеспечивает этот вывод. Мощность контрольного сигнала ослаблялась до такой степени, чтобы он содержал в среднем один фотон на импульс.

На рис. 3 представлена зависимость вероятности не зарегистрировать контрольный сигнал P_0 на выходе оптического волокна от его длины l. При выполнении оценки учитывались влияние затухания и деполяризации оптического излучения в волокне, величина квантовой эффективности регистрации счетчика фотонов. Под квантовой эффективностью понимается вероятность события, что единичный фотон оптического излучения будет зарегистрирован при его поступлении на вход счетчика фотонов. Отметим, что квантовая эффективность регистрации счетчика фотонов в основном зависит от типа использованного в нем фотоприемника и температуры T, при которой фотоприемник эксплуатируется [9].

Как видно из полученных зависимостей (рис. 3), увеличение длины оптического волокна приводит к росту вероятности P_0. При длине оптического волокна свыше 6000 м для всех исследуемых значений температуры T вероятность P_0 близка к единице. С увеличением длины волокна увеличивается затухание оптического излучения, и, соответственно, растет P_0.

Понижение температуры T приводит к уменьшению вероятности P_0. Это связано с тем, что с понижением температуры T увеличивается квантовая эффективность регистрации. Так, для температуры T = 300 К квантовая эффективность регистрации составляет η =0,03, а для температур T = 250 К и T = 170 К ее значения равняются 0,1 и 0,25, соответственно.

Далее будем рассматривать случай, когда длина оптического волокна обеспечивает затухание интенсивности оптического излучения на его выходе не более, чем в e раз при температуре T = 300 К. Соответственно, длина оптического волокна не должна превышать 1500 м.

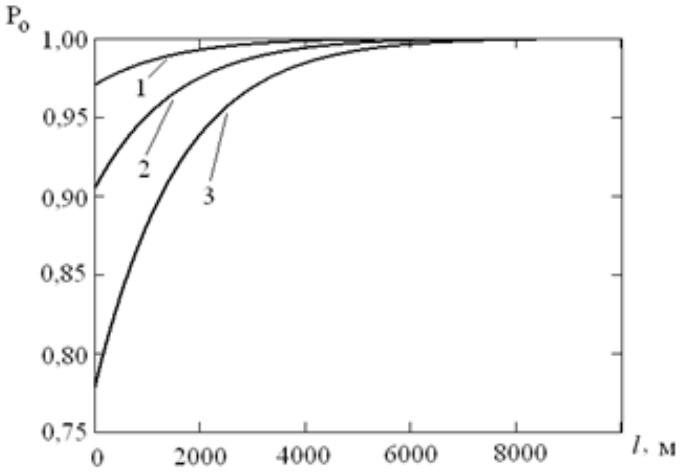

Рис.3. Зависимости вероятности не зарегистрировать контрольный сигнал на выходе оптического волокна от его длины.
1- температура эксплуатации фотоприемника Т = 300 К; 2 – Т = 250 К; 3 – Т = 170 К.

Для указанного интервала возможных значений длины оптического волокна выполнена оценка минимального времени обнаружения потери контрольного сигнала t_o, что соответствует P_n = 0,01. Полученные данные приведены в таблице. В таблице 1 приведены также значения скорости счета темновых импульсов (импульсы, которые формируются в лавинном фотоприемнике в отсутствие поступающего на него оптического излучения). Темновые импульсы приводят к ошибке в регистрации оптического излучения, а также к увеличению времени обнаружения потери контрольного сигнала t_o.

Таблица 1

Характеристики системы, реализующей квантовый метод распределения ключей

Скорость счета темновых импульсов, c^{-1}	Вероятность потерь P_n	Температура, К	Квантовая эффективность регистрации лавинного фотодиода	Длина оптического волокна l, м	Время обнаружения t_o, с
10^3	0,01	300	0,03	100	1,45
				1500	5,80
10^2		250	0,10	100	0,43
				1500	1,75
10		170	0,25	100	0,18
				1500	0,20

Результаты эксперимента показывают, что увеличение длины оптического волокна и уменьшение квантовой эффективности регистрации фотоприемников приводит к увеличению времени обнаружения злоумышленника.

Заключение

Предложен квантовый метод распределения ключей шифрования в системах, использующих в качестве среды передачи оптоволоконные линии. При этом безопасность передачи ключей обеспечивается путем своевременного обнаружения несанкционированного пользователя, подключенного к оптическому волокну, посредством оценки изменения параметров контрольного сигнала. Приведена структурная схема квантовой системы, реализующей предложенный метод, которая позволяет выполнить безопасную передачу ключа шифрования даже в условиях обнаружения подключения несанкционированного пользователя к одному из оптических волокон данной системы.

Определено влияние параметров фотоприемников, длины оптического волокна на время обнаружения несанкционированного пользователя, которые необходимо учитывать при создании квантовых систем связи, реализующих надежное обнаружение подслушивающего злоумышленника.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор № Т16К-006). Публикация содержит результаты исследований, проведенных при грантовой поддержке Государственного фонда фундаментальных исследований Украины по конкурсному проекту Ф73/49-2017.

Список использованной литературы

1. Бернет С. Криптография. Официальное руководство RSA Security / Бернет С., Пейн С. – М.: ООО «Бином-Пресс», 2007, 384 с.

2. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / С.П. Кулик, Е.А. Шапиро (пер. с англ.); С.П. Кулик, Т.А. Шмаонов (ред. пер.); Д. Боумейстер и др. (ред.). – М.: Постмаркет, 2002. – С. 33–73.

3. Килин С.Я. Квантовая криптография: идеи и практика / С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев; под ред. С.Я. Килина. – Минск: Бел. наука, 2007. – 391 с.

4. Барановский О.К. Обнаружение несанкционированного доступа при передаче информации по оптическому волокну / О.К. Барановский, А.О. Зеневич, А.Г. Косари, Е.В. Василиу // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2015. – № 2 (51). – С. 212–216.

5. Криптология: учебник / Ю. С. Харин [и др.]. – Мн., 2013.

6. Барановский О.К. Использование одноквантовых лавинных фотоприемников для создания кантовых генераторов случайных чисел / О.К. Барановский, О.Ю. Горбадей, А.О. Зеневич // Материалы XXI Междунар. науч.-техн. конф., 20 – 21 окт. 2016 года, Минск, Респ. Беларусь; редкол.: А. О. Зеневич [и др.]. – Минск: Белорусская государственная академия связи, 2016. – С. 225–226.

7. Дмитриев А.Л. Оптические системы передачи информации: Учебное пособие / Дмитриев А.Л. – СПб: СПбГУИТМО, 2007. – С. 54-57.

8. Гулаков И.Р. Фотоприемники квантовых систем: монография / Гулаков И.Р., Зеневич А.О. – Мн., 2012.

9. Зеневич А.О. Обнаружение несанкционированного доступа при передаче данных по волоконно-оптическим линиям связи / А.О. Зеневич // Веснік сувязі . – 2014. – № 5 (127). – С. 33–37.

Надійшла 03.01.2017 р. Рецензент: д.т.н., проф. Толубко В.Б.