© Baranovsky O., Gulakov I., Vasiliu Ye., Zenevich A., Limar I. Multichannel quantum system of fiber-optics secure communication // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 2, p. 156-162.

МНОГОКАНАЛЬНАЯ КВАНТОВАЯ СИСТЕМА ВОЛОКОННО-ОПТИЧЕСКОЙ БЕЗОПАСНОЙ СВЯЗИ

Олег Барановский[1], Иван Гулаков[1], Евгений Василиу[2], Андрей Зеневич[1], Игорь Лимарь[2]

[1]Учреждение образования «Белорусская государственная академия связи», Республика Беларусь
[2]Одесская национальная академия связи им. А.С. Попова, Украина

БАРАНОВСКИЙ Олег Константинович, к. ф.-м. н.

Год и место рождения: 1976, г. Гродно, Республика Беларусь.
Образование: Учреждение образования «Белорусский государственный университет».
Должность: проректор по научной работе учреждения образования «Белорусская государственная академия связи» с 2015 года.
Научные интересы: шумовые процессы в электронных приборах, методы и средства зашиты информации.
Публикации: больше 70 научных публикаций, среди которых 25 научных статей.
E-mail: o.baranovskiy@bsac.by

ГУЛАКОВ Иван Романович, д. ф.-м. н.

Год и место рождения: 1946, д. Костеничи, Мглинский р-н, Брянская обл., РФ.
Образование: Учреждение образования «Высший государственный колледж связи».
Должность: профессор кафедры математики и физики с 2006 года.
Научные интересы: фотоэлектронные процессы в фотоприемниках при одноквантовой регистрации, методы и техника регистрации сверхслабых оптических потоков.
Публикации: больше 150 научных публикаций, среди которых монографии, учебные пособия, научные статьи, патенты на изобретения.
E-mail: gulakov@bsu.by

ВАСИЛИУ Евгений Викторович, д. т. н.

Год и место рождения: 1966, Ялта, Крым, Украина.
Образование: Одесский государственный университет имени И.И. Мечникова, 1990.
Должность: директор Учебно-научного института «Радио, телевидения и информационной безопасности» Одесской национальной академии связи им. А.С. Попова с 2013 года.
Научные интересы: квантовая криптография, квантовые протоколы распределения ключей, квантовые протоколы прямой безопасной связи, квантовые протоколы разделения секрета, квантовая стеганография.
Публикации: более 100 научных публикация, среди которых 5 монографий, более 60 научных статей, материалы конференций, патенты.
E-mail: vasiliu@ua.fm

ЗЕНЕВИЧ Андрей Олегович, д. т. н.

Год и место рождения: 1969, г. Минск, Республика Беларусь.
Образование: Учреждение образования «Высший государственный колледж связи».
Должность: ректор учреждения образования «Белорусская государственная академия связи» с 2009 года.
Научные интересы: фотоэлектронные процессы в фотоприемниках при одноквантовой регистрации, методы и техника регистрации сверхслабых оптических потоков.
Публикации: больше 70 научных публикаций, среди которых монография, учебные пособия, научные статьи, патенты на изобретения.
E-mail: a.zenevich@bsac.by

ЛИМАРЬ Игорь Валерьевич

Год и место рождения: 1973, Одесса, Украина.
Образование: Одесская государственная академия холода, 1995, Одесский национальный университет имени И.И. Мечникова, 2010.
Должность: аспирант Одесской национальной академии связи им. А.С. Попова.
Научные интересы: квантовая криптография, квантовые протоколы разделения секрета, квантовое битовое обязательство.
Публикации: 10 научных публикаций, среди которых 6 научных статей, 4 материала конференций.
E-mail: limar.i@onat.edu.ua

Аннотация. *Разработаны способ и схема многоканальной квантовой системы безопасной связи для передачи конфиденциальной информации по оптическому волокну. Рассматриваемая схема сочетает в себе квантовое распределение ключей и квантовую безопасную передачу данных. Такой подход не дает возможности подслушивающему агенту расшифровать ту часть информации, которую он может получить до своего обнаружения. Предложенная схема обеспечивает более высокий уровень защиты передаваемой конфиденциальной информации, чем известные, которые используют традиционные протоколы симметричного шифрования в сочетании с квантовым распределением ключей. В ходе исследования установлено, что для защищенной таким образом передачи по оптическому волокну оптимальным является выбор длин волн 850 и 1625 нм. Определено, что при использовании в таких системах лавинного фотодиода ФД-115Л можно обеспечить скорость передачи информации до 0,8 Мбит/с в одном канале. Для увеличения скорости передачи предложено использовать два и более каналов передачи.*

Ключевые слова: *квантовое распределение ключей, многоканальная квантовая система безопасной связи, оптическое волокно, обнаружение несанкционированного доступа, лавинный фотодиод.*

Введение

В современных системах волоконно-оптической связи достигаются скорости передачи информации (СПИ) до 10 Тбит/с. Для обеспечения конфиденциальности передаваемой информации по волоконно-оптическим линиям связи все чаще используются методы квантовой криптографии, которые обеспечивают высокую, вплоть до абсолютной, степень защиты информации [1-3]. Однако квантово-криптографические системы в режиме распределения ключей обладают низкой СПИ из-за несовершенства используемого оборудования и сложной процедуры обмена данными: несколько Мбит/с на расстояниях до 50 км, десятки Кбит/с и меньше на расстояниях свыше 100 км [4, 5].

В данной работе предлагается новый подход к защите информации, передаваемой в оптоволоконных линиях связи. Для защиты информации в системах квантовой безопасной связи используется квантово-механический ресурс, при этом каждый бит информации кодируется состоянием фотона. При попытке несанкционированного считывания информации происходит изменение состояния фотона, что обнаруживается авторизованными в системе пользователями. Такие системы позволяют обеспечить степень защищенности передаваемой информации, как и в квантовых системах распределения ключей, при этом в определенных случаях позволяя повысить СПИ. В связи с этим для увеличения СПИ таких систем связи предлагается использовать многоканальный подход, реализация которого применительно к квантовым системам связи не рассматривалась детально в литературе до настоящего времени.

Для обнаружения несанкционированного пользователя в системах квантовой безопасной связи требуется некоторый промежуток времени [6]. За этот промежуток времени некоторая часть передаваемой информации может стать известна несанкционированному пользователю. Одним из способов решения этой проблемы является шифрование передаваемых данных с помощью ключа, сформированного в указанной системе квантовой связи в режиме квантового распределения ключа. Такая система, сочетающая квантовое распределение ключей с квантовой системой безопасной связи, передающей непосредственно конфиденциальные данные, будет обладать более высоким уровнем безопасности, чем традиционные системы, используемые в настоящее время. В традиционных системах, например [7, 8], квантовое распределение ключей сочетается с обычной системой симметричного шифрования, что обеспечивает высокий уровень безопасности, однако несанкционированный пользователь может быть надежно обнаружен только в системе квантового распределения ключа.

Квантовая система безопасной связи позволит обеспечить обнаружение несанкционированного пользователя при передаче конфиденциальных данных, что, в свою очередь, сделает возможным немедленно прервать передачу после его обнаружения. С другой стороны, использование шифрования данных обеспечивает их защиту до того момента, когда несанкционированный пользователь будет обнаружен.

Целью данной работы является разработка многоканальной квантовой системы безопасной связи для передачи конфиденциальной информации по оптическому волокну, позволяющей повысить уровень защищенности и скорость передачи информации.

Описание принципа работы устройства
Структурная схема устройства, реализующего мно-

гоканальную квантовую безопасную связь для передачи конфиденциальной информации по оптическому волокну, представлена на рис. 1.

Работа устройства подразделяется на два цикла. Первый цикл заключается в передаче секретного ключа от одного санкционированного пользователя (Алисы) к другому санкционированному пользователю (Бобу). Второй цикл заключается в передаче данных от Алисы к Бобу. Во время передачи секретного ключа и данных осуществляется проверка на наличие несанкционированного пользователя (Евы), подключенного к оптическому волокну.

В первом цикле работы устройства для передачи секретного ключа используется квантовый протокол распределения ключа B92, в котором для генерирования ключа применяются два неортогональных состояния фотона [9]. В качестве таких состояний используются фотоны с углами поляризации 0^0 и 45^0. При этом фотоны, поляризованные под углом 0^0, применяются для передачи двоичного символа «0», а фотоны, поляризованные под углом 45^0, – для передачи двоичного символа «1» [9].

Для увеличения скорости передачи секретного ключа предлагается использовать различные длины волн оптического излучения. Это позволяет единовременно формировать количество бит секретного ключа, равное числу длин волн излучения, передаваемых одновременно по оптическому волокну. В соответствии с рис. 1, схема установки использует оптическое излучение двух длин волн λ_1 и λ_2. Для последующего увеличения СПИ необходимо использовать дополнительное количество источников и приемников оптического излучения, соответствующих числу добавляемых длин волн. Принципы формирования состояний фотонов и их регистрации для различных длин волн необходимо использовать те же.

Процедура распределения ключа по протоколу B92 включает все стандартные элементы стека протоколов квантового распределения ключей: передача неортогональных состояний Алисой; их измерения Бобом; сообщение от Боба к Алисе, какие по порядку фотоны им были приняты; оценка уровня ошибок после завершения передачи с целью обнаружения несанкционированного доступа; исправление ошибок и усиление секретности, если уровень ошибок не превышает некоторого порогового значения [1].

Распределение ключа производится до тех пор, пока его длина не будет удовлетворять необходимым параметрам безопасности. Легитимные (авторизированные в системе) пользователи должны оценить максимальное время обнаружения несанкционированного пользователя в зависимости от настроек и параметров их аппаратуры. Так, в работе [6] получено максимальное время обнаружения 150 мкс (минимальное – 20 мкс). Далее легитимные пользователи вычисляют количество информации, которое может быть перехвачено несанкционированным пользователем за это время и, зная параметры безопасности используемой системы симметричного шифрования, получают минимальную длину ключа, при которой в случае перехвата зашифрованных данных их невозможно расшифровать за приемлемое время. Поскольку при используемом способе обнаружения несанкционированного пользователя количество перехватываемой информации будет невелико, можно использовать шифрование в режиме одноразового блокнота, обеспечивающего безусловную стойкость. Тогда длина ключа, который нужно распределить по протоколу B92, должна быть равна длине передаваемого сообщения.

После передачи и формирования секретного ключа начинается второй цикл работы устройства, связанный с передачей данных.

При передаче символа «1» от Алисы к Бобу направляется однофотонный импульс. В случае передачи символа «0» оптическое излучение от Алисы к Бобу не передается. Для формирования однофотонных импульсов используется способ ослабления оптического излучения при помощи нейтрального светофильтра, описанный в работе [2].

Установление факта подключения Евы к оптическому волокну осуществляется по увеличению ошибки регистрации при передаче данных или (и) по изменению времени задержки между регистрацией двух символов «1», передаваемых на различных длинах волн λ_1 и λ_2.

Если Ева для перехвата информации использует пассивный или активный метод съема данных [10], то это приведет к частичной или полной потере мощности оптического излучения, используемого для передачи символа «1», что в свою очередь приведет к увеличению числа ошибок регистрации. Рост числа ошибочных регистраций будет свидетельствовать о наличии подключения Евы к оптическому волокну.

В случае, когда Ева использует компенсационный метод съема данных [10], то число ошибочных регистраций может не измениться. Для обнаружения подключения Евы в этом случае выполняется измерение временной задержки между моментами времени регистрации символов «1», передаваемых на длинах волн λ_1 и λ_2. Оптическое волокно обладает дисперсией, а это значит, что фотоны с длинами волн λ_1 и λ_2 распространяются в нем с различными скоростями. Следовательно, при одновременном входе двух фотонов с длинами волн λ_1 и λ_2 в оптическое волокно они будут регистрироваться на его выходе с некоторой временной задержкой τ, зависящей от длины волокна. Временная задержка τ для оптического волокна измеряется до его установки в устройство. После установки волокна в устройство и при передаче данных выполняется измерение времени задержки τ_0 на выходе оптического волокна между двумя одновременно испущенными фотонами с длинами волн λ_1 и λ_2, используемыми для передачи символов «1». Затем сравнивают между собой величины τ и τ_0 и, если эти величины не совпадают, то делают вывод о наличии подключения Евы к оптическому волокну.

При обнаружении подключения Евы к оптическому волокну передачу данных прекращают.

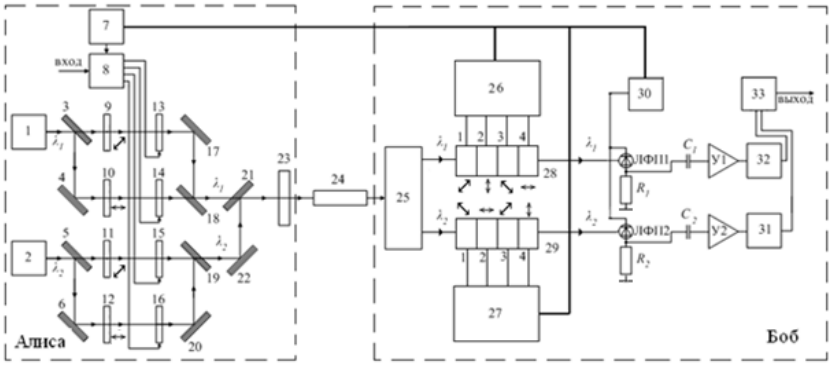

Рис. 1. Структурная схема устройства

Описание циклов работы устройства

Первый цикл, заключающийся в формировании секретного ключа, реализуется следующим образом. Источник излучения 1 генерирует непрерывное оптическое излучение с длиной волны λ_1. Источник излучения 2 генерирует непрерывное оптическое излучение с длиной волны λ_2. Оптическое излучение от источников излучения 1 и 2 до попадания в оптическое волокно 24, проходит через набор полупрозрачных и отражающих зеркал 3−6, 17–22, набор поляризаторов 9–12 и модуляторов 13–16. Полупрозрачное зеркало 3 и отражающее зеркало 4 обеспечивают разделение оптического излучения с длиной волны λ_1 на два луча, которые с помощью поляризаторов 9 и 10 линейно поляризуются под углами 45° и 0° соответственно. Полупрозрачное зеркало 5 и отражающее зеркало 6 обеспечивают разделение оптического излучения с длиной волны λ_2 на два луча, которые с помощью поляризаторов 11 и 12 линейно поляризуются под углами 45^0 и 0^0.

Затем сформированные лучи последовательно модулируются при помощи модуляторов 13−16 и объединяются с помощью полупрозрачных и отражающих зеркал 17−22, ослабляются нейтральным светофильтром 23 и направляются в оптическую линию связи 24 (рис. 1). Работой модуляторов управляет генератор случайных чисел 8. Он подает управляющие сигналы одновременно на один из модуляторов 9 или 10 и на один из модуляторов 11 или 12. Выбор модуляторов 9 или 10, 11 или 12 происходит случайным образом. При поступлении сигнала на управляющий вход модулятора, он пропускает через себя оптическое излучение. В отсутствие сигнала на управляющем входе модуляторов они не пропускают через себя оптическое излучение. Поэтому, при поступлении управляющих сигналов от генератора 8 только один из лучей, исходящих от источников 1 и 2 направляется в оптическое волокно. Также необходимо отметить, что в оптическое волокно поступает оптическое излучение только с одной случайно выбранной поляризацией 0^0 или 45^0 от источников 1 и 2.

Отметим, что коэффициенты поглощения и отражения зеркал 3−6, 17−22 необходимо подбирать такими, чтобы интенсивность оптических лучей, поступающих в оптическое волокно 24, была одинаковой.

На приемной стороне оптическое излучение, поступившее из оптического волокна 24, разделяется на два луча в зависимости от длины волны излучения. Для этого оптическое излучение вначале подается на мультиплексор 25, который разделяет оптическое излучение на два луча, один из которых имеет длину волны λ_1, а второй – λ_2. Затем каждый из этих лучей с длинами волн λ_1 иλ_2 подается на набор ячеек Поккельса 28 и 29 соответственно.

Работой ячеек Поккельса 28 и 29 управляют генераторы случайных чисел 26 и 27 соответственно. Генераторы 26 и 27 случайным образом подают электрический импульс на один из четырех входов набора ячеек Поккельса. Это происходит в момент времени, когда на входах генераторов 28 и 29 присутствует сигнал от блока синхронизации 7. В результате чего через набор ячеек Поккельса может проходить оптическое излучение без изменения интенсивности только с одним из четырех видов линейной поляризации фотонов: 0^0, 45^0, 90^0 или 135^0, в зависимости от того, на какой из управляющих входов набора ячеек Поккельса поступил электрический импульс. Стоит отметить, что оптическое излучение с линейной поляризацией фотонов, ортогональной плоскости поляризации ячейки Поккельса, не проходит через эти ячейки.

Фотоны с выходов наборов ячеек Поккельса 28 и 29 поступают на лавинные фотоприемники ЛФП1 и ЛФП2 соответственно. Лавинные фотоприемники работают в режиме счета фотонов.

При работе устройства осуществляется синхронизация моментов времени передачи и приема битов информации для формирования секретного ключа, а также обеспечение согласованной работы источников излучения и лавинных фотоприемников. Эта синхронная работа обеспечивается при помощи блока синхронизации 7, который одновременно подает синхросигнал на входы генератора 8 и источника питания лавинных фотоприемников 30, а также генераторов случайных чисел 26 и 27.

При отсутствии на выходе блока 7 импульса синхронизации, оптическое излучение в оптическое волокно не поступает. При этом, источник напряжения питания 30 обеспечивает напряжение обратного смещения ЛФП, равное приблизительно 99% от уровня напряжения лавинного пробоя. Значение напряжения обратного смещения ЛФП, меньшее напряжения пробоя, не позволяет фотоприемникам работать в режиме счета фотонов.

По сигналу от блока синхронизации 7 в виде прямоугольного строба импульса источник питания 30 увеличивает напряжение смещения ЛФП до значений, превышающих напряжение их лавинного пробоя, переводя тем самым эти фотоприемники в режим одноквантовой регистрации. Длительность такого превышения совпадает с длительностью импульса синхронизации. В течение этого времени при регистрации фотона ЛФП на нагрузочных резисторах R_1 и R_2 формируются одноквантовые импульсы напряжения, поступающие через разделительные конденсаторы C_1 и C_2 на входы усилителей У1 и У2. После усиления импульсы подаются на входы амплитудных дискриминаторов 32 и 31, выделяющих одноквантовые импульсы на фоне собственных шумов усилителей и отделяющих импульсы помех, которые могут возникнуть в результате прохождения импульса стробирования через собственную емкость ЛФП и емкость разделительных конденсаторов C_1 и C_2.

На выходе дискриминаторов 32 и 31 одноквантовые импульсы напряжения нормируются по амплитуде и длительности. Выходы дискриминаторов 32 и 31 являются первым и вторым выходами устройства соответственно.

Далее формирование секретного ключа осуществляется по протоколу B92 [9]. Сформированный ключ используется для шифрования данных Алисой перед их передачей и дешифрования Бобом после получения.

Второй цикл работы заключается в передаче зашифрованных данных по оптическому волокну от Алисы к Бобу. В этом случае входная последовательность данных поступает на вход генератора 8. При этом при передаче символа «1» управляющие импульсы поступают только на модуляторы 14 и 15. Модуляторы 13 и 16 в цикле передачи данных оптическое излучение через себя не пропускают.

Оптическое излучение от источника излучения 1 до оптического волокна 24 проходит через набор полупрозрачных и отражающих зеркал 3, 4, 18, 21, поляризатор 10, модулятор 14 и ослабляющий нейтральный светофильтр 23. Оптическое излучение от источника излучения 2 до оптического волокна 24 проходит через набор полупрозрачных и отражающих зеркал 5,19, 22, 21, поляризатор 11, модулятор 15 и ослабляющий нейтральный светофильтр 23.

Оптическое излучение с выхода оптического волокна 24 подается на мультиплексор 25, который разделяет оптическое излучение на два луча, один из которых имеет длину волны λ_1, а второй – λ_2. Затем каждый из этих лучей с длинами волн λ_1 иλ_2 подается на набор ячеек Поккельса 28 и 29 соответственно. При передаче данных блокируется работа генераторов 26 и 27: управляющие сигналы от генераторов 26 и 27 на ячейки Поккельса не поступают. Поэтому оптическое излучение с длинами волн λ_1 и λ_2 беспрепятственно проходит через набор ячеек Поккельса. С выхода набора ячеек Поккельса 28 и 29 оптическое излучение с длинами волн λ_1 иλ_2 поступает на лавинные фотоприемники ЛФП1 и ЛФП2 соответственно.

Лавинные фотоприемники ЛФП1 и ЛФП2 регистрируют фотоны при поступлении стробирующих импульсов на вход источника питания 30. После усиления усилителями У1 и У2 импульсы подаются на входы амплитудных дискриминаторов 32 и 31. С выходов дискриминаторов 32 и 31 импульсы поступают на первый и второй входы блока сравнения 33 соответственно. Блок 33 осуществляет измерение задержки τ_0 между импульсами, поступившими с дискриминаторов 32 и 31. Если эта задержка τ_0 не совпадает с некоторой заранее заданной величиной τ, то на выходе блока 33 появляется сигнал тревоги. Сигнал тревоги означает, что к оптическому волокну подключен несанкционированный пользователь Ева. Также наличие Евы определяется по достижению уровнем битовых ошибок передачи данных некоторого порогового значения.

Экспериментальные результаты и их обсуждение

Для определения длин волн, которые необходимо использовать при передаче данных, выполнены исследования зависимости отношения $\Delta P_{pot}/\Delta D$ от длины волны оптического излучения (ΔP_{pot} – изменения вероятности потери оптического сигнала в оптическом волокне, ΔD – изменение диаметра макроизгиба), представленные на рис. 2. Измерения проводились для серийно выпускаемого оптического волокна G.652.

Исследования проведены в диапазоне длин волн от 850 до 1650 нм, позволяющем организовать передачу данных в оптическом волокне типа G.652.

Для оценки влияния макроизгиба измерения выполнены при ΔD = 55 мм, так как при D<5 мм высока вероятность излома оптического волокна. Измерения показали, что для наиболее часто используемых для передачи информации по оптическому волокну длин волн 850 нм, 1310 нм, 1490 нм, 1550 нм при D > 60 мм потери оптического сигнала в волокне практически не зависят от диаметра макроизгиба $P_{pot}(D)$ [11]. Исключение составляет длина волны 1625 нм. Наибольшие значения величины $\Delta P_{pot}/\Delta D$ соответствовало, среди этих длин волн, длине волны 1625 нм, а наименьшее – 850 нм. Поэтому, далее мы будет использовать эти длины волн, несмотря на то, что на этих длинах волн наблюдается большее затухания по сравнению с другими длинами волн. Это связано с тем, что именно такие длины волн позволяют обеспечить наилучшую безопасность передаваемой конфиденциальной информации, поскольку для вывода оптического излучения с длиной волны 850 нм из волокна Еве нужно сформировать макроизгиб диаметра ≥20 мм, который хорошо диагностируется на длине волны 1625 нм. Диагностирование макроизгиба на длине волны 1625 нм осуществляется по увеличению P_{pot} более чем на 50 %. Также одновременно испущенные фотоны с этими длинами волн после распространения по оптическому волокну имеют наибольшую временную задержку τ между собой. Временная задержка между этими фотонами при длине оптического волокна 1 км составляла 45±0,5 нс.

Для регистрации оптического излучения с длиной волны 850 нм использовались кремниевые

лавинные фотодиоды ФД-115Л, а для регистрации излучения с длиной волны 1625 нм применялись германиевые лавинные фотодиоды ЛФД-2 [12]. Германиевые фотодиоды имеют меньшее мертвое время регистрации и лучшее быстродействие по сравнению с кремниевыми фотодиодами. Поэтому оценку пропускной способности проводили для оптического канала, в котором в качестве приемника оптического излучения использовался кремниевый лавинный фотодиод ФД-115Л.

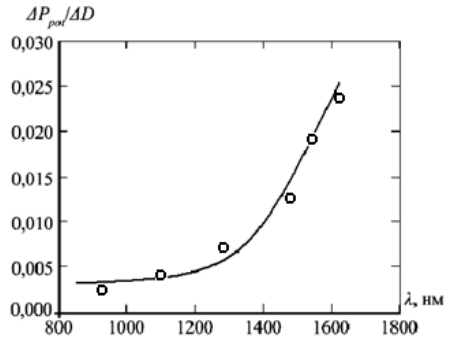

Рис. 2. Зависимость отношения $\Delta P_{pol}/\Delta D$ от длины волны оптического излучения

Зависимости величины пропускной способности одного оптического канала C_u от длительности импульсов стробирования Δt и времени передачи одного бита информации τ_b представлены на рисунках 3 и 4, соответственно.

Величина C_u определялась для периода следования импульсов стробирования 10 мкс. При этом длительность импульса стробирования изменялась в пределах 0,1 ÷ 1,0 мкс. Такой выбор связан с тем, чтобы за время следования импульса стробирования вероятность регистрации двух одноквантовых импульсов была достаточно мала.

В результате исследований установлено, что скорость передачи информации C_u достигает максимального значения при длительности импульса стробирования $\Delta t \approx 0{,}8$ мкс (рис. 3).

Максимум скорости передачи информации $C_u \approx 0{,}8$ Мбит/с достигается при значении $\tau_b = 1{,}1$ мкс (рис. 4). При использовании двух каналов, как в описываемой схеме, скорость передачи информации можно увеличить в два раза.

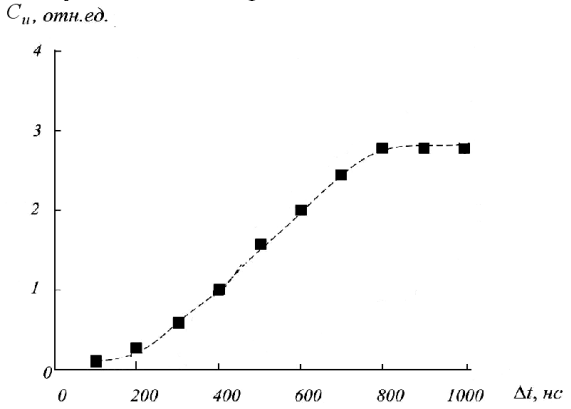

Рис. 3. Зависимость пропускной способности оптического канала связи от длительности импульса стробирования

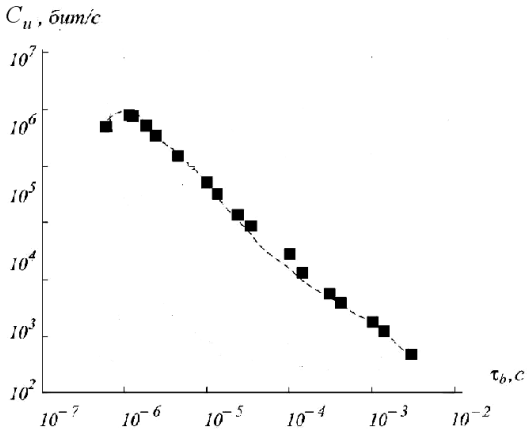

Рис. 4. Зависимость пропускной способности оптического канала связи от времени передачи 1 бита информации

Выводы

Разработан способ и схема многоканальной квантовой системы безопасной связи для передачи конфиденциальной информации по оптическому волокну. Предложенная квантовая система использует квантовый криптографический протокол B92, при этом скорость передачи секретного ключа увеличивается в два раза за счет использования двух длин волн.

На втором этапе работы системы выполняется передача зашифрованной распределенным ключом конфиденциальной информации. При этом благодаря использованию квантовых свойств отдельных фотонов выявляется наличие несанкционированного подключения к оптическому волокну, и в случае обнаружения такого подключения передача данных прекращается. Шифрование передаваемых данных обеспечивает их защиту до того момента, когда несанкционированное подключение будет обнаружено. Предложенная система, сочетающая в себе преимущества квантовых систем распределения ключей и квантовых систем прямой безопасной связи, обеспечивает более высокий уровень защиты передаваемой конфиденциальной информации, чем имеющиеся системы, использующие традиционные протоколы симметричного шифрования в сочетании с квантовым распределением ключей.

В рамках разработанного способа установлено, что для передачи конфиденциальной информации по волоконно-оптическим квантовым линиям связи целесообразно использовать длины волн 850 и 1625 нм, на которых обеспечивается высокая безопасность передачи информации за счет контроля несанкционированного вывода оптического излучения через поверхность оптического волокна. Определено, что при использовании в таких системах лавинного фотодиода ФД-115Л можно обеспечить скорость передачи информации $C_u \approx 0{,}8$ Мбит/с в одном канале. Для увеличения скорости передачи информации предложено использовать два и более каналов передачи.

Література

[1] Gisin N. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Review of Modern Physics. – 2002. – V. 74, issue 1. – P. 145–195.

[2] Килин С.Я. Квантовая криптография: идеи и практика / Килин С.Я., Хорошко Д.Б., Низовцев А.П. – Минск: ИД «Белорусская наука». – 2008. – 392 с.

[3] Korchenko O. Quantum Secure Telecommunication Systems / Korchenko O., Vorobiyenko P., Lutskiy M., Vasiliu Ye., Gnatyuk S. // Telecommunications Networks – Current Status and Future Trends (Ed. by J.H. Ortiz). – InTech, 2012. – P. 211–236.

[4] Dixon A. R. High Speed and Adaptable Error Correction for Megabit/s Rate Quantum Key Distribution / A.R. Dixon, H. Sato. – Nature Publishing Group, November 2, 2014. – P. 23–24.

[5] Lo H.K. Measurement-Device-Independent Quantum Key Distribution / H.K. Lo, M. Curty, B. Qi. – Phys. Rev. Lett. – 2012. – V. 108. – 130503.

[6] Барановский О.К. Обнаружение несанкционированного доступа при передаче информации по оптическому волокну / О.К. Барановский, А.О. Зеневич, А.Г. Косари, Е.В. Василиу // Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». – 2015. – № 2. – С. 212-216.

[7] QPN Security Gateway (QPN–8505) // [Электронный ресурс] http://www.magiqtech.com/Products_files/8505_Data_Sheet.pdf .

[8] Centauris Link Encryption // [Электронный ресурс] http://www.idquantique.com/quantum-safe-crypto/network-encryption/centauris-ethernet-encryption/.

[9] Bennett C.H. Quantum cryptography using any two nonorthogonal states / C.H. Bennett // Physical Review Letters. – 1992. – V. 68, issue 21. – P. 3121–3124.

[9] Манько А. Защита информации на волоконно-оптических линиях связи от несанкционированного доступа / А. Манько, В. Каток, М. Задорожний // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – №2.- С. 249-255.

[10] Гулаков И.Р. Использование одноквантовой регистрации для систем передачи конфиденциальной информации по волоконно-оптическим линиям связи / И.Р. Гулаков, А.О. Зеневич, А.М. Тимофеев, А.Г. Косари // Доклады БГУИР. – 2014. – №7(85). – С. 38-43.

[11] Гулаков И.Р. Метод счета фотонов в оптико-физических измерениях / И.Р. Гулаков, С.В. Холондырев. – Минск: Университетское, 1989. – 256 с.

УДК 004.056.53+530.145+621.383.92 (045)

Барановський О.К., Гулаков І.Р., Василіу Є.В., Зеневич А.О., Лімарь І.В. Багатоканальна квантова система волоконно-оптичного безпечного зв'язку

Анотація. *Розроблено спосіб і схему багатоканальної квантової системи безпечного зв'язку для передачі конфіденційної інформації по оптичному волокну. Розглянута схема поєднує у собі квантовий розподіл ключів і квантову безпечну передачу даних. Такий підхід не дає можливості агентові, що підслуховує, розшифрувати ту частину інформації, яку він може одержати до свого виявлення. Запропонована схема забезпечує більш високий рівень захисту переданої конфіденційної інформації, чим відомі, які використають традиційні протоколи симетричного шифрування в поєднанні із квантовим розподілом ключів. У ході дослідження встановлено, що для захищеної в такий спосіб передачі по оптичному волокну оптимальним є вибір довжин хвиль 850 і 1625 нм. Визначено, що при використанні в таких системах лавинного фотодіода ФД-115Л можна забезпечити швидкість передачі інформації до 0,8 Мбіт/с в одному каналі. Для збільшення швидкості передачі запропоновано використовувати два й більше канали передачі.*

Ключові слова: *квантовий розподіл ключів, багатоканальна квантова система безпечного зв'язку, оптичне волокно, виявлення несанкціонованого доступу, лавинний фотодіод.*

Baranovsky O., Gulakov I., Vasiliu Ye., Zenevich A., Limar I. Multichannel quantum system of fiber-optics secure communication

Abstract. *The method and the scheme of multichannel quantum system of secure communication for transfer of confidential data on optical fiber are developed. The considered scheme combines quantum key distribution with quantum secure data transmission. Such approach does not give possibility to the eavesdropper to decipher that part of information, which he can receive before the detection. The suggested scheme provides higher security level of transferred confidential information, than known, which use traditional protocols of symmetric enciphering in a combination to quantum key distribution. It is found out that for the transmission protected in such a way on optical fiber the choice of wavelengths of 850 and 1625 nanometers is optimum. It is found out that when using in such systems of the avalanche photo diode FD-115L it is possible to provide a speed of information transfer up to 0,8 Mbps in one channel. For increase in speed of transfer, it is proposed to use two and more channels of transfer.*

Key words: *quantum key distribution, multichannel quantum system of secure communication, optical fiber, detection of unauthorized access, avalanche photodiode.*

Отримано *26 квітня 2016 року*, затверджено редколегією *6 травня 2016 року*