УДК 621.383

Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи

Тимофеев А.М.

Белорусский государственный университет информатики и радиоэлектроники,
ул. П. Бровки, 6, г. Минск 220013, Беларусь

Поступила 17.11.2017
Принята к печати 05.02.2018

При передаче информации по волоконно-оптическим каналам связи необходимо обеспечить ее конфиденциальность и определять подлинность источника информации. Абсолютная скрытность информации от доступа третьих лиц, которым она не предназначена, может быть реализована путем использования квантово-криптографических систем, которые предполагают передачу каждого бита при помощи маломощных оптических сигналов, содержащих от десятка до отдельных фотонов излучения, однако характеризуются большим количеством ошибок вследствие эффекта деполяризации оптического излучения. Поэтому цель работы – создать устройство для передачи и приема конфиденциальных данных, которое бы обеспечивало абсолютную скрытность передаваемой информации, присущую квантово-криптографическим системам связи, и вместе с тем имело малое количество таких ошибок.

Предложено устройство для систем квантово-криптографической связи, в котором в качестве приемного модуля использовался счетчик фотонов. Продемонстрирована возможность применения кремниевых лавинных фотоприемников в режиме счета фотонов для систем передачи конфиденциальной информации, определяющих подлинность источника передаваемой информации.

Разработанная система волоконно-оптической связи, содержащая в качестве приемного модуля счетчик фотонов на базе лавинного фотоприемника, позволяет обнаружить несанкционированный доступ к информации и нарушение ее целостности и ускорить процесс обмена информацией, в сравнении с известными квантово-криптографическими системами связи.

Ключевые слова: счетчик фотонов, система конфиденциальной передачи информации, лавинный фотоприемник.

DOI: 10.21122/2220-9506-2018-9-1-17-27

Адрес для переписки:
Тимофеев А.М.
Белорусский государственный университет информатики и радиоэлектроники,
ул. П. Бровки, 6, г. Минск 220013, Беларусь
e-mail: tamvks@mail.ru

Address for correspondence:
Timofeev A.M.
Belarusian State University of Informatics and Radioelectronics,
P. Brovka str., 6, Minsk 220013, Belarus
e-mail: tamvks@mail.ru

Для цитирования:
Тимофеев А.М.
Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи.
Приборы и методы измерений.
2018. – Т. 9, № 1. С. 17–27.
DOI: 10.21122/2220-9506-2018-9-1-17-27

For citation:
Timofeev A.M.
[Device for binary data transmitting and receiving over a fiber-optic communication channel].
Devices and Methods of Measurements.
2018, vol. 9, no. 1, pp. 17–27 (in Russian).
DOI: 10.21122/2220-9506-2018-9-1-17-27

Device for binary data transmitting and receiving over a fiber-optic communication channel

Timofeev A.M.

Belarusian State University of Informatics and Radioelectronics,
P. Brovka str., 6, Minsk 220013, Belarus

Received 17.11.2017
Accepted for publication 05.02.2018

Abstract

When transferring data over optical fiber communication channels, it is required to provide data security and the authenticity of their source. To limit the access to the data for a third party, there can be applied quantum-cryptographical systems which are supposed to transfer every data bit by means of low power optical signals containing radiation photons the number of which could be in the range from 10 to 1, however, are far from being perfect and suffer from shortcomings, the main of which being a large number of errors due to the depolarization effect of optical radiation. The aim of this work was, therefore, to create device for sending and receiving confidential data which could provide complete security of transferred data, inherent to quantum-cryptographical communication systems at the same time could have a low number of such errors.

A device for quantum-cryptographic communication system with a photon counter applied as a receiving module has been proposed. The possibility to use silicon avalanche photodetectors operating in the photon counting mode for confidential information transmission systems and defining authenticity of the source of transmitted information has been shown.

I develop modern optical fiber communication system incorporating avalanche photodetector photon counter as a receiving module, that allow to detect unauthorized access to information and violation of its integrity and speed up the exchange of information in comparison with well-known quantum-cryptographical communication systems.

Keywords: photon counter, confidential information transmission system, avalanche photodetector.

DOI: 10.21122/2220-9506-2018-9-1-17-27

Адрес для переписки:
Тимофеев А.М.
Белорусский государственный университет информатики и радиоэлектроники,
ул. П. Бровки, 6, г. Минск 220013, Беларусь
e-mail: tamvks@mail.ru

Address for correspondence:
Timofeev A.M.
Belarusian State University of Informatics and Radioelectronics,
P. Brovka str., 6, Minsk 220013, Belarus
e-mail: tamvks@mail.ru

Для цитирования:
Тимофеев А.М.
Устройство для передачи и приема двоичных данных по волоконно-оптическому каналу связи.
Приборы и методы измерений.
2018. – Т. 9, № 1. С. 17–27.
DOI: 10.21122/2220-9506-2018-9-1-17-27

For citation:
Timofeev A.M.
[Device for binary data transmitting and receiving over a fiber-optic communication channel].
Devices and Methods of Measurements.
2018, vol. 9, no. 1, pp. 17–27 (in Russian).
DOI: 10.21122/2220-9506-2018-9-1-17-27

Введение

В настоящее время к аппаратно-программным комплексам, используемым для систем защиты информации, предъявляют ряд требований, включая как обеспечение конфиденциальности передаваемой информации, так и определение подлинности их источника [1, 2]. Для выполнения этих требований целесообразно применять криптографические преобразования информации, которые используют шифрование и расшифрование данных, механизмы взаимной идентификации и аутентификации пользователей и данных [1–4]. Однако в силу открытости большинства криптографических алгоритмов их криптостойкость зависит от вычислительных возможностей злоумышленника, что является угрозой информационной безопасности криптосистем. Абсолютную конфиденциальность передаваемой информации обеспечивают системы связи, использующие принципы квантовой криптографии [5]. Такие системы требуют достаточно сложной процедуры согласования базисов, используемых для кодирования передаваемых символов и их приема, и характеризуются появлением большого количества ошибок вследствие эффекта деполяризации оптического излучения в волоконно-оптических линиях связи, что ограничивает область практического применения квантово-криптографических систем связи. В этой связи представляет интерес разработать приемо-передающее устройство для систем квантово-криптографической связи, которое упрощает известные устройства за счет устранения процедуры согласования базисов, в которых переданы и приняты символы, обеспечивает определение подлинности источника передаваемой информации, конфиденциальность данных, а также уменьшает ошибку передачи данных, связанную с деполяризацией оптического излучения.

Сущность функционирования системы связи

Сущность функционирования системы квантово-криптографической связи заключается в том, что на передающей стороне данные, подлежащие передаче, смешивают с идентификационной информацией отправителя, зашифровывают данные и идентификационную информацию отправителя на открытом криптографическом ключе отправителя, кодируют и передают по незащищенному волоконно-оптическому каналу связи на одной длине волны шифртекст при помощи оптических импульсов слабой мощности, которые содержат от одного до нескольких десятков фотонов. На принимающей стороне декодируют оптические импульсы слабой мощности посредством работающего в режиме счета фотонов приемника, расшифровывают полученный шифртекст на секретном ключе получателя, выделяют идентификационную информацию отправителя и определяют подлинность принятых данных и их отправителя.

Формирование предельно слабого оптического излучения осуществляется с помощью источника одиночных фотонов, полученного путем ослабления оптических импульсов. Такие источники позволяют получить направленный поток фотонов на длинах волн, используемых для всех окон прозрачности волоконно-оптических линий связи, и не требуют ультравысокого вакуума, экстремально низких температур и наличия дорогостоящих искусственных кристаллов и лазеров [5].

Для зашифровывания на открытом криптографическом ключе отправителя смеси данных, подлежащих передаче, и идентификационной информации отправителя, а также их последующего расшифровывания на секретном криптографическом ключе получателя могут быть использованы асимметричные алгоритмы, описанные в [3, 4].

Регистрация предельно слабого оптического излучения выполняется с помощью приемного модуля, функционирующего в режиме счета отдельных фотонов. Этот режим регистрации позволяет обеспечить лучшую пороговую чувствительность в сравнении с другими [6]. При этом счетчик фотонов целесообразно выполнять на базе лавинных фотодиодов (ЛФД), т.к. эти фотоприемники имеют высокий квантовый выход, широкий диапазон спектральной чувствительности, включающий окна прозрачности оптического кабеля, низкие напряжения питания, обладают высоким коэффициентом умножения фотоносителей, имеют небольшие габариты (несколько миллиметров в диаметре) и вес (несколько грамм). Следует также отметить, что кремниевые ЛФД позволяют реализовывать режим счета фотонов при комнатных температурах для первого и второго окон прозрачности оптического кабеля и имеют лучшую пороговую чув-

ствительность в сравнении с германиевыми ЛФД и ЛФД на основе соединений галлия [7, 8].

Установление подлинности принятых данных и их отправителя осуществляется на основе схемы непрерывной проверки, описанной в [2–4]. В этой схеме отправителю и получателю сообщаются идентификационная информация отправителя и дополнительные блоки данных для подстановки, которые являются общими для отправителя и получателя данных, поставляются и обновляются в установленном порядке, редко изменяются и сохраняются в секрете.

Информация, хранящая и передающаяся в системе квантово-криптографической связи (данные, подлежащие передаче, идентификационная информация отправителя, криптографические ключи), представляется в виде двоичных кодовых слов, состоящих из символов «0» и «1».

Структурная схема и описание работы приемо-передающего устройства

Квантово-криптографическая система связи содержит два приемо-передающих устройства, одно из которых устанавливается на стороне отправителя данных, второе – на стороне получателя данных. Структурная схема приемо-передающего устройства для систем квантово-криптографической связи представлена на рисунке 1.

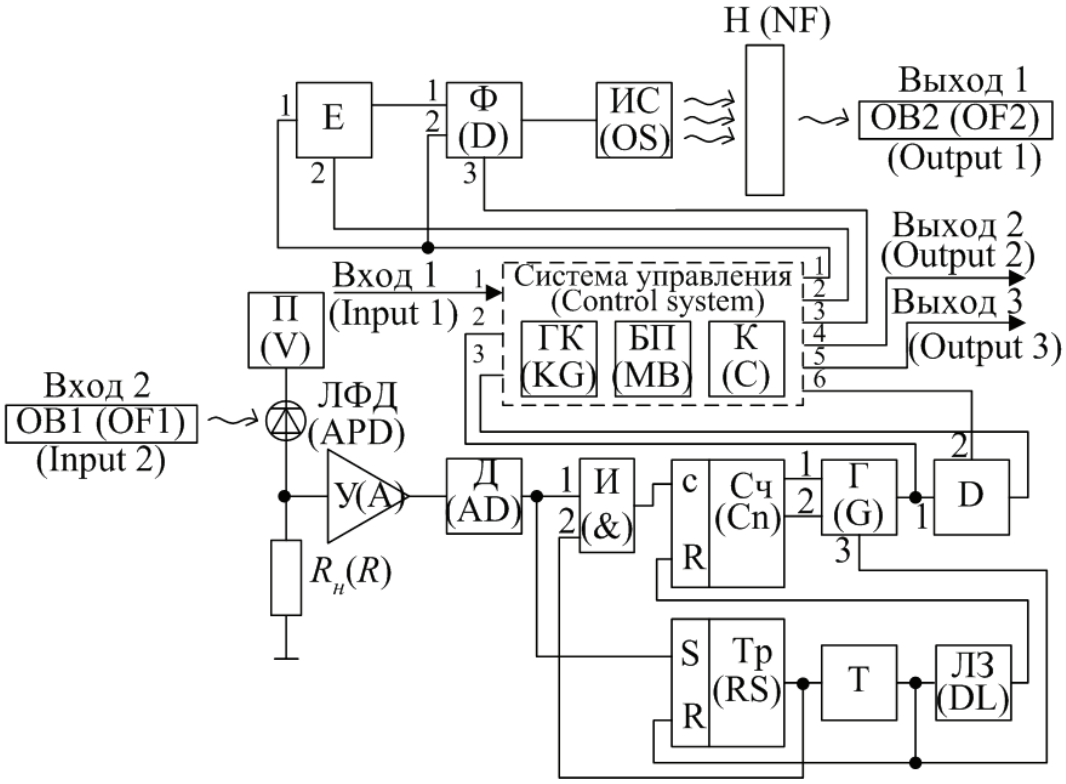

Рисунок 1 – Структурная схема приемо-передающего устройства для систем квантово-криптографической связи: OB1 и OB2 – входное и выходное оптические волокна соответственно; Е и *D* – блоки зашифрования и расшифрования данных соответственно; П – источник постоянного напряжения; ЛФД – лавинный фотодиод; $R_н$ – нагрузочный резистор; У – усилитель; Ф – формирователь данных; Д – амплитудный дискриминатор; ГК – генератор криптографических ключей; И – логический элемент «И»; ИС – источник оптического сигнала; БП – блок памяти; Н – нейтральный светофильтр; К – компаратор; Сч – счетчик импульсов; Тр – *RS*-триггер; Г – генератор прямоугольных импульсов; Т – таймер; ЛЗ – линия задержки

Figure 1 – Structural diagram of the transceiver for cryptographic communication systems: OF1/OF2 – input/output optical fiber; E/D – data encryption/decryption unit; V – constant voltage source; APD – avalanche photodiode; R – resistor; A – amplifier; D – data shaper; AD – amplitude discriminator; KG – cryptographic key generator; & – logical element «AND»; OS – optical signal source; MB – memory block; NF – neutral filter; C – comparator; Cn – pulse counter; RS – RS-trigger; G – square wave generator; T – timer; DL – delay line

Приемо-передающее устройство содержит два входа и три выхода. Первых вход подключен к источнику данных, подлежащих передачи по волоконно-оптическому каналу связи. Второй вход и первый выход устройства соединены соответственно с приемным оптическим волокном ОВ1 и передающим оптическим волокном ОВ2. Второй выход устройства подключен к приемнику данных. Третий выход приемо-передающего устройства является сигнальным и используется для индикации наличия злоумышленника, осуществляющего несанкционированный съем информации, передаваемой по волоконно-оптическому каналу связи, и/или навязывающего ложные данные.

Каждое приемо-передающее устройство содержит систему управления, блоки зашифрования и расшифрования, передающий и приемный модули и работает в четырех режимах: передачи открытого криптографического ключа, приема открытого криптографического ключа, передачи шифртекста и приема шифртекста. Причем при построении квантово-криптографической системы связи необходимо приемо-передающие устройства соединить таким образом, чтобы передающий модуль отправителя через первый выход устройства был подключен ко второму входу приемного модуля устройства получателя. Переключение между режимами работы приемо-передающих устройств осуществляется посредством их систем управления.

На стороне отправителя данных приемо-передающее устройство последовательно работает в режимах приема открытого криптографического ключа и передачи шифртекста.

На стороне получателя данных приемо-передающее устройство последовательно работает в режимах передачи открытого криптографического ключа и приема шифртекста.

До начала передачи данных счетчики импульсов Сч, *RS*-триггеры Тр и внешние выводы систем управления приемо-передающих устройств отправителя и получателя сбрасывают в нулевое состояние и записывают в блоки памяти БП (рисунок 1) блоки данных для подстановки в виде двоичных кодовых слов, которые являются долговременными секретными элементами, общими для отправителя и получателя данных. Блоки памяти БП, а также генераторы ключей ГК и компараторы К реализуются в системах управления, построенных на базе микроконтроллеров *MCS*-51, программистская и схемотехническая модели которых наиболее предпочтительны для осуществления обработки данных, передачи управляющих сигналов и выполнения логических и арифметических операций в режиме реального времени [9].

Количество блоков данных для подстановки равно числу бит идентификационной информации отправителя *IDA*, длина которой, в свою очередь, определяется по аналогии с выбором длины имитовставки[1]. Каждый блок данных для подстановки содержит $(\log 2n + 1)$ двоичных разрядов, где n – количество двоичных разрядов данных, подлежащих передачи по волоконно-оптическому каналу связи. Причем старший бит первого блока данных для подстановки содержит первый бит *IDA*, старший бит второго блока данных для подстановки – второй бит *IDA* и т.д. Остальные биты блоков данных для подстановки образуют кодовые слова, которые используются для определения порядка смешивания данных, подлежащих передачи по волоконно-оптическому каналу связи, и идентификационной информации отправителя *IDA* следующим образом. Кодовое слово первого блока данных для подстановки определяет номер бита данных, подлежащих передачи, после которого подмешивается первый бит *IDA*, кодовое слово второго блока данных для подстановки – второй бит *IDA* и т.д.

Следует отметить, что для выполнения криптографических преобразований информации при формировании шифртекста из смеси данных и идентификационной информации отправителя и последующего обратного преобразования информации при выделении из шифртекста смеси данных и идентификационной информации отправителя целесообразно применять в качестве алгебраической структуры поля Галуа $GF(2^n)$ с множеством 2^n элементов, что позволяет использовать все целые числа в диапазоне от 0 до $2^n - 1$ и реализовывать необходимые криптографические операции на полиномах [2–4].

Затем одновременно приемо-передающие устройства на сторонах отправителя и получателя данных переходят соответственно в режимы приема и передачи открытого криптографического ключа, который будет использован для получения шифртекста из смеси данных и идентификационной информации отправителя.

1 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования: ГОСТ 28147-89. – Введ. 01.07.90. – М. : ИПК Издательство стандартов, 1996. – 26 с.

Сущность функционирования приемо-передающего устройства на стороне получателя данных в режиме передачи открытого криптографического ключа заключается в следующем. Генератор ключей ГК (рисунок 1) вырабатывает открытый и секретный криптографические ключи в виде двоичных кодовых слов. Условия, которым должны соответствовать эти криптографические ключи, определяются выбранным асимметричным алгоритмом и реализуются посредством программного обеспечения системы управления. Следует отметить, что такой выбор зависит от криптографических требований, предъявляемых непосредственно к системе квантово-криптографической связи. При этом целесообразно использовать алгоритмы, для которых длина шифртекста не превышает длины зашифровываемых данных, поскольку в противном случае при прочих равных условиях передачи и приема не удастся обеспечить максимально возможную пропускную способность канала связи [10]. Секретный криптографический ключ получателя передается через шестой выход системы управления на второй вход блока расшифрования *D*. Одновременно на первый выход системы управления побитно передается открытый криптографический ключ, на третий выход – логическая единица.

Сигнал с первого выхода системы управления поступает на первый вход блока зашифрования данных Е и на второй вход формирователя данных Ф. Сигнал с третьего выхода системы управления поступает на третий вход формирователя данных Ф. Первый и второй входы формирователя данных Ф являются информационными, а третий – управляющим.

Формирователь Ф, источник оптического сигнала ИС и нейтральный светофильтр Н образуют передающий модуль устройства, который работает в режиме асинхронной передачи информации. Такой режим не требует наличия дополнительной линии связи для передачи и приема синхроимпульсов, что в ряде случаев оказывается более предпочтительным, чем организация режима синхронной передачи информации.

Передающий модуль устройства функционирует следующим образом. Формирователь Ф кодирует поступающие на его информационные входы импульсы, которые представляют собой двоичную последовательность, таким образом, что символам «0» и «1» соответствуют прямоугольные импульсы длительностью Δt и напряжением U_1 и U_2 соответственно ($U_1 < U_2$). Причем между каждой парой символов находится так называемый защитный временной интервал, в течение которого сигнал на выходе формирователя Ф отсутствует, как показано на рисунке 2.

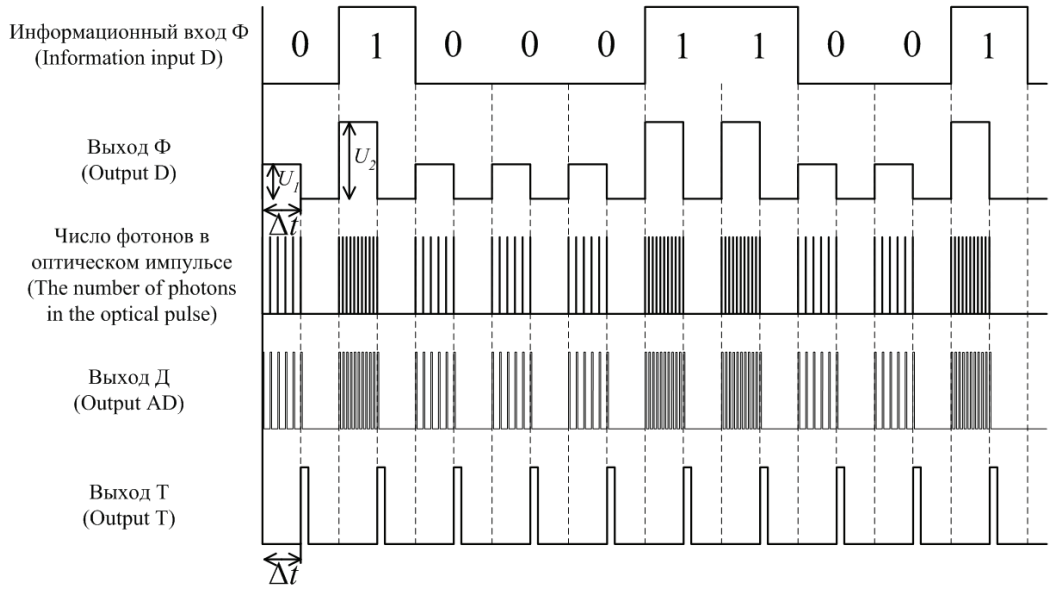

Рисунок 2 – Временная диаграмма функционирования устройства

Figure 2 – Timing diagram of the device operation

Выбор первого или второго кодируемого информационного входа формирователя Ф управляется сигналом, поступающим на его третий вход: при наличии на управляющем входе логического нуля и логической единицы формирователь Ф кодирует соответственно первый и второй информационные входы.

Таким образом, в режиме передачи открытого криптографического ключа формирователь Ф, входящий в состав передающего модуля приемо-передающего устройства получателя, кодирует импульсы, поступающие на его второй информационный вход.

С формирователя Ф импульсы поступают на вход источника оптического сигнала ИС. На выходе источника ИС формируется оптический сигнал длительностью Δt и мощностью P_1 под воздействием на его вход напряжения U_1. При появлении на входе источника ИС импульса с напряжением U_2 на его выходе генерируется оптический сигнал длительностью Δt и мощностью P_2 ($P_1 < P_2$).

Оптическое излучение с выхода источника сигнала ИС поступает через нейтральный светофильтр Н, обеспечивающий ослабление мощности оптического сигнала, на первый выход устройства и далее в оптическое волокно ОВ2.

В результате двоичная кодовая последовательность импульсов, соответствующая символам открытого криптографического ключа, передается по волоконно-оптическому каналу связи отправителю. После этого приемо-передающее устройство получателя переходит в режим приема шифртекста.

Сущность функционирования приемо-передающего устройства на стороне отправителя данных в режиме приема открытого криптографического ключа заключается в следующем.

Оптическое излучение поступает на второй вход приемо-передающего устройства отправителя из оптического волокна ОВ1, которое подключено к приемному модулю устройства.

Приемный модуль устройства содержит источник постоянного напряжения П, лавинный фотодиод ЛФД, резистор нагрузки $R_н$, усилитель У, амплитудный дискриминатор Д, логический элемент «И», счетчик импульсов Сч, *RS*-триггер Тр, генератор прямоугольных импульсов Г, таймер Т и линию задержки ЛЗ.

Приемный модуль устройства работает в режиме асинхронного приема информации следующим образом. Из оптического волокна ОВ1 излучение подается на лавинный фотодиод ЛФД. При помощи источника постоянного напряжения П на лавинный фотодиод ЛФД подается постоянное напряжение обратного смещения, превышающее напряжение пробоя *p*-*n*-перехода ЛФД. В этом случае лавинный фотодиод ЛФД работает в режиме счета фотонов [6]. Под действием оптического излучения в ЛФД формируются однофотонные импульсы тока. Количество этих импульсов прямо пропорционально энергии оптического импульса, которая равна произведению мощности оптического сигнала на время Δt. Количество однофотонных импульсов N также прямо пропорционально числу фотонов в импульсе.

Поскольку символы «0» и «1» передаются импульсами различной мощности, то на выходе лавинного фотодиода ЛФД за время передачи символа Δt формируется различное количество электрических импульсов, которое прямо пропорционально мощности оптического излучения. Поэтому число импульсов, соответствующее символу «0», будет меньше, чем число импульсов, соответствующее символу «1».

Максимальное число однофотонных импульсов N_0 ЛФД, сформированных за время Δt при передаче символа «0», будет меньше, чем минимальное число импульсов N_1, сформированных при передаче символа «1». Эти импульсы создают падения напряжений на резисторе нагрузки $R_н$, т.е. импульсы напряжения. После этого однофотонные импульсы усиливаются усилителем У и поступают на вход амплитудного дискриминатора Д. При помощи амплитудного дискриминатора Д выполняется амплитудная селекция усиленных импульсов напряжения на фоне шумов усилителя, а также их стандартизация по амплитуде и длительности. С выхода амплитудного дискриминатора Д импульсы поступают одновременно на *S*-вход *RS*-триггера Тр и на первый вход логического элемента «И». Первый импульс из последовательности импульсов переводит *RS*-триггер Тр в единичное состояние. Выход *RS*-триггера Тр соединен со вторым входом логического элемента «И» и управляющим входом таймера Т. Появление напряжения на втором входе логического элемента «И», соответствующего логической единице, позволяет импульсам с выхода амплитудного дискриминатора Д поступать на вход счетчика импульсов Сч, который подсчитывает число импульсов последовательности, поступающих на его вход (рисунок 1).

В момент времени переключения *RS*-триггера Тр из нулевого в единичное состояние запускается таймер Т. Через промежуток времени Δt на выходе таймера Т формируется импульс, который поступает на *R*-вход *RS*-триггера Тр, переводя его в нулевое состояние (см. рисунки 1 и 2). На выходе *RS*-триггера Тр формируется сигнал, соответствующий логическому нулю, который

подается на второй вход логического элемента «И», что останавливает поступление импульсов на вход счетчика импульсов Сч, а следовательно, останавливает и подсчет импульсов счетчиком Сч. Импульс с выхода таймера Т поступает также на вход линии задержки ЛЗ и на третий вход генератора прямоугольных импульсов Г.

При количестве импульсов $0 \le N \le N_0$, сосчитанных счетчиком Сч при передаче символа «0», на его первом выходе появляется уровень, соответствующий логической единице, а на втором выходе – уровень, соответствующий логическому нулю. В случае подсчета количества импульсов счетчиком Сч $N > N_0$ при передаче символа «1» на его первом и втором выходах появляются уровни, соответствующие логической единице. Выходы 1 и 2 счетчика импульсов Сч соединены с первым и вторым информационными входами генератора прямоугольных импульсов Г соответственно.

При наличии на первом информационном входе генератора прямоугольных импульсов Г уровня напряжения, соответствующего логической единице, а на втором входе – логического нуля, и при наличии на управляющем входе генератора прямоугольных импульсов Г импульса с выхода линии задержки ЛЗ на выходе генератора Г появляется уровень, соответствующий логическому нулю. При наличии на информационных входах генератора прямоугольных импульсов Г уровней напряжений, соответствующих логической единице, и при наличии импульса на его управляющем входе с выхода линии задержки ЛЗ на выходе генератора Г появляется уровень, соответствующий логической единице.

Сброс счетчика импульсов Сч происходит через некоторый промежуток времени после прихода импульса от таймера Т на управляющий вход генератора прямоугольных импульсов Г. Длительность этого времени задается линией задержки ЛЗ.

В результате двоичная кодовая последовательность импульсов, соответствующая символам открытого криптографического ключа, поступает с выхода генератора прямоугольных импульсов Г на первый вход блока расшифрования данных *D* и на второй вход системы управления устройства. Система управления устройства передает символы открытого криптографического ключа на свой второй выход.

После этого приемо-передающее устройство на стороне отправителя данных переходит в режим передачи шифртекста. Сущность этого режима заключается в следующем. Двоичные данные, подлежащие передачи по волоконно-оптическому каналу связи, поступают на первый вход системы управления устройства отправителя.

Система управления устройства отправителя устанавливает на своем третьем выходе уровень, соответствующий логическому нулю, разбивает данные, поступающие на ее первый вход, на кодовые слова длиной *n* бит, дополняя при необходимости слово символами «0», на основании блоков данных для подстановки, содержащихся в блоке памяти БП, подмешивает к каждому такому слову идентификационную информацию отправителя *IDA*, формирует и передает полученную смесь данных и идентификационной информации отправителя на свой первый выход.

Дополнение кодовых слов символами «0» необходимо выполнять, если длина кодового слова, используемого для получения смеси данных и идентификационной информации отправителя, меньше *n* бит. Такая ситуация может возникнуть в случае, когда общая длина данных, подлежащих передаче по волоконно-оптическому каналу связи, либо меньше, либо не кратна числу *n*. При этом недостающие биты дополняются символами «0» со стороны старших разрядов кодового слова.

Сформированная смесь данных и идентификационной информации отправителя поступает через первый выход системы управления на первый вход блока зашифрования данных Е и на второй вход формирователя данных Ф.

Блок зашифрования данных Е зашифровывает данные, поступающие на его первый информационный вход, на открытом криптографическом ключе, который подается на второй управляющий вход Е со второго выхода системы управления устройства. Это обеспечивает зашифрование смеси данных и идентификационной информации отправителя и получение шифртекста. Шифртекст побитно поступает на первый информационный вход формирователя данных Ф передающего модуля устройства отправителя через выход блока зашифрования данных Е. Поскольку на третий управляющий вход формирователя данных Ф подается логический нуль, формирователь Ф кодирует импульсы, поступающие на его первый информационный вход. В результате двоичная кодовая последовательность импульсов, соответствующая символам шифртекста, передается по волоконно-оптическому каналу связи получателю.

Приемо-передающее устройство на стороне получателя в режиме приема шифртекста функционирует следующим образом.

На второй вход устройства поступают оптические импульсы шифртекста, которые в режиме асинхронного приема информации регистрируются с помощью приемного модуля получателя и подаются с выхода генератора прямоугольных импульсов Г на первый вход блока расшифрования данных *D* и на второй вход системы управления устройства.

Блок расшифрования данных *D* расшифровывает данные, поступающие на его первый информационный вход, на секретном криптографическом ключе получателя. Этот ключ подается на второй управляющий вход *D* с шестого выхода системы управления устройства. С выхода блока расшифрования *D* данные подаются на третий вход системы управления устройства.

Система управления приемо-передающего устройства на стороне получателя разбивает данные, поступающие на ее третий вход, на кодовые слова длиной ($n + IDA$) бит, выделяет из каждого такого слова идентификационную информацию отправителя *IDA'* и на ее основе устанавливает подлинность принятых данных и их отправителя.

Выделение из каждого кодового слова *IDA'* осуществляется на основании блоков данных для подстановки, хранящихся в блоке памяти БП устройства получателя. При этом значения и номера бит *IDA'* определяются аналогично, как и при подмешивании *IDA* в устройстве отправителя.

Установление подлинности принятых данных и их отправителя осуществляется путем сравнения *IDA* и *IDA'*, что реализуется посредством компаратора К (см. рисунок 1). Если эта информация совпадает для каждого кодового слова, то делается вывод о подлинности принятых данных и их отправителя, и система управления передает данные отправителя на свой четвертый выход. В противном случае устанавливается факт нелегальности данных и их отправителя, и система управления сигнализирует об этом, передавая на свой пятый выход уровень напряжения, соответствующий логической единице.

Следует отметить, что в разработанной системе квантово-криптографической связи конфиденциальность информации, передаваемой по волоконно-оптическому каналу связи, обеспечивается ее шифрованием. При этом наличие двух ключей, один из которых используется для зашифрования данных, а второй – для расшифрования, позволяет передавать открытые ключи по незащищенному волоконно-оптическому каналу связи и сохранять секретные ключи в той части системы связи, в которой будет осуществляться расшифрование данных. В сравнении с известными двухключевыми алгоритмами шифрования и расшифрования данных [1–4] разработанная квантово-криптографическая система связи на базе предложенного приемо-передающего устройства является более защищенной. Это объясняется тем, что информационная безопасность системы связи, предложенной в данной работе, основана не только на безопасности алгоритма шифрования и расшифрования данных, но и на секретности идентификационных данных отправителя (значениях идентификационных данных и их расположения в блоках данных, подлежащих зашифрованию) и используемых принципах передачи и приема шифртекстов при помощи оптических импульсов слабой мощности, которые содержат от одного до нескольких десятков фотонов.

Смешивание на передающей стороне данных, подлежащих передаче, с идентификационной информацией отправителя в виду случайности данных и секретности значений и расположения бит *IDA* не позволяет выделить несанкционированному пользователю ни данных, ни *IDA*, а также не позволяет навязывать ложные данные, которые злоумышленник может пытаться выдавать за подлинные, транслируя в канал связи. Вместе с тем для легальных пользователей системы связи соответственно гарантируется конфиденциальность передаваемой информации и подлинность как самих данных, так и их отправителя.

Следует также отметить, что несанкционированный съем данных, передаваемых по волоконно-оптическому каналу связи, приведет к потере части мощности оптического излучения, в результате чего количество импульсов, сосчитанных счетчиком импульсов Сч при передаче символа «1», окажется меньше либо равным N_0, поэтому на выходе генератора прямоугольных импульсов Г будут формироваться только символы «0». При использовании несанкционированным пользователем компенсационного метода съема данных, описанного в [11], количество импульсов, сосчитанных счетчиком Сч, окажется больше N_0 как при передаче символов «0», так и при передаче символов «1», поэтому на выходе генератора прямоугольных импульсов Г будут формироваться только символы «1». Это объясняется тем, что при подключении несанкциони-

рованного пользователя к волоконно-оптической линии связи в некоторой точке расстояние от нее до выхода линии связи будет всегда меньше, чем длина линии между легальными пользователями системы связи. Следовательно, вероятность поглощения оптических импульсов, передаваемых от несанкционированного передатчика к легальному получателю, окажется меньше вероятности поглощения оптических импульсов, передаваемых от легального отправителя к легальному получателю. Очевидно, что в соответствии с описанными выше принципами функционирования разработанной квантово-криптографической системы связи на базе предложенного приемо-передающего устройства при установлении подлинности принятых данных и их отправителя в случае приема кодовых слов, состоящих только из одноименных символов, будет обнаружен факт нелегальности данных и их отправителя, и система управления просигнализирует об этом, передав на свой пятый выход уровень напряжения, соответствующий логической единице

Заключение

Разработано устройство для систем квантово-криптографической связи, в котором в качестве приемного модуля применен счетчик фотонов. Устройство не требует использования для передачи данных поляризационного оптического излучения, что, в сравнении с известными, упрощает его, ускоряет процесс обмена информацией за счет устранения процедуры согласования базисов, в которых переданы и приняты символы, и уменьшает ошибку передачи данных, связанную с деполяризацией оптического излучения.

Продемонстрирована возможность применения кремниевых лавинных фотоприемников в режиме счета фотонов для систем передачи конфиденциальной информации, определяющих подлинность источника передаваемой информации.

Разработанная система волоконно-оптической связи, содержащая в качестве приемного модуля счетчик фотонов на базе лавинного фотоприемника, позволяет обнаружить несанкционированный доступ к информации и нарушение ее целостности и ускорить процесс обмена информацией в сравнении с известными квантово-криптографическими системами связи.

Информационная безопасность системы квантово-криптографической связи, построенной на базе разработанного приемо-передающего устройства, определяется безопасностью алгоритма шифрования и расшифрования данных, секретностью как самих идентификационных данных отправителя, так и их расположением в блоках данных, подлежащим зашифрованию, а также за счет используемых режимов асинхронной передачи и приема информации при помощи оптических импульсов слабой мощности, которые содержат от одного до нескольких десятков фотонов.

Применительно к предложенной в данной работе системе квантово-криптографической связи для достоверного определения подлинности источника передаваемой информации и обеспечения конфиденциальности данных особенно важно учитывать количество возможных ошибок, возникающих при регистрации данных и обусловленных неидеальностью характеристик оборудования легитимных пользователей. В этой связи автору настоящей работы видится перспективным установление влияния мощности оптического излучения, используемого для передачи двоичных символов, и среднего времени однофотонной передачи на вероятности ошибочной регистрации символов «0» и «1», что планируется выполнить в ходе дальнейших исследований.

Список использованных источников

1. *Олифер, В.Г.* Безопасность компьютерных сетей / В.Г. Олифер, Н.А. Олифер. – М. : Горячая линия-Телеком, 2016. – 644 с.

2. *Шнайер, Б.* Прикладная криптография / Б. Шнайер. – М. : Триумф, 2002. – 816 с.

3. *Лапонина, О.Р.* Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия / О.Р. Лапонина. – М. : НОУ «Интуит», 2016. – 244 с.

4. Криптография / Н. Смарт. – М. : Техносфера, 2005. – 528 с.

5. *Килин, С.Я.* Квантовая криптография: идеи и практика / С.Я. Килин ; под ред. С.Я. Килин, Д.Б. Хорошко, А.П. Низовцева. – Минск : Белорус. наука, 2007. – 391 с.

6. *Тимофеев, А.М.* Исследование распределения временных интервалов между импульсами лавинных фотоприемников, работающих в режиме счета фотонов / А.М. Тимофеев // Вестник связи. – 2011. – № 1 (105). – С. 39–41.

7. Resonant-cavity-enhanced single-photon avalanche diodes on reflecting silicon substrates / M. Ghioni [et al.] // IEEE Photonics Technology Letters. – 2008. – Vol. 20, no. 6. – P. 413–415.

8. Solid-state single-photon detectors / F. Zappa [et al.] // Optical Engineering. – 1996. – Vol. 35, – no. 4. – P. 938-945.

9. *Микушин, А.В.* Программирование микропроцессоров семейства MCS-51 / А.В. Микушин, В.И. Синин. – Новосибирск : СибГУТИ, 2016. – 161 с.

10. *Клюев, Л.Л.* Теория электрической связи : учебник / Л.Л. Клюев. – Минск : Технoперспектива, 2008. – 423 с.

11. Способ связи по волоконно-оптической линии с обнаружением несанкционированного доступа к передаваемым данным : пат. 20051 Респ. Беларусь, МПК (2013.01) H 04B 10/00, H 04B 10/85 / И.Р. Гулаков, А.О. Зеневич, А.М. Тимофеев; заявитель Бел. гос. ун-т. – № a 20131068; заявл. 10.09.2013; опубл. 30.04.2016 // Официальный бюл. / Нац. центр интеллектуал. собственности. – 2016. – №2. – С. 125.

References

1. Olifer V.G, Olifer N.A. *Bezopasnost' komp'yuternykh setei* [Security of computer networks]. Moscow, Hot line-Telecom Publ., 2016, 644 p. (in Russian).

2. Shnayer B. *Prikladnaya kriptografiya* [Applied cryptography]. Moscow, Triumph Publ., 2002, 816 p. (in Russian).

3. Laponina O.R. *Osnovy setevoi bezopasnosti: kriptograficheskie algoritmy i protokoly vzaimodeistviya* [Fundamentals of network security: cryptographic algorithms and protocols of interaction]. Moscow, NOU «Intuit», 2016, 244 p. (in Russian).

4. Smart N. *Kriptografiya* [Cryptography]. Moscow, Technosphere Publ., 2005, 528 p. (in Russian).

5. Kilin S.Ya. *Kvantovaya kriptografiya: idei i praktika* [Quantum cryptography: ideas and practices]. Minsk, Belarus. Nauka Publ., 2007, 391 p. (in Russian).

6. Timofeev A.M. [Investigation of the distribution of time intervals between pulses of avalanche photodetectors operating in the photon counting mode]. *Vestnik svyazi* [Communication bulletin], 2011, no. 1 (105), pp. 39–41 (in Russian).

7. Ghioni M., Armellini G., Maccagnani P., Rech I., Emsley M., Unlu M. Resonant-cavity-enhanced single-photon avalanche diodes on reflecting silicon substrates. *IEEE Photonics Technology Letters*, 2008, vol. 20, no. 6, pp. 413–415.

8. Zappa F., Lacaita A., Cova S., Lovati P. Solid-state single-photon detectors. *Optical Engineering*, 1996, vol. 35, no. 4, pp. 938–945.

9. Mikushin A.V. *Programmirovanie mikroprotsessorov semeistva MSS-51* [Programming microprocessors of the MSS-51]. Novosibirsk, SibGUTI, 2016, 161 p. (in Russian).

10. Klyuev L.L. *Teoriya elektricheskoi svyazi : uchebnik* [The theory of electrical communication: textbook]. Minsk, Tekhnoperspektiva Publ., 2008, 423 p. (in Russian).

11. Gulakov I.R., Zenevich A.O., Timofeev A.M. *Sposob svyazi po volokonno-opticheskoi linii s obnaruzheniem nesanktsionirovannogo dostupa k peredavaemym dannym* [The method of communication over a fiber optic line with the detection of unauthorized access to transmitted data]. Patent RF, no. 20051, 2016.