DOI 10.31891/2307-5732-2020-291-6-28-32
УДК 004.056.53

П.М. ШПАТАР, О.В. ГРЕСЬ, В.В. КАЧУР, А.Я. ТОМУЛЕЦЬ
Чернівецький національний університет імені Юрія Федьковича

ДЕТЕКТУВАННЯ ПООДИНОКИХ ФОТОНІВ В КВАНТОВИХ КРИПТОГРАФІЧНИХ СИСТЕМАХ

Технологія квантової криптографії, основана на квантових властивостях світла, дозволяє передавати по незахищеному каналу зв'язку випадкову послідовність біт таким чином, що втручання зловмисника в процес передачі породжує додатковий шум в каналі і виявляється легітимними користувачами. Одним із важливих елементів системи квантової розсилки ключа є детектор поодиноких фотонів.

Квантова криптографія виводить на новий рівень стандарти захищеної передачі даних через відкриті канали зв'язку. Проте, практична реалізація протоколів квантової криптографії на базі доступних на сьогоднішній день компонентів стикається зі значними труднощами.

В статті запропонована апаратна реалізація пристрою реєстрації поодиноких фотонів на ESP8266. Запропонований пристрій підвищує точність вимірювання інтенсивності випромінювання з допомогою лавинного фотодіода, що працює в режимі лічильника фотонів, за допомогою стабілізації величини різниці між напругою живлення і напругою пробою лавинного фотодіода без втрат часу вимірювання.

Ключові слова: квантова криптографія, детектори поодиноких фотонів, лавинні фотодіоди, оптоволоконні лінії зв'язку, розподілення квантового ключа.

P. SHPATAR, O. HRES, V. KACHUR, A. TOMULETS
Yuriy Fedkovych Chernivtsi National University

DETECTION OF SINGLE PHOTONS IN QUANTUM CRYPTOGRAPHIC SYSTEMS

Quantum cryptography technology, based on the quantum properties of light, allows an unsecured sequence of bits to be transmitted over an unsecured communication channel in such a way that an intruder interferes with the transmission process and creates additional noise in the channel and is legitimate by users. One of the important elements of the quantum key distribution system is the single photon detector.

The basic principles of data protection in quantum communication lines are the impossibility of copying the previously unknown state of an individual quantum object and the impossibility of obtaining any information about the quantum states of this object without damaging them. Thus, the guarantee of protection of transmitted information are the fundamental laws of quantum mechanics.

Quantum cryptography takes to a new level the standards of secure data transmission over open communication channels. However, the practical implementation of quantum cryptography protocols based on currently available components faces significant difficulties.

Therefore, the development of new protocols for quantum key distribution, as well as achieving a high level of their cryptographic stability through the use of sensitive detectors of single photons based on avalanche photodiodes is an actual problem.

The article proposes a hardware implementation of a single photon detection device on ESP8266. The proposed device increases the accuracy of measuring the intensity of radiation using an avalanche photodiode operating in the mode of a photon counter, by stabilizing the value of the difference between the supply voltage and the breakdown voltage of the avalanche photodiode without loss of measurement time. With this system, measurements can be made at room temperature without the use of energy-intensive refrigerants. Dark noise and temperature instability are taken into account in the value of the voltage ΔU. The developed device allows to increase the quantum efficiency of registration up to 45%.

Keywords: quantum cryptography, single photon detectors, avalanche photodiodes, fiber optic communication lines, quantum key distribution.

Постановка проблеми. Необхідність реєстрації поодиноких фотонів виникла ще в 20 столітті після фундаментальних робіт М. Планка та А.Ейнштейна. Перші прилади, що дозволяють здійснювати таку реєстрацію, багатокаскадні фотоелектронні помножувачі, були створені в 30-х роках минулого століття. Подальші вдосконалення фотоелектронних помножувачів полягали в розширенні їх оптичного діапазону і збільшенні коефіцієнту підсилення. Тенденція підвищення швидкодії та квантової ефективності привела до створення лавинних фотодіодів (ЛФД). При роботі в якості детектора фотонів ЛФД переводиться в режим, близький до лавинного пробою. Поодинокий фотон в такому режимі здатний викликати лавинний пробій. Саме струм пробою і дозволяє зареєструвати акт поглинання фотона. Оскільки даний режим не є стандартним, існує достатньо велика кількість параметрів схеми ввімкнення, зміна яких дає можливість досягти покращення характеристик приймача фотонів в цілому.

Технологія квантової криптографії, основана на квантових властивостях світла, дозволяє передавати по незахищеному каналу зв'язку випадкову послідовність біт таким чином, що втручання зловмисника в процес передачі породжує додатковий шум в каналі і виявляється легітимними користувачами [1]. Одним із важливих елементів системи квантової розсилки ключа є детектор поодиноких фотонів.

Аналіз основних публікацій. В сучасних роботах розрізняють два основних підходи до розуміння квантового сигналу: поодинокі фотони і когерентні стани [2, 3]. Відомо декілька механізмів генерації поодиноких фотонів, зокрема, з використанням квантових точок [4] и спонтанного параметричного розсіювання [5].

Альтернативним є використання коротких лазерних імпульсів, які послаблені до критичного рівня так, що середнє число фотонів в них менше одиниці [2, 6]. В квантовій криптографії у зв'язку з цим часто

використовується термін «одна десята фотона», який означає, що одиночний фотон присутній в середньому лишень в одному із десяти часових відліків.

Основоположними принципами захисту даних в квантових лініях зв'язку є неможливість копіювання заздалегідь невідомого стану окремого квантового об'єкта і неможливість отримання будь-якої інформації про квантові стани цього об'єкта без їх пошкодження. Таким чином, гарантією захисту переданої інформації виступають фундаментальні закони квантової механіки. Багатьма експертами квантова криптографія розглядається як єдиний метод, здатний забезпечити реальний захист систем комунікацій. Ідеї і перспективи цього напряму досліджень виявилися настільки привабливими, що дослідницькі групи відразу ж почали активну роботу зі створення реально працюючих установок і пристроїв. На даний момент проблеми створення квантових систем зв'язку є актуальними, і ця область динамічно розвивається.

Для збільшення відстані і швидкості передачі необхідний пошук нових теоретичних підходів модифікацій протоколів квантової криптографії, що дозволяють ефективніше використовувати лазерні імпульси в якості джерел квантових станів і знижувати обмеження на співвідношення сигнал / шум

У квантової криптографії стійкість протоколів квантового розподілу ключів обґрунтовується теоретично. Таким чином квантова криптографія виводить на новий рівень стандарти захищеної передачі даних через відкриті канали зв'язку [7]. Проте, практична реалізація протоколів квантової криптографії на базі доступних на сьогоднішній день компонентів стикається зі значними труднощами.

Метою роботи є розробка нових протоколів квантового розподілу ключів, а також досягнення високого рівня їх криптографічної стійкості завдяки застосуванню чутливих детекторів поодиноких фотонів на основі лавинних фотодіодів.

Структурна схема квантово-криптографічної системи

При аналізі існуючих квантово-криптографічних систем можна виділити три основні види таких систем: з поляризаційним кодуванням, з фазовим кодуванням і часовим кодуванням. Чим більше параметрів безпеки дослідник накладає на систему і контролює їх, тим більшою мірою користувач може отримати рівень безпеки і захисту від зловмисника. При аналізі недоліки були виявлені в кожній системі. Тому при комбінуванні систем в один комплекс ми намагалися позбутися від таких негативних рис.

Перед розглядом структурної схеми слід ввести деякі фундаментальні поняття для квантової системи.

У даній системі ми вводимо поняття синхронізаційних та інформаційних фотонів. Інформаційний фотон - носій інформації, який передає основну (корисну) інформацію.

Синхронізаційний фотон - це фотон, який необхідний для синхронізації дій відправника і отримувача і є точкою відліку при передачі ключовий послідовності. Необхідно підкреслити необхідність і корисність даного кроку: якщо зловмисник якимось чином і проникне в канал передачі інформації, то, не знаючи попередньої домовленості учасників передачі, він жодним чином не відрізнить інформаційний фотон від синхронізаційного.

Отже, перейдемо до розгляду структурної схеми комплексу, яка представлена на рис. 1.

Як показано на рис. 1, система має один напівпровідниковий діодний лазер, що використовується для генерації інформаційного і синхронізаційного фотонів.

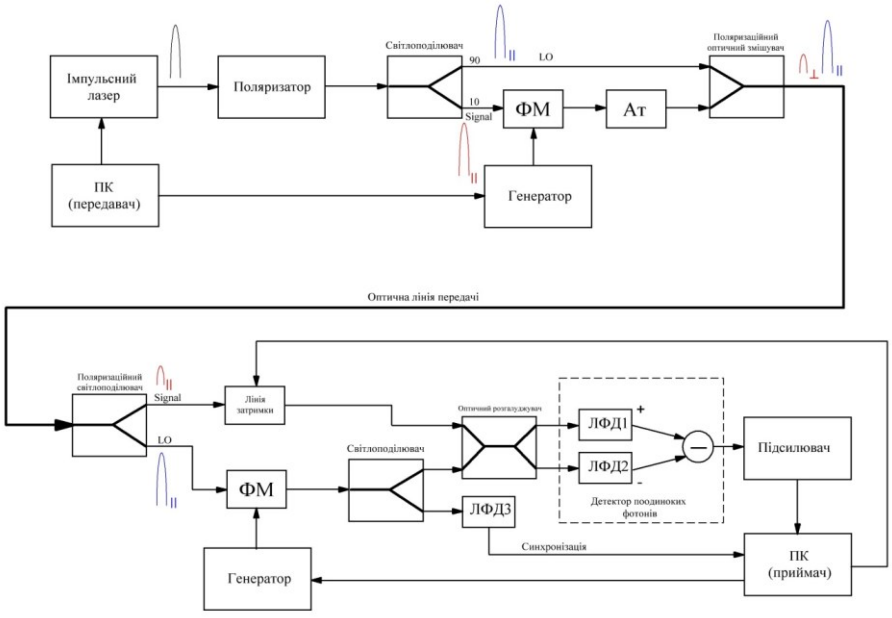

Рис. 1. Структурна схема криптографічної системи

Звичайно, лазер повинен бути термостабілізованим. З персонального комп'ютера для початку і завершення генерації випромінювання на лазер подаються керуючі сигнали. Після поляризатора імпульс лазерного випромінювання потрапляє на світлоподілювач 90/10. Сигнал з більшою потужністю називають

локальним осцилятором (local oscillator, LO). Один із світлових сигналів використовується для синхронізації, а інший – є інформаційним. Після фазового модулятора встановлений атенюатор, який послаблює пучок, і забезпечує необхідну ступінь однофотонності. Після атенюатора ми отримали «живий матеріал», з яким можна працювати і з яким можна задавати потрібні параметри. Потім випромінювання потрапляє на поляризаційний оптичний змішувач і передається в оптичну лінію зв'язку. На приймальній стороні здійснюються зворотні дії. Сигнал поступає на поляризаційний світлоподілювач, де здійснюється розподіл інформаційного і синхронізаційного фотонів.

Слід зауважити, що час приходу обох сигналів на приймач різний і його необхідно компенсувати. Обидва сигнали потрапляють на поляризаційний світлоподілювач і, оскільки вони мають ортогональну поляризацію, проходять знову по різним плечам інтерферометра. Але тепер пучок, який проходив по короткому плечу буде проходити по довгому плечу, і навпаки для іншого пучка. Приймач вмикає свій фазовий модулятор (ФМ), який так само як і на стороні передавача, генерує відповідний зсув фази, який необхідний для отримання інформації шляхом детектування. Приймач надає фазовий зсув своїм модулятором локальному осцилятору після чого сигнал локального осцилятора потрапляє в лінію затримки, де відбувається компенсація часової різниці надходження між корисним сигналом та сигналом локального осцилятора. Після цього обидва промені потрапляють до поляризаційного оптичного розгалужувача, який підключений до детектора поодиноких фотонів.

Перед початком передачі ключової послідовності учасники інформаційного обміну проводять попередню домовленість. У даній системі передавачу і отримувачу необхідно домовитися про фази фотона, який генерує передавач, і задання часових проміжків між парами синхронізаційних фотон - інформаційний фотон. Може виникнути питання, навіщо потрібно задавати послідовність фази фотонів, які будуть генеруватися передавачем.

У даній гібридній системі ми використовуємо прогнозування в часовій і фазовій області. Передавач і отримувач знають технологічні характеристики системи і таким чином можуть спрогнозувати, яку фазу ми отримаємо на виході. Якщо зловмисник перехопить такий фотон і застосує атаку типу вимірювання - пересилання, то ця спроба підробки ключа провалиться, оскільки він не знає, на який кут повороту повинна повернутися фаза. Також в системі велику роль відіграє час і часові затримки, про які зловмисник, до речі, не знає нічого. І якщо він і перехопить хоч частину ключової послідовності, то точно не зможе сказати, де інформаційні біти (фотони), а де синхронізаційні. Отже, після попередньої домовленості сторони інформаційного обміну починають передачу ключової послідовності.

Квантово-криптографічний система з можливостями прогнозування жорстко закріплює параметри фотона і дозволяє ними керувати, забезпечуючи тим самим підвищення секретності ключової послідовності. Звичайно, квантові криптографічні системи зв'язку не є панацеєю від витоку інформації, але надають достатній рівень захисту для використання в мережах зв'язку.

Приймач поодиноких фотонів на основі лавинних фотодіодів

Найбільш близьким для вирішення даної задачі є пристрій реєстрації поодиноких фотонів з використанням лавинних фотодіодів (ЛФД) [8 – 10, 13]. При цьому на зворотно зміщений лавинний фотодіод подається напруга, що перевищує напругу пробою ЛФД на величину ΔU. Пробій фотодіода не відбувається до тих пір поки в області сильного електричного поля не з'явиться термо- або фотогенерований носій електричного заряду. Тоді у фотодіоді за рахунок лавинного помноження цього заряду виникає імпульс струму. Помноження заряду буде відбуватися до тих пір, поки напруга на діоді не зменшиться до величини, меншої напруги пробою. Між струмом, що протікає через ЛФД під час пробою, і ΔU існує прямопропорційна залежність, тому і середня амплітуда імпульсів, що формуються на резисторі навантаження, пропорційна величині ΔU. Однак а процесі роботи ЛФД напруга його пробою змінюється із-за зміни параметрів навколишнього середовища і умов реєстрації оптичного випромінювання. При цьому змінюється і величинаΔU, від якої залежать такі характеристики фотодіода як квантова ефективність реєстрації, швидкість підрахунку імпульсів та ін. Величина ΔU також може змінюватися із-за нестабільності напруги джерела живлення. Тому для стабільної роботи ЛФД необхідно підтримувати постійне значення ΔU.

Задача стабілізації ΔU вирішується за допомогою функціональної схеми, зображеної на рис. 2.

За допомогою джерела живлення встановлюється напруга живлення фотодіода вище його напруги пробою. Під дією оптичного випромінювання в фотодіоді виникає лавинний пробій і через резистор навантаження протікають імпульси струму, які поступають на вхід підсилювача П1. Після підсилення імпульси поступають на входи компараторів К1 і К2. Поріг амплітудної дискримінації К1 вибирається над рівнем власних шумів підсилювача. Поріг амплітудної дискримінації К2 вибирається таким чином, щоб швидкість підрахунку імпульсів на виході компаратора К1 була в n раз більшою, ніж на виході К2. З виходу К1 імпульси поступають на вхід D5 мікроконтролера MCU (ESP8266). З виходу К2 імпульси поступають на вхід D6 мікроконтролера MCU. Коли мікроконтролер нараховує задане число N імпульсів, на його виході формується відповідний сигнал для ЦАП (MCP4728).

Дані з виходів D1 – D4 поступають на чотирьох-канальний цифро-аналоговий перетворювач ЦАП, що перетворює цифровий сигнал в напругу керування джерелом живлення. Якщо напруга ЦАП вища деякого заданого значення, то напруга джерела живлення ЛФД зменшується, якщо нижча – збільшується. Таким чином здійснюється постійне підналагодження напруги ΔU. Задавати значення порогів амплітудної дискримінації компараторів та контролювати значення встановлених параметрів можна з допомогою

персонального комп'ютера (ПК), що зв'язується з мікроконтролером бездротовою мережею WiFi, або дисплея Nextiion, що оснащений тачскріном.

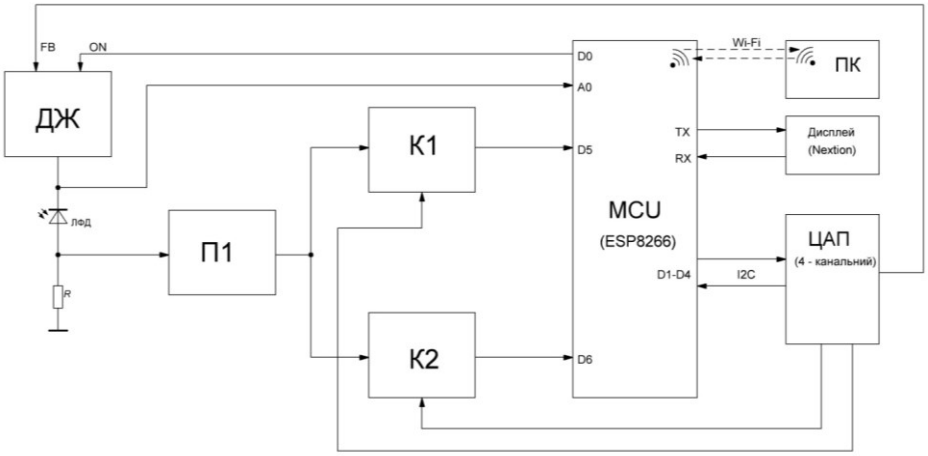

Рис. 2. Функціональна схема пристрою реєстрації поодиноких фотонів

При роботі ЛФД в режимі лічильника фотонів амплітудний розподіл вихідних імпульсів фотодіода залежить від ΔU. Під амплітудним розподілом розуміють залежність ймовірності появи імпульсів від величини амплітуди. Така відмінність амплітуд імпульсів пов'язана зі статичним характером процесу помноження носіїв заряду. Для однакових амплітуд розподіли будуть однаковими і ймовірність перевищення або не перевищення імпульсами деякого порогу амплітудної дискримінації. Тому, якщо в процесі вимірювання інтенсивності оптичного випромінювання будуть контролюватися ймовірності перевищення імпульсами деякого порогу амплітудної дискримінації, то можна здійснити стабілізацію величини ΔU по відхиленню ймовірності перевищення імпульсами деякого порогу амплітудної дискримінації від наперед заданого значення. Якщо на виході фотоприймача загальне число імпульсів рівне N, то із них тільки N1 імпульсів перевищать заданий поріг амплітудної дискримінації. Тоді ймовірність перевищення порогу може бути визначена за співвідношенням N1/N [14, 15]. Контролюючи це співвідношення, можна зробити висновок про зміну величини ΔU. Якщо ΔU змінилась, то автоматично здійснюється її підналагодження. При збільшенні співвідношення N1/N величину ΔU необхідно зменшити, а при зменшенні N1/N – збільшити ΔU.

Виміряні значення квантової ефективності реєстрації від величини шумів в перерахунку на один імпульс становлять 30 ÷ 45%. Ймовірність реєстрації і рівень темнового шуму визначались сумарною зворотною напругою зміщення ЛФД, яка змінювалась при проведенні вимірювань.

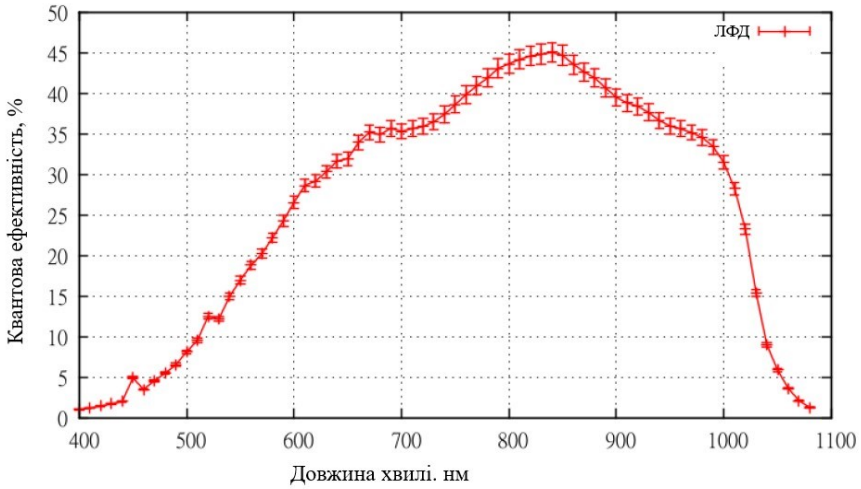

Рис. 3. Залежність квантової ефективності від довжини хвилі

Висновки

Розроблений пристрій реєстрації поодиноких фотонів підвищує точність вимірювання інтенсивності випромінювання з допомогою лавинного фотодіода, що працює в режимі лічильника фотонів, за допомогою стабілізації величини різниці між напругою живлення і напругою пробою лавинного фотодіода без втрат часу вимірювання. За допомогою даної системи можна проводити вимірювання при кімнатних температурах без використання енергозатратних засобів охолодження. Темнові шуми і температурна нестабільність враховані у значенні величини напруги *ΔU*. Розроблений пристрій дозволяє підвищити квантову ефективність реєстрації до 45 %.

Література

1. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers Systems and Signal Processing. 1984. Pp. 175–179.

2. Егоров В.И., Латыпов И.З., Рупасов А.В., Глейм А.В., Чивилихин С.А. Установка квантовой криптографии с источником одиночных фотонов, основанным на явлении спонтанного параметрического рассеяния света. Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2012. № 1 (77). С. 25 - 29.

3. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography. Rev. Mod. Phys. 2002. Vol. 74 , № 1. Pp. 145–190.

4. Unitt D.C., Bennett A.J., Atkinson P. et.al. Quantum dots as single-photon sources for quantum information processing. Journal of optic. 2005. Vol. 7, № 7. Pp. 129–134.

5. Scarani V., Bechmann-Pasquinucci H., Cerf N.J. et al. The security of practical quantum key distribution. Rev. Mod. Phys. 2009. Vol. 81. Pp. 1301–1350.

6. Калачев А.А., Калашников Д.А., Калинкин А.А., Митрофанова Т.Г., Самарцев В.В., Шкаликов А.В. Бифотонная спектроскопия кристалла рубина. Учен. зап. Казан. гос. ун-та. Сер. физ.-матем. науки. 2008. Т. 150. Кн. 2. С. 125–130.

7. Корченко О.Г., Васіліу Є.В., Гнатюк С.О. Сучасні квантові технології захисту інформації. Науково-технічний журнал «Захист інформації». 2010. № 1. С. 77–89.

8. Курочкин Ю.В., Курочкин В.Л. Детекторы одиночних фотонов на основе лавинних фотодиодов. 2011. Т. 54, №2. С. 202-205.

9. Курочкин В.Л., Зверев А.В., Курочкин Ю.В., Рябцев И.И., Неизвестный И.Г. Применение детекторов одиночных фотонов для генерации квантового ключа в экспериментальной оптоволоконной системе связи. Автометрия. 2009. Т. 45, № 4. С. 110–119.

10. Trew R.T., Stucki D., Gautier J.-D. Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths. Appl. Phys. Lett. 2007. Vol.91. P. 201114.

11. Trifonov A., Subacius D., Berzanskis A., Zavriev A. Single photon counting at telecom wavelengths and quantum key distribution. Journ. Mod. Optics. 2004. Vol. 51, № 9-10. P.1399-1415.

12. Фотоприемники и фотоприемные устройства. Каталог ОАО «Кварц» . 2000-2001. С.61.

13. Болонна Є.І., Шпатар П.М. Приймач одиночних фотонів систем квантової криптографії. Наукові записки Українського науково-дослідного інституту зв'язку. 2017. №2(46). С. 74 – 79.

14. Bolonna E., Shpatar P. Device for registration of single photons. Scientific Light (Wroclaw, Poland). 2017. Vol.1, №5. P. 143-145.

15. Bolonna I. I., Shpatar P. M. Experimental scheme of single photon detection for quantum cryptography. Proceedings of 12 International conference "Correlation optics 2015", Chernivtsi, September 14-18, 2015. Chernivtsi, Ukraine.

References

1. Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers Systems and Signal Processing. 1984. Pp. 175–179.

2. Egorov V.I., Latypov I.Z., Rupasov A.V., Gleim A.V., Chivilikhin S.A. Ustanovka kvantovoi kriptografii s istochnikom odinochnykh fotonov, osnovannym na yavlenii spontannogo parametricheskogo rasseyaniya sveta. Nauchno-tekhnicheskii vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta informatsionnykh tekhnologii, mekhaniki i optiki. 2012. № 1 (77). S. 25 - 29.

3. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography. Rev. Mod. Phys. 2002. Vol. 74 , № 1. Pp. 145–190.

4. Unitt D.C., Bennett A.J., Atkinson P. et.al. Quantum dots as single-photon sources for quantum information processing. Journal of optic. 2005. Vol. 7, № 7. Pp. 129–134.

5. Scarani V., Bechmann-Pasquinucci H., Cerf N.J. et al. The security of practical quantum key distribution. Rev. Mod. Phys. 2009. Vol. 81. Pp. 1301–1350.

6. Kalachev A.A., Kalashnikov D.A., Kalinkin A.A., Mitrofanova T.G., Samartsev V.V., Shkalikov A.V. Bifotonnaya spektroskopiya kristalla rubina. Uchen. zap. Kazan. gos. un-ta. Ser. fiz.-matem. nauki. 2008. T. 150. Kn. 2. S. 125–130.

7. Korchenko O.G., Vasiliu Є.V., Gnatyuk S.O. Suchasni kvantovi tekhnologiї zakhistu informatsiї. Naukovo-tekhnichnii zhurnal «Zakhist informatsiї». 2010. № 1. S. 77–89.

8. Kurochkin YU. V., Kurochkin V. L. Detektory odinochnikh fotonov na osnove lavinnikh fotodiodov. 2011. T. 54, №2. S. 202-205.

9. Kurochkin V.L., Zverev A.V., Kurochkin YU.V., Ryabtsev I.I., Neizvestnyi I.G. Primenenie detektorov odinochnykh fotonov dlya generatsii kvantovogo klyucha v ehksperimental'noi optovolokonnoi sisteme svyazi. Avtometriya. 2009. T. 45, № 4. S. 110–119.

10. Trew R.T., Stucki D., Gautier J.-D. Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths. Appl. Phys. Lett. 2007. Vol.91. P. 201114.

11. Trifonov A., Subacius D., Berzanskis A., Zavriev A. Single photon counting at telecom wavelengths and quantum key distribution. Journ. Mod. Optics. 2004. Vol. 51, № 9-10. P.1399-1415.

12. Fotopriemniki i fotopriemnye ustroistva. Katalog OAO «Kvarts» . 2000-2001. S.61.

13. Bolonna Ye.I., Shpatar P.M. Priimach odinochnikh fotoniv sistem kvantovoi kriptografii. Naukovi zapiski Ukrainskogo naukovo-doslidnogo institutu zVyazku. 2017. №2(46). S. 74 – 79.

14. Bolonna E., Shpatar P. Device for registration of single photons. Scientific Light (Wroclaw, Poland). 2017. Vol.1, №5. P. 143-145.

15. Bolonna I. I., Shpatar P. M. Experimental scheme of single photon detection for quantum cryptography. Proceedings of 12 International conference "Correlation optics 2015", Chernivtsi, September 14-18, 2015. Chernivtsi, Ukraine.

Надійшла / Paper received : 20.11.2020 р. Надрукована/Printed :04.01.2021 р.