УДК 535.14

Болонна Є.І., аспірант; **Шпатар П.М.,** канд. техн. наук

ПРИЙМАЧ ОДИНОЧНИХ ФОТОНІВ СИСТЕМ КВАНТОВОЇ КРИПТОГРАФІЇ

Bolonna E.I., Shpatar P.M. Receiver of single-photon quantum cryptography systems.

The scheme of the single photons receiver based on avalanche photodiodes for quantum cryptography systems. Reduction of dark noise avalanche photodiodes achieved by cooling Peltier's elements. After triggering avalanche photodiode eliminated by pulse power.

The scheme of a receiver single photon avalanche photodiodes based on exercise selectivity avalanche breakthrough in the time of their occurrence and allows to reduce the likelihood of false triggering received photons at high speeds. This scheme can be used for all types of avalanche photodiode with separate absorption and multiplication regions. The measured quantum efficiency depending on the size of registration noise in terms of one pulse at different temperatures. Chance of registration and dark noise level determined total reverse bias voltage of the avalanche photodiode. By varying the delay submission of laser pulses can be measured after the likelihood of pulses in time relative to the main pulse of light. To reduce false positives using avalanche photodiode enabling circuit using a micro-strip line. Use one line instead of two would reduce the amount of heat supplied to the avalanche photodiode, and it simplifies cooling avalanche photodiode Peltier elements.

Keywords: quantum cryptography, single photon detectors, avalanche photodiodes.

Болонна Є.І., Шпатар П.М. Приймач одиночних фотонів систем квантової криптографії. Запропонована схема приймача одиночних фотонів на основі лавинних фотодіодів для систем квантової криптографії. Зменшення темнових шумів досягається охолодженням лавинних фотодіодів елементами Пельтьє. Післялавинні спрацювання усуваються імпульсним живленням фотодіода. Виміряні залежності квантової ефективності реєстрації від величини шумів в перерахунку на один імпульс при різних температурах. Ймовірність реєстрації і рівень темнового шуму визначались сумарною зворотною напругою зміщення лавинного фотодіода.

Ключові слова: квантова криптографія, детектори одиночних фотонів, лавинні фотодіоди.

Болонная Е.И., Шпатарь П.М. Приемник одиночных фотонов систем квантовой криптографии. Предложена схема приемника одиночных фотонов на основе лавинных фотодиодов для систем квантовой криптографии. Уменьшение темновых шумов достигается охлаждением лавинных фотодиодов элементами Пельтье. Послелавинные срабатывания подавляются применением импульсного питания фотодиода. Измерены зависимости квантовой эффективности регистрации от величины шумов в перерасчете на один импульс при разных температурах. Вероятность регистрации и уровень темнового шума определялись суммарным обратным напряжением смещения лавинного фотодиода.

Ключевые слова: квантовая криптография, детекторы одиночных фотонов, лавинные фотодиоды.

Вступ

Необхідність реєстрації одиночних 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. Одиночний 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.

Метою даної роботи є розробка приймача одиночних фотонів для інфрачервоного діапазону, що задовольняє умовам роботи в складі систем квантової криптографії.

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 одиночних фотонів.

В сучасних роботах розрізняють два основних підходи до розуміння квантового сигналу: одиночні фотони і когерентні стани [2, 3]. Відомо декілька механізмів генерації одиночних 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.

Реєстрація одиночних фотонів, які пройшли через оптичну лінію зв'язку, вимагає чіткого виявлення фотонів на фоні шумів і зменшення хибних спрацювань. Тому створення приймачів одиночних фотонів є актуальною науково-технічною задачею.

1. Структурна схема приймача одиночних фотонів

Оскільки для секретності передачі необхідна наявність не більше одного фотона в кожному лазерному імпульсі, до фотодетекторів ставляться високі вимоги. Вони повинні володіти високою квантовою ефективністю реєстрації, малими шумами і високою швидкістю підрахунку. Криптосистеми для передачі ключа по оптоволокну зазвичай працюють на телекомунікаційній довжині хвилі 1550 нм, яка забезпечує найменше затухання і мінімальну дисперсію у волокні [3]. Найкращими однофотонними детекторами для практичного використання є лавинні фотодіоди (ЛФД) [3, 8]. При реєстрації окремих фотонів ЛФД вмикають таким чином, щоб вони працювали в гейгеровському режимі [3, 8], коли один фотон здатний викликати лавину носіїв заряду. Для цього зворотну напругу живлення на них піднімають вище порогової напруги пробою: чим більша напруга над порогом, тим вища ймовірність реєстрації фотона. Однак при цьому значно зростають темнові шуми і ймовірність появи так званих післяімпульсів, які виникають в результаті спрацювання ЛФД. Для зменшення цих небажаних ефектів застосовують ряд спеціальних заходів. Наприклад охолодження ЛФД дає значне зменшення темнових шумів. Температуру ЛФД понижують до -40÷ -70 ^{o}C з допомогою мікрохолодильників на основі елементів Пельтьє. Для зменшення ймовірності появи післяімпульсів застосовують метод активного гасіння лавини [9] або працюють в режимі з імпульсним живленням, коли напругу на ЛФД підтримують нижче порогової, а для реєстрації одиночних фотонів її короткочасно збільшують вище порогової [10].

Структурна схема приймача одиночних фотонів представлена на рис. 1. Приймач фотонів складається з формувача стробуючих імпульсів, ЛФД, реєструючого пристрою і схеми подавлення післялавинних спрацювань. ЛФД поміщається в холодильник, побудований на елементах Пельтьє і оснащений системою термостабілізації.

Сигнал тактової синхронізації поступає на вхід схеми подавлення післялавинних спрацювань. Комп'ютер задає кількість імпульсів, які будуть пропущені у випадку спрацювання детектора. Таким чином виділяється час на звільнення носіїв, що захоплені пастками. Частота тактового сигналу може бути достатньо високою (до 10 МГц) і повинна встановлюватися з високою точністю. З виходу схеми подавлення післялавинних спрацювань керуючий імпульс подається на формувач. Сформований імпульс заданої тривалості і амплітуди поступає на ЛФД. Для нормальної роботи системи необхідно, щоб фотон поглинувся в той момент, коли на ЛФД діє стробуючий імпульс. В реальних умовах за це відповідає спеціальна система синхронізації. Однак при передачі інформації на великі відстані нестабільність в часі приходу фотона може складати 2 - 3 нс.

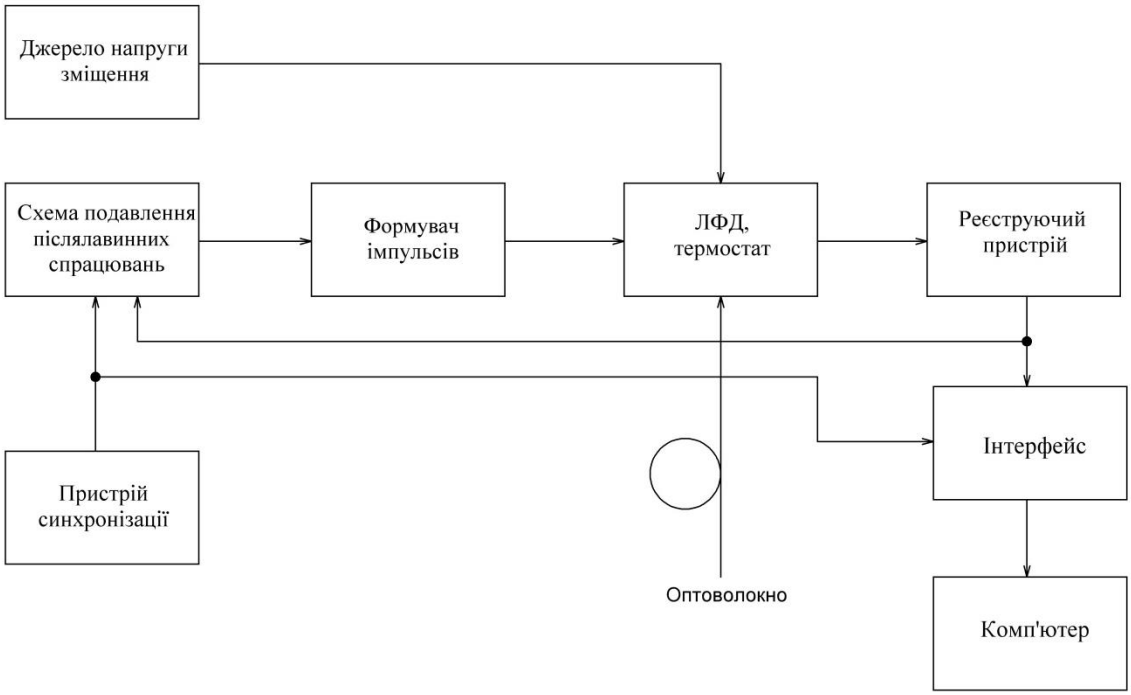

Рис. 1. Структурна схема приймача одиночних фотонів

Достатньо великі затримки виникають в схемі подавлення післялавинних спрацювань і у формувачі при його переналагодженні. Тому стривалість стробуючого імпульсу складає 3 – 5 нс. З виходу ЛФД імпульс поступає на вхід реєструючого пристрою, що складається з підсилювача і компаратора з буферним елементом на виході. З виходу реєструючого пристрою імпульс поступає на інтерфейсний блок і схему подавлення післялавинних спрацювань. Комп'ютер зчитує інформацію через інтерфейсний блок і при необхідності коректує кількість імпульсів після лавинного пробою.

При подачі стробуючого імпульсу відбувається заряд ємності ЛФД по фронту і спаду імпульсу. Струми заряду викликають скачки напруги на опорі навантаження. Додатний скачок створює заваду для детектування пробою. В тому випадку, коли поріг чутливості реєструючого пристрою налагоджений на максимум, детектор буде спрацьовувати по скачку напруги, що приведе до хибних спрацювань. Для зменшення цього ефекту використовується схема ввімкнення лавинного фотодіода з використанням однієї мікросмугової лінії (рис. 2).

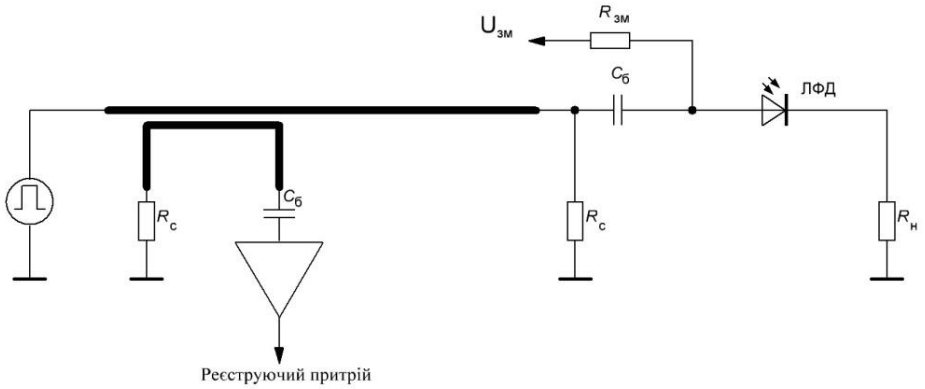

Рис. 2. Схема ввімкнення лавинного фотодіода

Імпульс струму лавини розповсюджується від ЛФД до генератора і через напрямлений відгалужувач попадає на реєструючий пристрій. Відгалужувач має розв'язку більше 10 дб, а також він є смуговим фільтром, який дозволяє реалізувати подавлення скачків струму заряду

ємності ЛФД. На виході відгалужувача ввімкнений широкосмуговий (100 МГц – 2,4 ГГц) НВЧ-підсилювач, що має коефіцієнт підсилення 20 дБ. Використання однієї лінії замість двох забезпечує зменшення кількості тепла, що підводиться до ЛФД, і це спрощує охолодження ЛФД елементами Пельтьє.

Імпульс струму лавини розповсюджується від ЛФД до генератора і через напрямлений відгалужувач попадає на реєструючий пристрій. Відгалужувач має розв'язку більше 10 дб, а також він є смуговим фільтром, який дозволяє реалізувати подавлення скачків струму заряду ємності ЛФД. На виході відгалужувача ввімкнений широкосмуговий (100 МГц – 2,4 ГГц) НВЧ-підсилювач, що має коефіцієнт підсилення 20 дБ. Використання однієї лінії замість двох забезпечує зменшення кількості тепла, що підводиться до ЛФД, і це спрощує охолодження ЛФД елементами Пельтьє.

В квантових криптографічних системах на приймальній стороні, як правило, встановлюють два приймачі фотонів. В схемі з точно підібраними довжинами волоконних з'єднань приймачі працюють синхронно. Важливим моментом є ідентичність характеристик приймачів та рівність квантових ефективностей і часових відгуків. З метою забезпечення таких умов ЛФД поміщаються в спільний холодильник. При цьому їх температура однакова і у випадку її зміни, наприклад, із-за помилок в роботі системи термостабілізації, тенденція зміни характеристики обох приймачів буде також однаковою.

2. Квантова ефективність приймача одиночних фотонів

В якості детекторів одиночних фотонів були протестовані спеціально відібрані лавинні фотодіоди ФД-312Л суміщені з оптоволокном. На лавинний фотодіод подавалися імпульси тривалістю 3,5 нс і амплітудою 4,2 В. Ця напруга добавлялася до постійної напруги зміщення ЛФД, яка вибиралася нижче порогової. Виміряні залежності квантової ефективності реєстрації від величини шумів в перерахунку на один імпульс при різних температурах зображені на рис. 3.

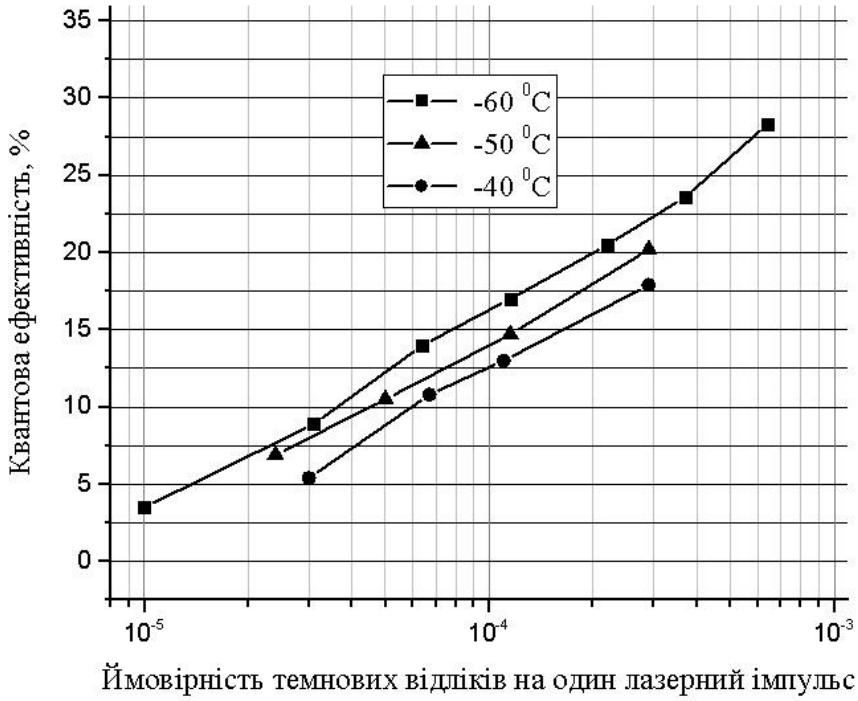

Рис. 3. Квантова ефективність детекторів одиночних фотонів

При цих вимірюваннях випромінювання лазера з частотою повторення лазерних імпульсів 1 МГц послаблювалось оптоволоконним атенюатором FC-20 дБ до рівня 0,1 фотон/імпульс. В момент приходу фотона на ЛФД подавався імпульс живлення, і фотодіод

переходив в гейгеровський режим для реєстрації одиночних фотонів. Ймовірність реєстрації і рівень темнового шуму визначались сумарною зворотною напругою зміщення ЛФД, яка змінювалась при проведенні вимірювань.

Залежність ймовірності появи післяімпульсів від часу при різних температурах показана на рис. 4. Частота повторення лазерних імпульсів вибиралася рівною 100 кГц для забезпечення часового інтервалу 10 мкс між лазерними імпульсами. Цей інтервал достатньо великий, щоб виключити взаємний вплив післяімпульсів між сусідніми світловими імпульсами. Потужність випромінювання лазера підбиралася так, щоб повна ймовірність детектування лазерних імпульсів була близькою до 100%. Наступний імпульс живлення ЛФД подавався з затримкою 0,1 ÷ 10 мкс по відношенню до основного, який синхронізований з моментом приходу фотона на ЛФД. Змінюючи затримку, можна вимірювати ймовірність появи післяімпульсів в часі відносно основного імпульсу світла.

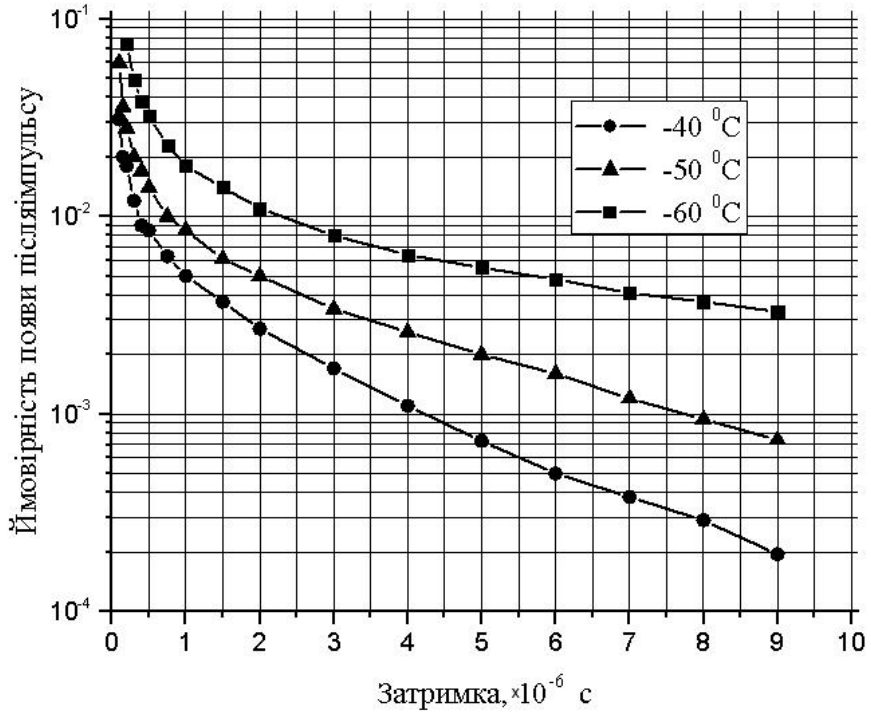

Рис. 4. Ймовірність появи післяімпульсів

Висновки

Розроблена схема приймача одиночних фотонів на основі ЛФД здійснює вибірковість лавинних пробоїв по часу їх виникнення і дозволяє на порядок зменшити ймовірність хибного спрацювання приймача фотонів при високих швидкостях передачі. Дана схема може використовуватися для всіх типів ЛФД з розділеними областями поглинання і помноження. Виміряні залежності квантової ефективності, ймовірності появи післяімпульсів для різних режимів роботи ЛФД в діапазоні температур -40÷ -60 ^{o}C. Ймовірність реєстрації і рівень темнового шуму визначались сумарною зворотною напругою зміщення лавинного фотодіода. Змінюючи затримку подачі лазерних імпульсів, можна вимірювати ймовірність появи післяімпульсів в часі відносно основного імпульсу світла. Для зменшення хибних спрацювань використовується схема ввімкнення лавинного фотодіода з використанням однієї мікросмугової лінії. Використання однієї лінії замість двох забезпечує зменшення кількості тепла, що підводиться до лавинного фотодіода, і це спрощує охолодження лавинного фотодіода елементами Пельтьє.

Список використаної літератури

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

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

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

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

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

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

7. Feihu Xu. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system / Xu Feihu, Qi Bing, Lo. Hoi-Kwong // New J. Phys. – 2010. – V. 12. – P. 113026.

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

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

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

Автори статті

Болонна Єлизавета Ігорівна - аспірант кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича, Чернівці, Україна. Тел. +38 037 224 24 36. E-mail: liza_000@mail.ru.

Шпатар Петро Михайлович – кандидат технічних наук, доцент, доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича, Чернівці, Україна. Тел. +38 050 978 50 14. E-mail: p.shpatar@chnu.edu.ua.

Authors of the article

Bolonna Elizaveta Igorivna- postgraduate student, department of the Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine. Tel. +38 037 224 24 36. E-mail: liza_000@mail.ru.

Shpatar Petro Mihaylovich - candidate of science (technic), assistant professor, associate professor department of the Radio Engineering and Information Security, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine. Tel. +38 050 978 50 14. E-mail: p.shpatar@chnu.edu.ua.

Дата надходження в редакцію: 25.03.2017 р. Рецензент: д.т.н., проф. В.А. Дружинін