DOI: 10.25586/RNU.V9187.19.01.P.019 УДК 519.8

В.А. Минаев, И.Д. Королев, О.А. Кулиш, А.В. Мазин

# МОДЕЛЬНЫЕ ИССЛЕДОВАНИЯ ВОЛОКОННО-ОПТИЧЕСКИХ КАНАЛОВ КОММУНИКАЦИИ В КВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

Посвящено модельным исследованиям волоконно-оптических каналов связи (ВОКС) в квантовых криптографических системах (ККС). Отмечены две основные проблемы использования ККС, связанных с достоверностью передачи информации. Проведен анализ факторов энергетических потерь в классическом волоконно-оптическом канале и детально обсуждается аддитивная формула потерь в нем. Рассмотрен волоконно-оптический канал передачи квантовой информации с применением интегрально-оптических устройств. Обсуждена аддитивная формула оптических потерь в таком канале. Показаны особенности потерь в интегрально-оптических устройствах, в частности затухание света в оптическом волокне, потери на изгибах и микроизгибах, технологические, дисперсионные и переходные потери. Охарактеризованы особенности квантово-криптографической системы передачи информации. Например, при построении модели фотоприемного устройства учитываются три основных параметра: квантовая эффективность, быстродействие, уровень шумов. В результате предложена модель ВОКС ККС с учетом энергетических потерь, позволяющая теоретически грамотно и наглядно представить прохождение информации через современные квантово-криптографически защищенные телекоммуникации при обеспечении управления в государственных структурах.

*Ключевые слова:* моделирование, волоконно-оптический канал, связь, квантовая криптографическая система, энергетические потери, защищенные коммуникации.

V.A. Minaev, I.D. Korolev, O.A. Kulish, A.V. Mazin

# MODEL STUDIES OF FIBER-OPTICAL COMMUNICATION CHANNELS IN QUANTUM CRYPTOGRAPHIC SYSTEMS

Dedicated to model studies of fiber-optic communication channels (FOCC) in quantum cryptographic systems (QCS). There are two main problems with the use of QCS related to the reliability of information transfer. The analysis of the energy loss factors in the classical fiber-optic channel has been carried out and the additive loss formula in it is discussed in detail. The fiber-optic channel of quantum information transmission using integrated optical devices is considered. The additive formula of optical losses in such a channel is discussed. The features of losses in integrated optical devices are shown, in particular light attenuation in optical fiber, losses on bends and micro-bends, technological, dispersion and transition losses. The features of quantum cryptographic system of information transmission are characterized. For example, when constructing a model of a photo detector, three main parameters are taken into account: quantum efficiency, speed, noise level. As a result, the model of FOCC QCS taking into account energy losses is proposed, which allows competently in theoretical terms and visualize the passage of information through modern quantum cryptographically secure telecommunications while providing control in government structures.

*Keywords:* modeling, fiber-optic channel, communication, quantum cryptographic system, energy losses, protected communications.

*Введение*

Существующие методы доставки информации до стратегического и тактического звена управления многих государственных структур дороги и не всегда надежны, не обеспечивают достаточной оперативности. Во многом в связи с этим в последние годы активно развиваются направления, относящиеся к разработке квантовых криптографических систем (ККС) [1].

Однако существует ряд теоретических и практических проблем использования ККС, связанных с достоверностью передачи информации [7]. В частности, известные волоконно-оптические каналы связи (ВОКС) не предназначены для передачи однофотонных сигналов [10], что приводит к сложностям их криптографической защиты [6]. Другой проблемой выступает учет энергетических потерь и ошибок при оценке характеристик передачи информации [3].

Целью настоящей статьи является построение модели ВОКС ККС с учетом энергетических потерь.

*Анализ энергетических потерь в волоконно-оптическом канале*

В классической волоконно-оптической системе передачи информации ряд традиционных компонентов может быть заменен на интегрально-оптические устройства, позволяющие повысить достоверность передачи информации по ВОКС ККС за счет решения следующих технических проблем: достижения идентичности оптических путей интерферирующего излучения с точностью до долей длины волны, уменьшения дрейфа фазы, поляризационного согласования интерферирующего излучения.

В ВОКС ККС с фазовым кодированием применяются оптические фазовые модуляторы, достоверность передачи информации по которым можно повысить с помощью применения технологий интегральной оптики. Кроме того, в качестве оптических распределителей в них используются интегрально-оптические коммутаторы. Для увеличения длины волоконно-оптического кабеля могут быть применены квантовые повторители, а для управления поляризацией излучения в систему введен поляризационный расщепитель, который может быть изготовлен на основе технологий интегральной оптики.

Проанализируем потери, возникающие в классическом ВОКС. Модель энергетических потерь представляется следующим выражением [4]:

$$A_{ОС} = A_{ВВ} + A_{ИЗГ} + A_{С} + A_{Д} + A_{ТЕХ} + A_{ВЫВ} + A_{Э} + A_{АДД}, \quad (1)$$

где $A_{ОС}$ – общие потери системы связи; $A_{ВВ}$ – потери при вводе излучения в оптическое волокно; $A_{ИЗГ}$ – потери на изгибах и микроизгибах; $A_{С}$ – потери в соединениях оптических волокон; $A_{Д}$ – дисперсионные потери; $A_{ТЕХ}$ – технологические потери; $A_{ВЫВ}$ – потери при выводе излучения из волокна; $A_{Э}$ – энергетический запас; $A_{АДД}$ – аддитивные переходные помехи, возникающие в многоволоконном оптическом кабеле.

Энергетический запас $A_{Э}$ включает потери за счет флуктуации фазы и поляризации оптического излучения [Там же]:

$$A_{Э} = A_{Ф} + A_{П}. \quad (2)$$

Для волоконно-оптического тракта передачи квантовой информации с применением интегрально-оптических устройств модель оптических потерь несколько отличается:

$$A_{ОС} = A_{ВВ} + A_{ИЗГ} + A_{ЛЗ} + A_{ПР} + A_{С} + A_{Д} + A_{ТЕХ} + A_{ВЫВ}, \quad (3)$$

где $A_{ЛЗ}$ – потери в линиях задержки интегрально-оптического интерферометра; $A_{ПР}$ – потери в интегрально-оптическом поляризационном расщепителе.

Отметим, что потери оптического излучения в интегрально-оптических устройствах выше, чем в волоконно-оптических [2], поэтому особенно необходимо учитывать потери интерферометров у передатчика и приемника ключа, а также потери в изогнутых волноводах линии задержки. Однако при использовании интегрально-оптических устройств можно пренебречь дрейфом фазы и флуктуациями поляризации излучения, поскольку в ВОКС ККС обычно применяются одноволоконные оптические кабели, что дает возможность пренебречь аддитивными переходными помехами.

Свет по мере распространения в оптическом волокне (ОВ) постепенно ослабевает. Затухание светового сигнала определяется по следующей формуле [8]:

$$\alpha = \frac{10}{l}\lg\left(\frac{P_{\text{вх}}}{P_{\text{вых}}}\right), \tag{4}$$

где $\alpha$ – затухание сигнала, дБ/км; $l$ – длина световода; $P_{\text{вх}}$ – мощность светового сигнала на входе ОВ; $P_{\text{вых}}$ – мощность светового сигнала на выходе ОВ.

Технологические потери $A_{\text{ТЕХ}}$ обусловлены непостоянством размеров поперечных сечений сердцевины ОВ по длине и неровностями границы раздела «сердцевина – оболочка». Они включают три составляющие: ослабление за счет поглощения; ослабление за счет наличия в материале ОВ постоянных примесей; ослабление за счет потерь на рассеяние. Технологические потери рассчитываются по следующей формуле [Там же]:

$$A_{\text{ТЕХ}} = \alpha l. \tag{5}$$

На изгибах, обусловленных скруткой ОВ вдоль оси оптического кабеля, нарушается условие полного внутреннего отражения. Луч при этом преломляется и рассеивается в окружающем пространстве (оболочке).

Потери от микроизгибов возникают в результате случайных отклонений волокна от его прямолинейности. Размах таких отклонений составляет менее 1 мкм, а протяженность – менее миллиметра. Подобные отклонения могут появляться в процессе наложения защитного покрытия и изготовления из стекловолокон кабеля, в результате температурных расширений и сжатий непосредственно волокна и защитных покрытий. Потери от изгибов рассчитываются по формуле [Там же]

$$A_{\text{ИЗГ}} = -10\lg\left(1 - \frac{\alpha n_1}{R(n_1 - n_2)}\right), \tag{6}$$

где $R$ – радиус изгиба волокна; $n_1$ – показатель преломления оболочки волокна; $n_2$ – показатель преломления сердцевины волокна.

Потери энергии существенно возрастают из-за наличия в материале ОВ примесей, таких как ионы металлов *Fe, Ni, Cr, V, Cu*, и других включений. Более существенной в отношении поглощения примесью являются ионы $OH^-$. Содержание ионов $OH^-$ в стекле связано с технологией его изготовления.

Рассеяние света в оптоволоконном световоде в основном обусловлено наличием в материале сердечника мельчайших (около одной десятой доли длины волны) случайных неоднородностей. Эти неоднородности рассеивают свет во всех направлениях. Согласно закону Рэлея с увеличением длины волны потери от рассеяния уменьшаются. Оно обратно пропорционально четвертой степени длины волны.

Кроме вышеперечисленных потерь необходимо учитывать потери $A_{ВВ}$, возникающие при вводе излучения в ОВ. К ним относятся апертурные потери, обусловленные несовпадением апертур излучателя и световода; френелевские потери на отражение от торцов световода.

Особую составляющую потерь представляют дисперсионные. В ступенчатых одномодовых ОВ проявляется хроматическая дисперсия (волноводная и материальная), они почти равны по абсолютной величине и противоположны по фазе в широком спектральном диапазоне при $\lambda = 1{,}2 \div 1{,}7$ мкм [9].

Возникновение хроматической дисперсии в материале световода обусловлено тем, что оптический источник, возбуждающий вход ОВ, формирует световые импульсы, имеющие непрерывный волновой спектр определенной ширины. Различные спектральные компоненты импульса распространяются с разными скоростями и приходят к концу волокна в разное время, приводя к уширению импульса на выходе. Дисперсионные потери описываются выражением [4]

$$A_{Д} = 2\left(\frac{t_e}{T}\right), \tag{7}$$

где $t_e$ – ширина оптического импульса на уровне $1/e$ ($e$ – основание натурального логарифма); $T$ – длительность тактового интервала.

Для оценки ширины оптического импульса в тракте волоконно-оптической системы необходимо учесть материальную дисперсию как составную часть хроматической дисперсии. Тогда рассчитать ширину оптического импульса на уровне $1/e$ можно по формуле [9]

$$A(t)_{вых} = \frac{\sqrt{P_{вх}}}{\sqrt[4]{1+\dfrac{t\lambda^2 M_{хр}}{2\pi t_{вх}^2}}} \exp\left(-\frac{t^2}{2t_{вых}^2}\right), \tag{8}$$

где $A(t)_{вых}$ – огибающая гауссового импульса на выходе; $\lambda$ – длина волны излучения; $M_{хр}$ – величина хроматической дисперсии; $t_{вх}$ – длительность импульса на входе линии связи; $t_{вых}$ – длительность импульса на выходе линии связи.

*Особенности квантово-криптографической системы передачи информации*

При построении модели фотоприемного устройства ВОКС ККС необходимо учесть, что фотоприемники в ВОКС характеризуются прежде всего тремя основными параметрами: квантовой эффективностью, быстродействием, уровнем шумов [12].

Квантовая эффективность лавинных фотодиодов, применяемых в системах квантовой криптографии, определяется так же, как у обычных фотодиодов. Отношение фототока (числа электронов, поступающих во внешнюю цепь в секунду) к числу падающих фотонов называется квантовой эффективностью $\eta_ф$ [Ibid.]:

$$\eta_ф = \frac{I_ф / e}{N}, \tag{9}$$

где $I_ф$ – сила фототока; $e$ – заряд электрона; $N$ – число фотонов.

Для создания тракта волоконно-оптической системы передачи квантовой криптографии применяются однофотонные детекторы, регистрирующие результат интерференции

амплитуд двух возможных переходов фотона по ВОКС ККС. Такие фотодетекторы обладают высокой вероятностью темнового отсчета (ложное срабатывание, когда фотон не детектирован), поэтому оценкой однофотонного детектора может выступать понятие энергии шумового эквивалента (*NEP*) [12]:

$$NEP = \frac{h\nu}{\eta}(2P)^{\frac{1}{2}}, \tag{10}$$

где $h = 6{,}626\,070\,040(81) \cdot 10^{-34}$ Дж · с – постоянная Планка; ν – частота приходящих фотонов; η – эффективность детектирования; $P$ – вероятность темнового отсчета.

При расчете скорости передачи ключа по ВОКС ККС необходимо учитывать процедуры коррекции ошибок и усиления скрытности. Число потерянных битов из-за коррекции ошибок длинных (более 100 бит) цепочек символов как функции квантового коэффициента ошибки QBER определяется как [13]

$$r_{ec} = QBER(3{,}5 - QBER). \tag{11}$$

Доля потерь битов, связанных с введением процедуры усиления скрытности, определяется по формуле [Ibid.]

$$r_{pa} = \log_2(1 + 4QBER(1 - QBER)). \tag{12}$$

Окончательно скорость передачи информации в ККС после обработки будет определяться выражением [Ibid.]

$$B = (1 - r_{ec})(1 - r_{pa})V. \tag{13}$$

Скорость передачи $V$ (число битов, переданных в секунду) без дополнительной процедуры коррекции ошибок дается выражением [Ibid.]

$$V = q\mu\nu\eta_{\text{ф}}\eta_t, \tag{14}$$

где $q$ – системный фактор, зависящий от выбранного варианта технической реализации (он не может быть больше чем 0,5 по той причине, что половину времени выбираемые случайным образом базисы передатчика и приемника несовместимы); μ – среднее число фотонов на импульс; ν – частота импульсов излучения; $\eta_{\text{ф}}$ и $\eta_{\text{t}}$ – эффективность детектора и передачи соответственно.

Для построения модели квантового коэффициента ошибки тракта волоконно-оптической системы передачи квантовой криптографии используется соотношение [5]

$$QBER = QBER_{opt} + QBER_{det}. \tag{15}$$

Из (15) следует, что квантовый коэффициент ошибки состоит из двух частей: первая часть $QBER_{opt}$ зависит от части фотонов, чья поляризация или фаза определены неверно. Вторая часть $QBER_{det}$ вызвана темновыми отсчетами фотодетектора. Данное слагаемое будет определяющим для больших длин волоконной линии связи. Скорость темнового отсчета в комбинации с потерями в оптоволокне ограничивает длину линии связи:

$$QBER_{det} = \frac{\eta_{dark}\Delta t}{\mu\eta_t\eta_{\text{ф}}}, \tag{16}$$

где $\eta_{dark}$ – скорость темновых отсчетов; $\Delta t$ – временное окно детектирования.

В отличие от классического тракта волоконно-оптической системы при расчете входящего в формулу параметра эффективности передачи необходимо учитывать энергети-

ческие потери излучения на стороне приемника информации, которые входят в формулу эффективности передачи. Эффективность передачи в ВОКС ККС можно представить как [5]

$$\eta_t = 10\frac{-(\alpha l + L_B)}{10}, \qquad (17)$$

где $L_B$ – оптические потери на стороне аппаратуры приемника.

Таким образом, применительно к ВОКС ККС обоснована и построена модель энергетических потерь, скорости передачи информации, квантового коэффициента ошибки и эффективности передачи в ВОКС ККС.

*Выводы*

1. С учетом того что существующие методы доставки информации до стратегического и тактического звена управления многих государственных структур дороги, не всегда надежны и оперативны [11], в последние годы активно разрабатываются ККС.

2. Имеются теоретические и практические проблемы использования ВОКС ККС, связанные с достоверностью передачи информации. В частности, существующие волоконно-оптические каналы связи не предназначены для передачи однофотонных сигналов, что приводит к сложностям их криптографической защиты; кроме того, недостаточно проработан в методическом плане учет энергетических потерь и ошибок при оценке характеристик передачи информации в ВОКС ККС.

3. Обоснованная и построенная модель ВОКС ККС с учетом энергетических потерь позволяет теоретически грамотно и наглядно представить прохождение информации через современные квантово-криптографически защищенные телекоммуникации при обеспечении управления государственных структур.

## Литература

1. *Алиев Ф.К., Бородин А.М., Вассенков А.В., Матвеев Е.А., Царьков А.Н., Шеремет И.А.* О способе дистанционного изменения меры несепарабельности квантовых систем и возможности его применения в области связи // Известия Института инженерной физики. 2014. № 3 (33). С. 30–38.

2. *Векшин М.М., Захаров В.В., Никитин В.А., Прохоров В.П., Шевченко А.В., Яковенко Н.А.* Новые элементы интегральной оптики для сбора и обработки информации // Труды Международного форума по проблемам науки, техники и образования. М., 1997. С. 55–57.

3. *Гладкий В.П., Никитин В.А., Прохоров В.П., Яковенко Н.А.* Элементы волноводной оптоэлектроники для устройств функциональной обработки цифровой информации // Квантовая электроника. 1995. № 10. С. 1027–1033.

4. *Горлов Н.И., Богачков И.В.* Волоконно-оптические линии передачи. Методы и средства измерений параметров. – М.: Радиотехника, 2009. 192 с.

5. Квантовая криптография: идеи и практика / под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. Минск: Беларуская навука, 2007. 391 с.

6. *Килин С.Я.* Квантовая информация // Успехи физических наук. 1999. № 5, Т. 169. С. 507–525.

7. *Ненадович Д.М.* Методологические аспекты экспертизы телекоммуникационных проектов. – М.: Горячая линия-Телеком, 2008. 280 с.

8. *Рассел Дж.* Волоконно-оптическая линия передачи. М.: Книга по Требованию, 2013. 112 с.

9. *Скляров О.К.* Волоконно-оптические сети и системы связи. М.: Лань, 2010. 272 с.
10. Физика квантовой информации. Квантовая криптография. Квантовая телепортация. Квантовые вычисления / под ред. Д. Боумейстера, А. Экерта, А. Цайлингера; пер. с англ. под ред. С.П. Кулика, Т.А. Шмаонова. М.: Постмаркет, 2002. 376 с.
11. *Фисун А.П., Касилов А.Г., Фисенко В.Е., Минаев В.А., Афанасьев В.В., Митяев В.В., Фисун Р.А., Джевага К.А., Кожухов С.А.* Развитие методологических основ информатики и информационной безопасности систем. Орел: Орловский государственный университет, 2004. 253 с. Деп. в ВИНИТИ 07.07.2004, № 1165-В2004.
12. *Egorov V.I., Vavulin D.N., Latypov I.Z., Gleim A.V., Rupasov A.V.* Analysis of a Sidebands-Based Quantum Cryptography System with Different Detector Types // Nanosystems: Physics, Chemistry, Mathematics. 2013. № 4 (2). P. 190–195.
13. *Strenzke F., Tews E., Molter H., Overbeck R., Shoufan A.* Side Channels in the McEliece PKC // Post-Quantum Cryptography. PQCrypto: Lecture Notes in Computer Science. Berlin: Heidelberg Springer, 2008. Vol. 5299. P. 216–229.

## Literatura

1. *Aliev F.K., Borodin A.M., Vassenkov A.V., Matveev E.A., Car'kov A.N., Sheremet I.A.* O sposobe distancionnogo izmeneniya mery neseparabel'nosti kvantovyh sistem i vozmozhnosti ego primeneniya v oblasti svyazi // Izvestiya Instituta inzhenernoj fiziki. 2014. № 3 (33). S. 30–38.
2. *Vekshin M.M., Zaharov V.V., Nikitin V.A., Prohorov V.P., Shevchenko A.V., Yakovenko N.A.* Novye ehlementy integral'noj optiki dlya sbora i obrabotki informacii // Trudy Mezhdunarodnogo foruma po problemam nauki, tekhniki i obrazovaniya. M., 1997. S. 55–57.
3. *Gladkij V.P., Nikitin V.A., Prohorov V.P., Yakovenko N.A.* Ehlementy volnovodnoj optoehlektroniki dlya ustrojstv funkcional'noj obrabotki cifrovoj informacii // Kvantovaya elektronika. 1995. № 10. S. 1027–1033.
4. *Gorlov N.I., Bogachkov I.V.* Volokonno-opticheskie linii peredachi. Metody i sredstva izmerenij parametrov. M.: Radiotekhnika, 2009. 192 s.
5. Kvantovaya kriptografiya: idei i praktika / pod red. S.Ya. Kilina, D.B. Horoshko, A.P. Nizovceva. Minsk: Belaruskaya navuka, 2007. 391 s.
6. *Kilin S.Ya.* Kvantovaya informaciya // Uspekhi fizicheskih nauk. 1999. № 5, T. 169. S. 507–525.
7. *Nenadovich D.M.* Metodologicheskie aspekty ehkspertizy telekommunikacionnyh proektov. M.: Goryachaya liniya-Telekom, 2008. 280 s.
8. *Rassel Dzh.* Volokonno-opticheskaya liniya peredachi. M.: Kniga po Trebovaniyu, 2013. 112 s.
9. *Sklyarov O.K.* Volokonno-opticheskie seti i sistemy svyazi. M.: Lan', 2010. 272 s.
10. Fizika kvantovoj informacii. Kvantovaya kriptografiya. Kvantovaya teleportaciya. Kvantovye vychisleniya / pod red. D. Boumejstera, A. Ehkerta, A. Cajlingera; per. s angl. pod red. S.P. Kulika, T.A. Shmaonova. M.: Postmarket, 2002. 376 s.
11. *Fisun A.P., Kasilov A.G., Fisenko V.E., Minaev V.A., Afanas'ev V.V., Mityaev V.V., Fisun R.A., Dzhevaga K.A., Kozhuhov S.A.* Razvitie metodologicheskih osnov informatiki i informacionnoj bezopasnosti system. Orel: Orlovskij gosudarstvennyj universitet, 2004. 253 s. Dep. v VINITI 07.07.2004, № 1165-V2004.
12. *Egorov V.I., Vavulin* D.N., *Latypov I.Z., Gleim* A.V., *Rupasov A.V.* Analysis of a Sidebands-Based Quantum Cryptography System with Different Detector Types // Nanosystems: Physics, Chemistry, Mathematics. 2013. № 4 (2). P. 190–195.
13. *Strenzke F., Tews E., Molter H., Overbeck* R., *Shoufan A.* Side Channels in the McEliece PKC // Post-Quantum Cryptography. PQCrypto: Lecture Notes in Computer Science. Berlin: Heidelberg Springer, 2008. Vol. 5299. P. 216–229.