5. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 27.12.2018).– URL: http://www.consultant.ru/document/cons_doc_LAW_34683/98b31fb9ec68d01fefb5bb66cad3bfa2c9705789/.

6. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 27.12.2018).– URL: http://www.consultant.ru/document/cons_doc_LAW_34683/0bcb36bb1684e9183927055e83f44ce0bac15487/.

7. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 27.12.2018).– URL: http://www.consultant.ru/document/cons_doc_LAW_34683/b94bd4dad3b39d0497eb33b8fc3d99356959c2da/.

8. Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_48699/.

УДК 535.14

ОСОБЕННОСТИ ИССЛЕДОВАНИЯ ВОЛОКОННО-ОПТИЧЕСКИХ КАНАЛОВ КОММУНИКАЦИИ В КВАНТОВЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

В А. Минаев
доктор технических наук, профессор
Московский государственный технический университет им. Н. Э. Баумана
E-mail:m1va@yandex.ru

И.Д. Королев
доктор технических наук, профессор
Краснодарское высшее военное училище им. генерала армии С. М. Штеменко
E-mail: pi_korolev@mail.ru

М.П. Сычев
доктор технических наук, профессор
Московский государственный технический университет им. Н. Э. Баумана
E-mail: mpsichov@sm.bmstu.ru

О.А. Кулиш
кандидатфизико-математических наук, доцент
Краснодарское высшее военное училище им. генерала армии С. М. Штеменко
E-mail:culish_olga@mail.ru

Аннотация. Существующие методы доставки информации до стратегического и тактического звена управления многих государственных структур дороги не всегда надежны и оперативны. Поэтому в последние годы активно разрабатываются квантовые криптографические системы (ККС). В работе производится анализ факторов энергетических потерь в классическом волоконно-оптическом канале. Затем рассмотрен волоконно-оптический канал передачи квантовой информации с применением интегрально-оптических устройств.

Ключевые слова: волоконно-оптический канал, квантовая криптографическая система, энергетические потери.

PECULIAR PROPERTIES OF FIBER-OPTICAL COMMUNICATION CHANNELS STUDIES IN QUANTUM CRYPTOGRAPHIC SYSTEMS

V.A. Minaev, I.D. Korolev, M.P. Sychev, O.A. Kulish

Abstract. The existing methods of information delivery to the strategic and tactical management of many government agencies are expensive, not always reliable and efficient. Therefore, quantum cryptographic systems (QCS) have been actively developed in recent years. In article the analysis of the energy loss factors in the classical fiber-optic channel is carried out. Then we consider the fiber-optic channel of quantum information transmission with the use of integrated optical devices.

Keywords: fiber-optic channel, quantum cryptographic system, energy losses.

Введение

Существующие методы доставки информации до стратегического и тактического звена управления многих государственных структур дороги и не всегда надежны, к тому же не обеспечивают достаточной оперативности. Во многом в этой связи 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 [2]. В частности, существующие волоконно-оптические каналы связи(ВОКС) не предназначены для передачи однофотонных сигналов [3], что приводит к сложностям их криптографической защиты [4]. Другой проблемой выступает учет энергетических потерь и ошибок при оценке характеристик передачи информации [5].

Целью настоящей работы 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: достижение идентичности оптических путей интерферирующего излучения с точностью до долей длины волны, уменьшение дрейфа фазы, поляризационное согласование 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 выражением [6]:

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

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 [6]:

$$A_{Э} = A_{Ф} + A_{П}. \quad (2)$$

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 [7], 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 формуле [8]:

$$\alpha = \frac{10}{l} \cdot lg\left(\frac{P_{вх}}{P_{вых}}\right), \text{ дБ/км}, \quad (4)$$

где α – затухание сигнала, l – длина световая, $P_{вх}$ – мощность светового сигнала на входе ОВ; $P_{вых}$ – мощность светового сигнала на выходе ОВ.

Технологические потери A_{TEX} обусловлены непостоянством размеров поперечных сечений сердцевины ОВ по длине и неровностями границы раздела сердцевина-оболочка. Они состоят из трех составляющих: ослабление за счёт поглощения; ослабление за счёт наличия в материале ОВ постоянных примесей; ослабление за счёт потерь на рассеяние. Технологические потери рассчитываются по формуле [8]:

$$A_{\text{ТЕХ}} = \alpha \cdot l. \quad (5)$$

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 [8]:

$$A_{\text{изг}} = -10lg \cdot \left(1 - \frac{\alpha \cdot n_1}{R \cdot (n_1 - n_2)}\right) \quad (6)$$

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 выше перечисленных потерь, необходимо учитывать потери A_{BB}, 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 λ = 1,2 ÷ 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 [6]:

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

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 дисперсии как составную часть хроматической дисперсии. Тогда рассчитать ширину оптического импульса на уровне $1/e$ можно по формуле [9]:

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

где $A(t)_{вых}$– огибающая гауссового импульса на выходе, λ – длина волны излучения, – 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 фотоприёмного устройства ВОКС ККС необходимо учесть, что фотоприемники в ВОКС характеризуются, прежде всего, тремя основными параметрами: квантовой эффективностью, быстродействием, уровнем шумов [10].

Квантовая эффективность лавинных фотодиодов, применяемых в системах квантовой криптографии определяется также, как у обычных фотодиодов. Отношение фототока (числа электронов, поступающих во внешнюю цепь в секунду) к числу падающих фотонов называется квантовой эффективностью $\eta_ф$ [10]:

$$\eta_{\Phi} = \frac{I_{\Phi}/e}{N} \quad , \tag{9}$$

где I_{Φ} – 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*) [10]:

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

где h = 6,626 070 040(81) × 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 бит из-за коррекции ошибок длинных (более 100 бит) цепочек символов как функции квантового коэффициента ошибки QBER определяется как [11]:

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

Доля потерь бит, связанных с введение процедуры усиления скрытности, определяетсяпоформуле [11]:

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

Окончательно скорость передачи информации в ККС после обработки будет определяться выражением [11]:

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

Скорость передачи V (число бит, переданных в секунду) без дополнительной процедуры коррекции ошибок дается выражением [11]:

$$V = q\mu\nu\eta_{\Phi}\eta_t \tag{14}$$

где источник ν – частота импульсов излучения; μ – среднее число фотонов на импульс; η_{ϕ} и η_t – эффективности детектора и передачи, соответственно; 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.

Для построения модели квантового коэффициента ошибки тракта волоконно-оптической системы передачи квантовой криптографии используется соотношение [12]:

$$QBER = QBER_{opt} + QBER_{\text{det}} \quad (15)$$

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 $QBER_{\text{det}}$ 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.

$$QBER_{det} = \frac{\eta_{dark}\Delta t}{\mu \eta_t \eta_\phi}, \quad (16)$$

где η_{dark} – скорость темновых отсчетов, Δt – временное окно детектирования.

В отличие от классического тракта волоконно-оптической системы при расчете входящего в формулу параметра эффективности передачи необходимо учитывать энергетические потери излучения на стороне приемника информации, которые входят в формулу эффективности передачи.

Эффективность передачи в ВОКС ККС можно представить как [12]:

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

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 [13], в последние годы активно разрабатываются квантовые криптографические системы.

2. Имеются теоретические и практические проблемы использования ВОКС ККС, связанных 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

методически проработан 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 квантовыхсистем и возможности его применения в области связи // Известия Института инженерной физики. 2014. № 3(33). – С.30-38.
2. *Ненадович Д.М.* Методологические аспекты экспертизы телекоммуникационных проектов. М.: Горячая линия-Телеком, 2008. 280 с.
3. 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 и Т.А. Ашманова. М.: Постмаркет, 2002. 376 с.
4. *Килин С.Я.* Квантовая информация // Успехи физических наук. 1999. № 5. Т. 169. С. 507−525.
5. *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.
6. *Горлов Н.И., Богачков И.В.* Волоконно-оптические линии передачи. Методы и средства измерений параметров. М.: Радиотехника, 2009. – 192 с.
7. *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.
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. *EgorovV.I., Vavulin D.N., LatypovI. Z., Gleim A.V., Rupasov A.V.* Analysis of a Sidebands-based Quantum Cryptography System with Different Detector Types // Nanosystems: Physics, Chemistry, Mathematics. 2013. No 4(2). P. 190-195.
11. 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. Vol. 5299. Berlin: Heidelberg Springer, 2008. – Pp. 216-229.
12. Квантовая криптография: идеи и практика / Под ред. С.Я. Килина, Д.Б. Хорошко, А.П. Низовцева. Минск: Беларуская навука, 2007. 391с.
13. *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. Депонированная рукопись. № 1165-В2004. Место депонирования: ВИНИТИ Дата депонирования: 07.07.2004. Орел: Орловский гос. ун-т, 2004. 253 с.