



К.Е. Румянцев  
Н. Н. Shakir

# Проектирование системы квантового распределения ключа с интерферометрами Маха-Цендера

учебное пособие



УДК 621.391.64  
ББК 32.875я73-5  
Р865

*Печатается по решению кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности Южного федерального университета (протокол № 10 от 15 января 2020 г.)*

**Рецензенты:**

заместитель директора по научной работе Ростовского филиала Российской таможенной академии, заслуженный деятель науки РФ, доктор технических наук, профессор *Д. А. Безуглов*  
профессор кафедры «Антенны и радиопередающие устройства» Южного федерального университета, заслуженный работник высшей школы РФ, доктор технических наук, профессор *В. А. Обуховец*

**Румянцев, К. Е.**

Р865 Проектирование системы квантового распределения ключа с интерферометрами Маха – Цендера : учебное пособие / К. Е. Румянцев, Н. Н. Shakir ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. – 108 с.

ISBN 978-5-9275-3560-6

Пособие посвящено проектированию системы квантового распределения ключа по протоколу B92 с интерферометрами Маха – Цендера. Система содержит оптический однофотонный передатчик на станции Алиса и оптический однофотонный приёмник на станции Боб. Оптический передатчик и приёмник соединены волоконно-оптической линией связи на основе одномодового оптического волокна Coming®SMF-28e®ULL. В проектируемой системе для формирования и приёма квантового импульса используется ослабленный лазерный импульс.

Учебное пособие готовит студента к разработке нормативной, технической и отчётной документации, представлять результаты профессиональной деятельности с использованием стандартов, норм и правил. Проектирование системы квантового распределения ключа по протоколу B92 с интерферометрами Маха – Цендера требует от студента анализа и учёта текущего состояния и тенденций развития технических средств защиты информации, сетей и систем передачи информации при решении задач профессиональной деятельности.

Пособие предназначено для студентов специальности 10.05.02 «Информационная безопасность телекоммуникационных систем». Пособие полезно для подготовки дипломированных специалистов по специальностям и направлению укрупнённой группы 10.00.00 «Информационная безопасность».

УДК 621.391.64  
ББК 32.875я73-5

ISBN 978-5-9275-3560-6

© Южный федеральный университет, 2020  
© Румянцев К. Е., Shakir Н. Н., 2020  
© Оформление. Макет. Издательство Южного федерального университета, 2020

# 1. ПАРАМЕТРЫ ПРИМЕНЯЕМЫХ ОДНОМОДОВЫХ ОПТИЧЕСКИХ ВОЛОКОН

## 1.1. Параметры одномодового оптического волокна на станциях

Внутри оптического однофотонного передатчика на станции Алиса и оптического однофотонного приёмника на станции Боб ориентируемся на применение одномодового оптического волокна, сохраняющего состояние поляризации (PMF – Polarization Maintaining Fiber). В системах КРК с длиной волны 1550 нм применяется PM – волокно типа «Панда» (Panda). Это волокно отличается от обычного волокна тем, что внутри оболочки с двух сторон от сердцевины симметрично вдоль всей длины волокна проходят два стержня для внесения искусственной анизотропии для подавления перекрёстного смешивания мощности двух перпендикулярно поляризованных мод. За счёт этого перераспределение энергии между модами быстрого и медленного главных состояний поляризации (явление связывания мод) сведено к минимуму.

Выбор останавливаем на оптических волокнах Panda с сохранением поляризации IXF-PMG-1550-125-P [13] компании IxBlue (рис. 1.1).



**Рис. 1.1.** Оптическое волокно Panda IXF-PMG-1550-125-P

Волокно специально разработано для применения в космических условиях. Специально подобранный химический состав стекла, правильный выбор исходных материалов гарантируют очень низкую чувствительность к изменениям температуры. Контроль диаметра оболочки волокна (40, 80, 125 мкм) очень важен во время намотки его на катушку при изготовлении ВОЛЗ. Оптические волокна демонстрируют высокую стабильность диаметра покрытия ( $170 \pm 2$  мкм и  $120 \pm 2$  мкм для серии LS) каждой партии.

Технические параметры оптического волокна Panda с сохранением поляризации IXF-PMF-1550-125-P представлены в табл. 1.1.

Таблица 1.1

**Параметры волокна с сохранением поляризации IXF-PMG-1550-125-P**

Параметр	Значение
Центральная длина волны излучения, нм	1550
Длина волны отсечки, нм	менее 1480
Числовая апертура	0,12± 0,02
Диаметр поля моды, мкм	10±1,0
Погонное затухание, дБ/км	не более 1
Неконцентричность оболочки сердцевины, мкм	не более 1,0
Диаметр отражающей оболочки, мкм	125±1,0
Диаметр покрытия, мкм	250±15
Длина биения, мм	менее 5
Перекрёстные помехи, дБ	минус 25

Эффективный показатель преломления в сердцевине одномодового оптического волокна с сохранением поляризации Panda принимаем равным  $n_{PMF} = 1,468$  для излучения с длиной волны 1550 нм [14]. Скорость распространения фотона в оптическом волокне  $v_{PMF}$  определяется формулой

$$v_{PMF} = \frac{c_{opt}}{n_{PMF}} = \frac{300000}{1,468} \approx 204\,360 \frac{\text{км}}{\text{с}},$$

где  $c_{opt} = 300\,000$  км/с – скорость оптического излучения в вакууме.

При введении поляризованного излучения в PM-волокно вдоль одной из осей, на выходе получим строго поляризованный сигнал без эффекта уширения.

**1.2. Параметры оптического волокна Corning®SMF-28e®ULL**

Оптические передатчик и приёмник соединены волоконно-оптической линией связи (TF – Transmission Fiber) 3 на основе одномодового оптического волокна (SMF – Single Mode Fiber) Corning® SMF-28® ULL (далее SMF-28 ULL).

Оптическое волокно Corning® SMF-28® ULL соответствует требованиям отраслевого стандарта ITU-T G.652 [14]. Волокно имеет наименьшее затухание и поляризационную модовую дисперсию среди оптических волокон класса Corning® SMF-28 (рис. 1.2).

На длине волны 1550 нм максимальное значение коэффициента затухания оптического волокна составляет 0,17 ... 0,18 дБ/км при максимальном стандартном отклонении коэффициента затухания не более 0,02 дБ/км.



**Рис. 1.2.** Оптическое волокно Corning® SMF-28® ULL [15]

Потери мощности излучения на макроизгибах за счёт намотки ста витков волокна SMF-28 ULL на оправку диаметром 32 мм не превышают 0,05 дБ.

Значение диаметра поля моды волокна равно  $10,7 \pm 0,5$  мкм.

Коэффициент хроматической дисперсии не превышает 18,0 пс/(нм·км).

Длина волны нулевой дисперсии  $\lambda_0 = 1304 \dots 1324$  нм.

Наклон дисперсионной характеристики в области длины волны нулевой дисперсии  $S_0$  не превышает 0,092 пс/(нм<sup>2</sup>·км).

Коэффициент хроматической дисперсии при произвольной рабочей длине волны  $\lambda$  в диапазоне 1200 ... 1625 нм может быть рассчитан по формуле

$$K_{\text{хр.д}} = \frac{S_0}{4} \cdot \left( \lambda - \frac{\lambda_0^4}{\lambda^3} \right). \quad (1.1)$$

Коэффициент ПМД ООВ протяжённой линии не превышает 0,04 пс/ $\sqrt{\text{км}}$ , причём его максимальное значение меньше 0,10 пс/ $\sqrt{\text{км}}$ .

**Геометрические размеры ООВ SMF-28 ULL.** Радиус изгиба ОВ должен превышать 4,0 мм. Диаметр оболочки равен  $D_{\text{об}} = 125,0 \pm 0,7$  мкм.

Некруглость оболочки не превышает 0,7 %, а неконцентричность сердцевин и оболочки – 0,5 мкм. Диаметр защитного покрытия  $D_{\text{покр}} = 245,0 \pm 5$  мкм. Неконцентричность защитного покрытия не превышает 12 мкм.

**Воздействие окружающей среды на волокно SMF-28 ULL.** Рабочий диапазон температур – от минус 60 до плюс 85 °С. Приращение затухания на длине волны 1550 нм меньше 0,05 дБ/км в рабочем диапазоне температур.

**Рабочие характеристики волокон SMF-28 ULL.** Диаметр сердцевин – 8,2 мкм. Числовая апертура  $NA = 0,14$ . Длина волны нулевой дисперсии  $\lambda_0 = 1317$  нм. Наклон дисперсионной характеристики в области длины волны нулевой дисперсии  $S_0 = 0,088$  пс/(нм<sup>2</sup>·км). Разброс показателей преломления 0,36 %. Эффективный показатель преломления для группы равен 1,4677 для излучения с длиной волны 1550 нм. Коэффициент релеевского рассеяния при длительном воздействии равен минус 82 дБ для излучения с длиной волны 1550 нм. Порог рассеяния Мандельштама–Блиллюэна – 20 дБм. Коэффициент ПМД в индивидуальном волокне – 0,02 пс/ $\sqrt{\text{км}}$ .

Эффективный показатель преломления в сердечнике одномодового оптического волокна SMF-28 ULL равен  $n_{SMF} = 1,4682$  для излучения с длиной волны  $\lambda_s = 1550$  нм [14]. Скорость распространения фотона в оптическом волокне  $v_{SMF}$  определяется формулой

$$v_{SMF} = \frac{c_{opt}}{n_{SMF}} = \frac{300000}{1,4682} = 204\,332 \frac{\text{км}}{\text{с}}.$$

### 1.3. Параметры одномодовых оптических коннекторов

Одномодовые (SM) оптические коннекторы типа FC со скошенным торцом (полировка APC) предназначены для оконцевания оптического волокна диаметром 1,8; 2 и 3 мм [16], а также оптического волокна в буферном покрытии диаметром 0,9 мм (рис. 1.3). Коннекторы предназначены для оконцевания по технологии эпоксидной клеей.

Коннекторы с полировкой APC обеспечивают меньшее количество отражённого в сторону источника излучения. Благодаря скошенной под углом 8...9 градусов поверхностью ферулы, отражённое излучение практически не возвращается к передатчику. Минимальные возвратные потери составляют 60 дБ [16].



Рис. 1.3. Коннектор с полировкой APC [17]

Технические параметры одномодовых оптических коннекторов FC с полировкой APC представлены в табл. 1.2. Приведённые технические параметры достижимы при условиях применения соответствующей кабельной продукции и соблюдения технологических процессов.

Коннектор FC имеет керамический наконечник диаметром 2,5 мм, снабжён накидной гайкой с резьбой M8×0,75 для фиксации на розетке.

Соединения шнуров, оконцованных оптическими коннекторами FC через стандартную соединительную розетку, характеризуются высокой надёжностью, стойкостью к вибрации и одиночным ударам, так как наконечник коннектора не связан с корпусом и оболочкой кабеля.

Таблица 1.2

**Технические параметры одномодовых оптических коннекторов FC с полировкой APC**

Параметр	Значение
<b>Оптические характеристики</b>	
Прямые потери, дБ	типовые
	максимальные
	0,2
	0,4
Возвратные потери, дБ	типовые
	максимальные
	65
	60
<b>Механические характеристики</b>	
Число включений	1000
Вибрация с ускорением 4g, Гц	1...200
Удар (длительность импульса 18 мкс)	40g
Увеличение прямых потерь при механических воздействиях, дБ	менее 0,2
<b>Условия эксплуатации</b>	
Диапазон рабочих температур, °С <sup>1</sup>	– 40...+ 80
Атмосферное давление, кПа	26
Относительная влажность воздуха при температуре +25 °С, %	100

<sup>1</sup> В зависимости от характеристик оптического кабеля.

## 2. ПРОЕКТИРОВАНИЕ ИСТОЧНИКА ОДИНОЧНЫХ ФОТОНОВ

Проведённый анализ показывает, что источники одиночных фотонов всё ещё слишком сложны для использования в системах КРК. Кроме того, из-за низкой квантовой эффективности они не дают преимуществ по сравнению со слабым лазерным импульсом с чрезвычайно малым средним числом фотонов. Поэтому в проектируемой системе ориентируемся на формирование и приём квантового импульса, представляющего ослабленный лазерный импульс. Следовательно, анализируемый в дальнейшем однофотонный источник излучения представляет последовательно соединённые лазер 4 и регулируемый волоконно-оптический аттенуатор 5, как показано на рис. В.1. Отметим, что по ТЗ за длительность квантового импульса на выходе передающей станции среднее число регистрируемых фотонов не должно превышать 0,1.

### 2.1. Выбор передающего оптического модуля

В проектируемой системе КРК используем передающий оптический модуль ID300 фирмы ID Quantique на основе лазера с распределённой обратной связью (DFB-лазера). Внешний вид модуля показан на рис. 2.1.



Рис. 2.1. Внешний вид передающего оптического модуля ID300

Номенклатура изделия: **iD300-XXXX-YYY-ZZZ**,  
где XXXX – длина волны оптического излучения (1310 или 1550 нм);  
YYY – тип лазера (лазер с резонатором Фабри–Перро FB-лазера с распределённой обратной связью или DFB); ZZZ – триггерной вход для подачи управляющих импульсов. Выбор между NIM, ECL, PECL, LVPECL, TTL или TTL 50W.



В нашем случае выбор останавливаем на модуле iD300-1550-DFB-TTL 50W.

Производитель предусматривает использование оптического коннектора FC/APC с подключением оптического волокна, сохраняющего поляризацию (вывод PM/PM).

В качестве высокочастотного разъёма используется разъём типа BNC HYR-0101A (GB-101A) с монтажом на коаксиальный кабель RG-58 с волновым сопротивлением 50 Ом [18].

Модуль питается от источника переменного тока 220 В 50 Гц.

Параметры выбранного передающего оптического модуля ID300 отражены в табл. 2.1 [19].

Таблица 2.1

**Параметры передающего оптического модуля серии ID300 на основе лазера с распределённой обратной связью**

Параметр	Значение параметра
Длина волны излучения при температуре 25 °С, нм	
минимальное значение	1520
типовое значение	1550
максимальное значение	1580
Длительность импульса лазера при температуре 25 °С, пс	
типовое значение	300
максимальное значение	500
Частота следования импульсов лазера при температуре 25 °С, МГц	0 ... 500
Пиковая мощность излучения лазера в импульсе при температуре 25°С, мВт	
минимальное значение	0,7
типовое значение	1
Выходная мощность излучения лазера при температуре 25 °С и частоте следования импульсов лазера 1 МГц, дБм	
минимальное значение	минус 36
типовое значение	минус 35
максимальное значение	минус 34
Ширина спектра лазера на уровне минус 20 дБ при температуре 25° С, нм	
типовое значение	0,6

## СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ .....	3
СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ .....	4
ВВЕДЕНИЕ .....	6
1. ПАРАМЕТРЫ ПРИМЕНЯЕМЫХ ОДНОМОДОВЫХ ОПТИЧЕСКИХ ВОЛОКОН .....	12
1.1. Параметры одномодового оптического волокна на станциях	12
1.2. Параметры оптического волокна Corning®SMF-28e®ULL .....	13
1.3. Параметры одномодовых оптических коннекторов .....	15
2. ПРОЕКТИРОВАНИЕ ИСТОЧНИКА ОДИНОЧНЫХ ФОТОНОВ	17
2.1. Выбор передающего оптического модуля .....	17
2.2. Выбор волоконного поляризатора .....	25
2.3. Выбор регулируемого волоконно-оптического аттенюатора	26
3. ПРОЕКТИРОВАНИЕ ИНТЕРФЕРОМЕТРА МАХА – ЦЕНДЕРА ПЕРЕДАЮЩЕЙ СТАНЦИИ АЛИСА .....	31
3.1. Обоснование выбора волоконно-оптического разветвителя	32
3.2. Верхнее плечо первого интерферометра Маха – Цендера .....	35
3.3. Нижнее плечо первого интерферометра Маха – Цендера .....	40
3.4. Квантовые импульсы на выходе несбалансированного интерферометра Маха – Цендера станции Алиса .....	46
3.5. Уточнение требований к оптическому однофотонному передатчику станции Алиса .....	50
4. РАСЧЁТ ЭНЕРГОВРЕМЕННЫХ ПАРАМЕТРОВ ВОЛОКОННО-ОПТИЧЕСКОЙ ЛИНИИ СВЯЗИ .....	53
4.1. Расчёт потерь мощности излучения в волоконно-оптической линии связи .....	53
4.2. Исследование временных характеристик линии связи .....	54
4.3. Анализ поляризационных свойств линии связи .....	57
4.4. Компенсация поляризационных искажений в линии связи ...	60
5. ПРОЕКТИРОВАНИЕ ИНТЕРФЕРОМЕТРА МАХА – ЦЕНДЕРА ПРИЁМНОЙ СТАНЦИИ БОБ .....	63

---

5.1. Уточнение требований к интерферометру приёмной станции	63
5.2. Выбор поляризационного светоделителя .....	65
5.3. Выбор волоконно-оптической линии задержки .....	66
5.4. Выбор второго вращателя плоскости поляризации на $\pi/2$ .....	67
5.5. Выбор второго волоконно-оптического фазового модулятора	68
5.6. Выбор третьего контроллера поляризации .....	68
5.7. Выбор направленного волоконного ответвителя X-типа .....	70
6. ВРЕМЕННОЕ МУЛЬТИПЛЕКСИРОВАНИЕ КВАНТОВЫХ ИМПУЛЬСОВ .....	74
7. РЕГИСТРАТОР КВАНТОВЫХ ИМПУЛЬСОВ И ЭЛЕКТРОННЫЙ БЛОК СТРОБИРОВАНИЯ .....	77
7.1. Требования к однофотонному приёмному оптическому модулю .....	77
7.2. Уточнение требований к временным параметрам функционального модуля системы КРК .....	80
7.3. Формулирование требований к электронному блоку стробирования .....	81
8. РАСЧЁТ ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК РЕГИСТРАЦИИ КВАНТОВЫХ СОСТОЯНИЙ ФОТОНОВ .....	83
ЗАКЛЮЧЕНИЕ .....	87
СПИСОК ЛИТЕРАТУРЫ .....	88
ПРИЛОЖЕНИЕ. Статистические свойства длины волны лазера ID300 DFB фирмы ID QUANTIQUE .....	93
ТЕРМИНОЛОГИЧЕСКИЙ СЛОВАРЬ .....	100
ГЛОССАРИЙ .....	102