

УДК 621.391.63:004.056.52

ББК 32.86-5

Р865

Печатается по решению кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности Южного федерального университета (протокол № 18 от 22 апреля 2021 г.)

Рецензенты:

заведующий кафедрой «Информационная безопасность» Ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики (МТУСИ)», заслуженный деятель науки РФ, доктор технических наук, профессор *О. И. Шелухин*

профессор кафедры «Управление и интеллектуальные технологии» Федерального государственного образовательного учреждения высшего образования «Национальный исследовательский университет «МЭИ», доктор технических наук, профессор *Г. Ф. Филаретов*

Румянцев, К. Е.

Р865 Квантовые технологии в телекоммуникационных системах : учебник / К. Е. Румянцев ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2021. – 346 с.

ISBN 978-5-9275-3857-7

Изложены тенденции развития квантовых коммуникаций, вероятностные закономерности и основные понятия квантовой физики, раскрыты принципы квантовой криптографии, описаны направления развития и протоколы, типовые структуры и элементная база систем квантового распределения ключа и распределённых защищённых сетей на их основе. Освещены особенности функционирования систем квантового распределения ключа в условиях возможного несанкционированного доступа. Материал является основой для прослеживания технического уровня и тенденций развития систем квантового распределения ключа.

Учебник предназначен для студентов, обучающихся по специальности 10.05.02 Информационная безопасность телекоммуникационных систем.

УДК 621.391.63:004.056.52

ББК 32.86-5

ISBN 978-5-9275-3857-7

© Южный федеральный университет, 2021

© Румянцев К. Е., 2021

© Оформление. Макет. Издательство

Южного федерального университета, 2021

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ	3
СПИСОК СОКРАЩЕНИЙ ТЕРМИНОВ НА АНГЛИЙСКОМ ЯЗЫКЕ	8
СПИСОК СОКРАЩЕНИЙ ТЕРМИНОВ НА РУССКОМ ЯЗЫКЕ	11
ВВЕДЕНИЕ	12
ЧАСТЬ 1. ТЕНДЕНЦИИ РАЗВИТИЯ КВАНТОВЫХ КОММУНИКАЦИЙ	16
1. ВНЕДРЕНИЕ КВАНТОВЫХ ТЕХНОЛОГИЙ В ТЕЛЕКОММУНИКАЦИИ	17
1.1. Предпосылки внедрения квантовых коммуникаций	17
1.2. Идеи квантовой криптографии	25
Вопросы для самоконтроля усвоения материала	28
2. ТЕКУЩИЙ УРОВЕНЬ РАЗВИТИЯ ТЕХНОЛОГИЙ КВАНТОВОЙ КРИПТОГРАФИИ	30
2.1. Развитие технологий квантовой криптографии	30
2.2. Инфраструктура связи и квантовых коммуникаций	33
2.3. Развитие рынка квантовых коммуникаций	35
2.4. Постквантовая криптография	47
Вопросы для самоконтроля усвоения материала	48
ЧАСТЬ 2. ОСНОВЫ КВАНТОВОЙ ФИЗИКИ	50
3. ВЕРОЯТНОСТНЫЕ ЗАКОНОМЕРНОСТИ КВАНТОВОЙ ФИЗИКИ	51
3.1. Носители информации в квантовой коммуникации	51
3.2. Принципы квантовой механики	52
3.3. Условие интерференции волн	53
3.4. Интерференция амплитуд вероятности переходов	57
3.5. Классический опыт по регистрации электрона в интерферометре	60
3.6. Контроль поведения электрона в интерферометре	63
3.7. Суперпозиция состояний	66
3.8. Состояние двухуровневой квантово-механической системы	68
3.9. Парадокс «кота Шрёдингера»	69
3.10. Измерительный процесс в квантовой физике	72
3.11. Волновая функция	74

3.12. Основопологающие положения квантовой физики для квантовой коммуникации	76
Вопросы для самоконтроля усвоения материала	79
4. ОСНОВНЫЕ ПОНЯТИЯ И ПРИНЦИПЫ КВАНТОВОЙ ФИЗИКИ	82
4.1. Единичный квантовый бит	82
4.2. Геометрическое представление кубита	84
4.3. Состояние кубита после измерения в стандартном базисе ...	85
4.4. Принцип неопределённости Гейзенберга	86
4.5. Особенности проявления принципа неопределённости при приёме фотона	89
Вопросы для самоконтроля усвоения материала	90
5. ОДНОКУБИТНЫЕ ПРЕОБРАЗОВАНИЯ	92
5.1. Преобразование Адамара	92
5.2. Волоконный ответвитель Х-типа	93
5.3. Разделительный волоконный ответвитель Y-типа	97
5.4. Соединение двух волоконных ответвителей Х-типа	99
5.5. Интерферометр Маха – Цендера с фазовращателем	100
Вопросы для самоконтроля усвоения материала	102
6. КВАНТОВАЯ ТЕЛЕПОРТАЦИЯ	103
6.1. Парадокс Эйнштейна, Подольского и Розена	103
6.2. Сцепленные состояния	104
6.3. Сцепленные состояния между отдельными фотонами в результате спонтанного параметрического рассеяния излучения	107
6.4. Принципы квантовой телепортации	110
6.5. Неравенства Белла	111
6.6. Эксперимент с парой сцепленных фотонов	113
6.7. Процесс квантовой телепортации	119
6.8. Схема квантовой телепортации	121
6.9. Плотное кодирование	124
6.10. Вариант реализации протокола E91	129
6.11. Волоконно-оптические системы квантового распределения ключа с помощью сцепленных состояний	132
Вопросы для самоконтроля усвоения материала	133
ЧАСТЬ 3. КВАНТОВАЯ КРИПТОГРАФИЯ	135
7. НАПРАВЛЕНИЯ РАЗВИТИЯ КВАНТОВОЙ КРИПТОГРАФИИ	136

7.1. Квантовая криптография на основе кодирования квантового состояния одиночной частицы	136
7.2. Квантовая криптография на основе сцепленных состояний	137
7.3. Квантовое распределение ключа	138
7.4. Комплекс для передачи конфиденциальной информации с квантовым распределением ключа	140
7.5. Инфраструктура информационной безопасности при квантовом распределении ключа	142
Вопросы для самоконтроля усвоения материала	147
8. ПРОТОКОЛ BB84 ДВУХУРОВНЕВОЙ КВАНТОВОЙ СИСТЕМЫ	149
8.1. Теория кодирования состояний фотонов в протоколе BB84	149
8.2. Протокол BB84 с поляризационным кодированием состояний фотонов	150
8.3. Протокол BB84 с фазовым кодированием состояний фотонов	157
8.4. Протокол BB84 с временным кодированием состояний фотонов	165
Вопросы для самоконтроля усвоения материала	168
9. ПРОТОКОЛ КВАНТОВОЙ КРИПТОГРАФИИ B92	172
9.1. Теория кодирования состояний фотонов в протоколе B92 ...	172
9.2. Перспективы применения квантового распределения ключа по протоколу B92	173
9.3. Протокол B92 с поляризационным кодированием состояний фотонов	174
9.4. Протокол B92 с фазовым кодированием состояний фотонов	176
9.5. Протокол B92 с временным кодированием состояний фотонов	181
9.6. Контрольные задания	182
Вопросы для самоконтроля усвоения материала	188
ЧАСТЬ 4. ЭЛЕМЕНТНАЯ БАЗА КВАНТОВЫХ СИСТЕМ ТЕЛЕКОММУНИКАЦИИ	191
10. АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ И ТЕНДЕНЦИИ РАЗВИТИЯ ЭЛЕМЕНТНОЙ БАЗЫ КВАНТОВЫХ СИСТЕМ ТЕЛЕКОММУНИКАЦИИ	192
10.1. Анализ элементной базы атмосферных систем квантового распределения ключа	192

10.2. Анализ элементной базы волоконно-оптических систем квантового распределения ключа	194
10.3. Анализ элементной базы спутниковых систем квантового распределения ключа	195
10.4. Функциональные элементы систем квантового распределения ключа	201
Вопросы для самоконтроля усвоения материала	203
11. ОДНОФОТОННЫЕ ИСТОЧНИКИ ИЗЛУЧЕНИЯ	206
11.1. Источники одиночных фотонов	206
11.2. Специфика применения многофотонных лазеров	210
11.3. Поляризатор	214
11.4. Регулируемый волоконно-оптический аттенуатор	216
11.5. Спектральные свойства фотонов с однофотонного источника излучения	219
11.6. Требования к однофотонному источнику излучения	221
11.7. Расчётно-конструкторское задание	222
Вопросы для самоконтроля усвоения материала	223
12. ОДНОФОТОННЫЕ ПРИЁМНЫЕ ОПТИЧЕСКИЕ МОДУЛИ	225
12.1. Физические основы работы лавинных фотодиодов	225
12.2. Основные параметры лавинных фотодиодов	227
12.3. Цепи гашения однофотонных лавинных фотодиодов	233
12.4. Структура и параметры однофотонных приёмных оптических модулей	236
Вопросы для самоконтроля усвоения материала	239
13. ОПТОЭЛЕКТРОННЫЕ И ОПТИЧЕСКИЕ ЭЛЕМЕНТЫ	241
13.1. Фазовый оптический модулятор	241
13.2. Контроллер поляризации	243
13.3. Вращатель плоскости поляризации	246
13.4. Волоконно-оптический разветвитель	248
13.5. Волоконно-оптическая линия задержки	250
13.6. Поляризационный объединитель/светоделитель	252
13.7. Оптический циркулятор	253
13.8. Зеркало Фарадея	254
13.9. Оптические фильтры	254
13.10. Задание на проектирование волоконно-оптической линии задержки	255
	343

Вопросы для самоконтроля усвоения материала	255
ЧАСТЬ 5. ФОРМИРОВАНИЕ КЛЮЧЕВОЙ	
ПОСЛЕДОВАТЕЛЬНОСТИ	257
14. ЭТАПЫ ФОРМИРОВАНИЯ КЛЮЧЕВОЙ	
ПОСЛЕДОВАТЕЛЬНОСТИ	258
14.1. Обобщённая структура коммерческих системы КРК с фазо- вым кодированием состояний фотона	259
14.2. Формирование сырой ключевой последовательности	265
14.3. Формирование просеянной ключевой последовательности	266
14.4. Формирование одобренной ключевой последовательности	268
14.5. Коррекция ошибок	269
14.6. Усиление секретности	271
Вопросы для самоконтроля усвоения материала	274
15. СКОРОСТЬ ФОРМИРОВАНИЯ КЛЮЧЕВОЙ	
ПОСЛЕДОВАТЕЛЬНОСТИ	275
15.1. Оценка снижения скорости формирования ключевой после- довательности бит на физическом уровне	275
15.2. Оценка снижения скорости формирования ключевой после- довательности бит на логическом уровне	279
15.3. Скорость формирования секретной ключевой последова- тельности	285
15.4. Расчётное задание	286
ЧАСТЬ 6. ПРОБЛЕМЫ КВАНТОВОЙ КОММУНИКАЦИИ	289
16. КВАНТОВАЯ СЕТЬ	290
16.1. Концепция квантовой сети	290
16.2. Технология квантового распределения ключей в сетях с древовидной архитектурой	292
16.3. Квантовая сеть на основе квантовых повторителей	293
Вопросы для самоконтроля усвоения материала	295
17. СРЕДА РАСПРЕДЕЛЕНИЯ КВАНТОВЫХ КЛЮЧЕЙ	296
17.1. Волоконно-оптические направляющие среды	296
17.2. Открытое пространство	308
17.3. Расчётно-конструкторское задание	310
17.4. Оценка временных характеристик волоконно-оптической линии связи	311

17.5. Задание на расчёт принимаемой мощности оптического излучения в спутниковых системах связи	312
18. АТАКИ НА ВОЛОКОННО-ОПТИЧЕСКИЕ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА	313
18.1. Стратегия съёма информации в квантовых системах	313
18.2. Атаки на систему квантового распределения ключа с двухпроводной волоконно-оптической линией связи	313
18.3. Атаки на систему квантового распределения ключа с однопроводной волоконно-оптической линией связи	315
18.4. Роль процесса синхронизации в защите системы квантового распределения ключа от атак злоумышленника	316
18.5. Методы доступа к информации в волоконно-оптической линии и принципы защиты автокомпенсационных систем квантового распределения ключа от несанкционированного доступа	318
18.6. Принцип вхождения в синхронизм, защищённый от несанкционированного доступа к информации	322
Вопросы для самоконтроля усвоения материала	323
ЗАКЛЮЧЕНИЕ	324
СПИСОК ЛИТЕРАТУРЫ	326