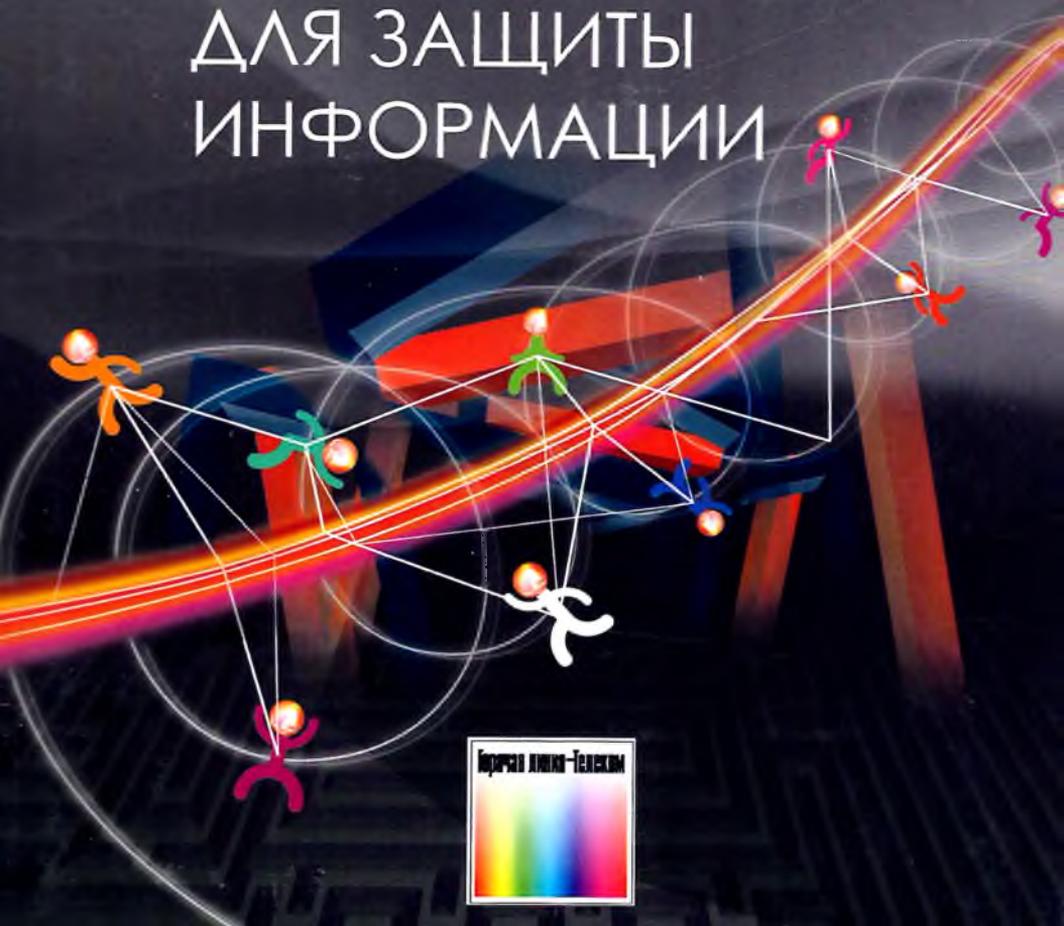


ПРИКЛАДНЫЕ КВАНТОВЫЕ ТЕХНОЛОГИИ

ДЛЯ ЗАЩИТЫ
ИНФОРМАЦИИ



Иррадиация - Техника



Оглавление

Благодарности	6
Предисловие.....	8
Структура книги	12
Введение	16
1 Кратко о применении технологии КРК в криптографии	20
Основы классической криптографии.....	20
Асимметричная криптография	23
Квантовая угроза и постквантовая криптография.....	30
Переход на квантовый уровень	39
Квантовое распределение криптографических ключей	42
Секретность квантовых протоколов	50
Повышение стойкости СКЗИ с помощью технологии КРК.....	52
Принцип построения модели угроз и нарушителя и некомпрометируемые коммуникации	52
Уменьшение нагрузки на ключ и защита от утечек по побочным каналам	56
Снижение эксплуатационных издержек с помощью технологии КРК	60
Квантовые сети.....	62
Идея квантовых сетей.....	62
Понятие о квантовозащищённых ключах	64
Квантовые сети произвольной топологии	68
2 Современные и перспективные сценарии применения КРК.....	74
Практика применения КРК.....	74
Сценарий 1. Защита ЦОД-ЦОД.....	74

Сценарий 2. Защита корпоративных коммуникаций	77
Сценарий 3. Удалённая доставка секретных ключей	81
Сети КРК — одна инфраструктура для многих сценариев применения	83
Перспективы применения систем КРК в России	87
3 Основы квантовой физики и квантовой информатики	89
Фотон и электромагнитные волны	89
Вероятностная теория измерений	92
Теорема о запрете клонирования фотона	94
4 Реализация технологии квантового распределения ключей	96
Разнообразие квантовых протоколов	96
Протокол BB84	99
Метод decoy state	101
Протокол РТС	104
Протокол ГОКС	106
КРК на боковых частотах	111
Протоколы с промежуточным узлом	112
КРК на непрерывных переменных	112
5 Атаки на протоколы и аппаратуру КРК	114
Виды квантовых атак	114
Атака с расщеплением по числу фотонов	116
Атака активного зондирования	117
Атака переизлучения	118
Атаки на детекторы	119
Атака лазерным повреждением	120
Меры защиты от атак на системы КРК	120
6 Практика использования КГСЧ в системах КРК	122
Где взять случайность?	122
Как работает КГСЧ	123
Реальность применения КГСЧ	125
Квантовый глоссарий	127
Ответы на часто задаваемые вопросы	132
Заключение	141
Список рекомендуемой литературы	143